

System Manual

P/N 063439-005

Model 200 Controller

 **ntermec**

A **UNOVA** Company

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 of Change
002	09/96	Added information on using the TRAKKER® Antares™ terminals with the Model 200 Controller. Made other minor corrections throughout the entire manual. Combined the information in the <i>JANUS™ Devices Quick Reference Guide</i> with the <i>Model 200 Controller User's Manual</i> .
003	04/97	Addendum 065395-001 was added to the manual. This addendum supports version 2.4 of the controller software, which includes VT and ANSI screen mapping and a direct TCP/IP socket interface.
004	10/97	Added information from the addendum to the manual. This manual supports controller software v3.0, which includes 3270 and 5250 terminal emulation on devices that run in Intermec's 900 MHz radio frequency network. The Script Builder tool was improved and a firmware upgrade utility for the TRAKKER Antares RF terminals was added.
005	07/98	This manual supports controller software v3.1, which adds DHCP and DNS support. It also contains information about a new remote console option, new system diagnostics, and new screen mapping functionality.

Quick Reference Guide

Fast Setup

 **ntermec**

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.

The information contained herein is proprietary and is provided solely for the purpose of allowing customers to operate and/or service Intermec manufactured equipment and is not to be released, reproduced, or used for any other purpose without written permission of Intermec.

Information and specifications in this manual are subject to change without notice.

© 1998 by Intermec Technologies Corporation
All Rights Reserved

The word Intermec, the Intermec logo, JANUS, IRL, TRAKKER, Antares, Adara, Duratherm, EZBuilder, Precision Print, PrintSet, Virtual Wedge, and CrossBar are either trademarks or registered trademarks of Intermec.

Throughout this manual, trademarked names may be used. Rather than put a trademark (™ or ®) symbol in every occurrence of a trademarked name, we state that we are using the names only in an editorial fashion, and to the benefit of the trademark owner, with no intention of infringement.

Contents

About Fast Setup 5

Network Adapter Cards 5

Using Online Help 6

Step 1 - Complete the Worksheets 8

Step 2 - Set Up the Controller 8

Power Cord 9

Monitor 9

Keyboard 9

Mouse 9

Step 3 - Install the Controller 10

Connecting to Your Data Collection Network 10

Connecting to Your Host Environment 10

Turning on the Controller 11

About the Fast Setup Main Menu 12

Step 4 - Set the System Parameters 13

Step 5 - Set Up the Data Collection Environment 16

Configuring an RF Card for Your Network 18

Configuring a UDP Plus Network 19

Configuring an Intermec Controller for Your Network 21

Verify Your Data Collection Environment 21

Step 6 - Set Up the Host Communications Environment 24

Ethernet Adapter Card 25

Token Ring Adapter Card 27

Coaxial Adapter Card 27

Twinaxial Adapter Card 28

SDLC Adapter Card 29

Step 7 - Configure the Host Environment Parameters 30

Setting Up Telnet Terminal Emulation 31

Setting Up 5250 SNA Terminal Emulation 36

Fast Setup Quick Reference Guide

Setting Up 3270 SNA Terminal Emulation 41

Setting Up Peer-to-Peer Links 47

Setting Up a Terminal Session 53

Verify Your Host Connection 65

Step 8 - Start the Controller 66

Where Do You Go From Here? 68



Index

This quick reference guide explains how to use Fast Setup to configure the Model 200 Controller.

About Fast Setup

Use Fast Setup to configure the Model 200 Controller quickly so you can

- demonstrate the controller.
- verify your network environment is functioning.
- learn about the controller and its graphical user interface (GUI) before using Advanced Setup.
- do preliminary configuration for your data collection network.

Fast Setup uses default values for many of the configuration parameters and it only prompts you to enter a few required parameters.

When you configure the controller in Fast Setup, you set up a host connection, define your Intermec equipment, and set up the routing for data to the correct destination.

Network Adapter Cards

Depending on the upline network cards in your controller, you can connect the controller to

- any TCP/IP host on an Ethernet or token ring network that supports Telnet.
- any SNA host on a token ring, twinaxial, coaxial, or SDLC network that supports APPC and 5250 or 3270 terminal connections.

Note: You can also set up VT, ANSI, 3270, and 5250 terminal sessions, but you can only start these terminal sessions on your controller. Fast Setup does not let you configure screen mapping.

Depending on the downline cards in your controller, you can connect the controller to

- Intermec's 900 MHz RF network.
- Intermec's 2.4 GHz RF network (UDP Plus) through access points connected to the Ethernet network.

Fast Setup Quick Reference Guide

The controller also has two serial ports (COM1 and COM2) that let you connect external Intermec controllers for CrossBar™ network support, a 9180 Network Controller, an uninterruptable power supply, or an external modem.

Using Online Help

The Model 200 Controller includes online help that provides descriptions of the toolbars, dialog boxes, and options. Help also includes step-by-step procedures and some background information.

To get help

- 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. Colored or underlined text indicates that you can jump to topics.

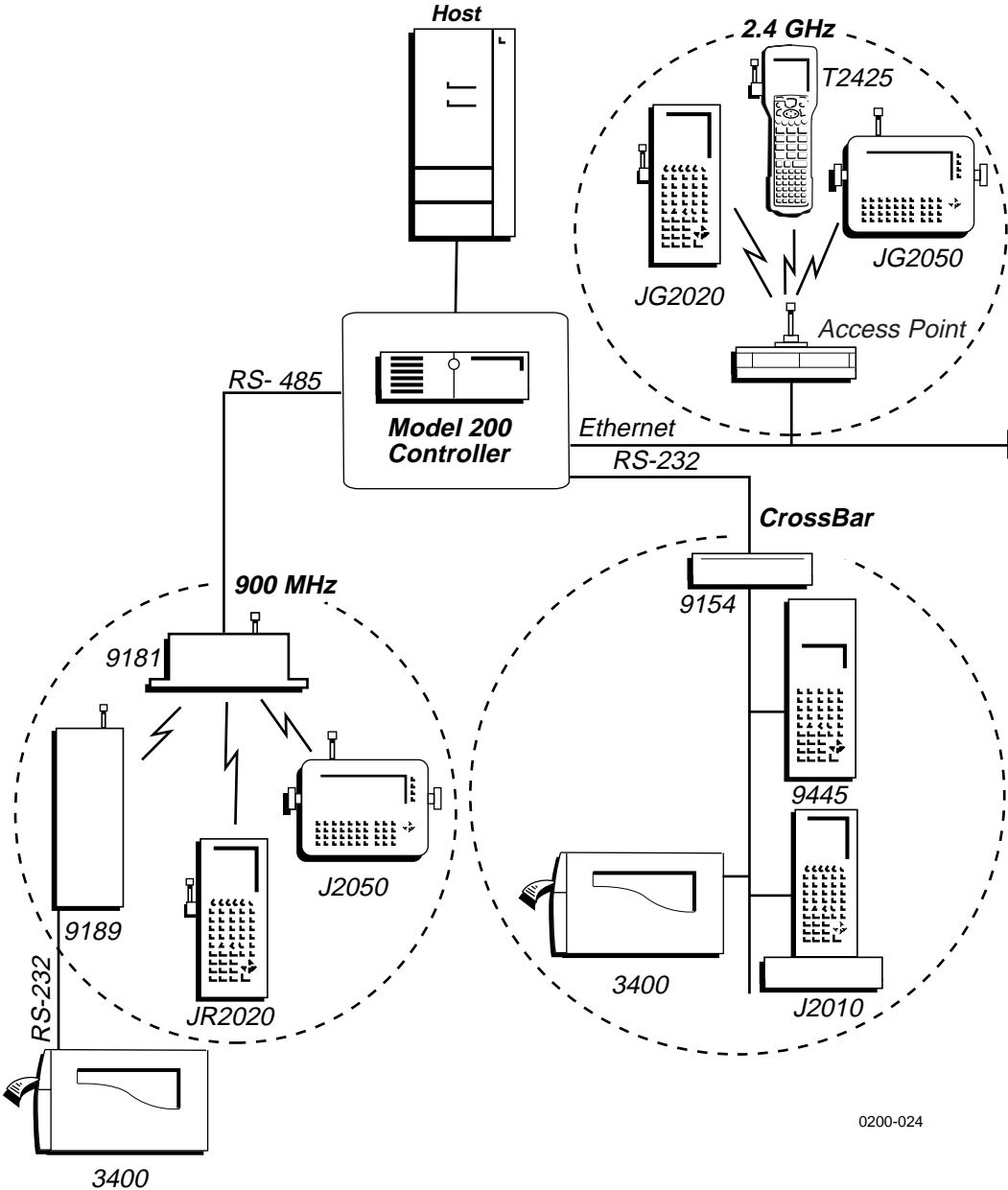
To jump to another help topic

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

To use the help buttons

- Choose Previous or press **Esc** to jump to the previous topic.
- 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.

Connecting the Controller to Your Data Collection Network



0200-024

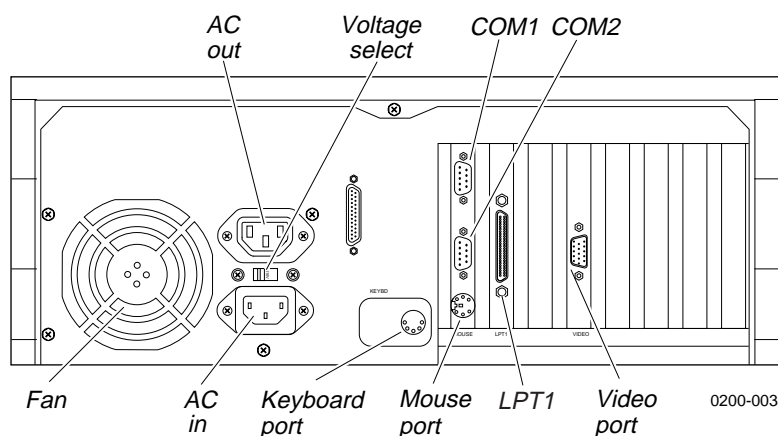
Step 1 - Complete the Worksheets

Before you use Fast Setup, complete the relevant worksheets in Appendix E in the *Model 200 Controller User's Manual*. You will need to obtain much of this information from your network administrator. After you have completed the worksheets, you will have all the information you need to run Fast Setup and to configure the controller successfully.

Step 2 - Set Up the Controller

Connect these accessories to the Model 200 Controller: power cord, monitor, keyboard, and mouse. Use the figure below to help you locate the ports for these accessories. For help, see Chapter 2, "Setting Up the Controller," in the *Model 200 Controller User's Manual*.

Model 200 Controller Rear Panel



Power Cord

The standard power cord that comes with the controller is a 110V U.S. cord. If you need another power cord, contact your local Intermec representative.

Note: Intermec recommends that you plug the power cord into a surge protector or an uninterruptable power supply.

1. Plug the power cord's 3-pin connector into the AC in receptacle in the rear panel of the controller.
2. Plug the other end of the power cord into an AC power outlet, a surge protector, or an uninterruptable power supply.
3. Set the voltage select switch to 110V or 220V.

Monitor

1. Plug the end of the monitor cable into the video port in the rear panel of the controller.
2. Attach one end of the power cable to the monitor and the other end to an AC outlet.

Keyboard

- Plug the keyboard connector into the keyboard port in the rear panel of the controller.

Mouse

- Plug the mouse connector into the mouse port in the rear panel of the controller.

Step 3 - Install the Controller

You must physically connect the Model 200 Controller to your data collection network and to your host environment.

Connecting to Your Data Collection Network

- Connect the controller to your data collection network. For help, see “Installing the Controller” in the chapter designed for your downline network in the *Model 200 Controller User’s Manual*.

Connecting to Your Host Environment

- Connect the controller to your host environment. For help, see “Installing the Controller” in the chapter designed for your upline network in the *Model 200 Controller User’s Manual*.

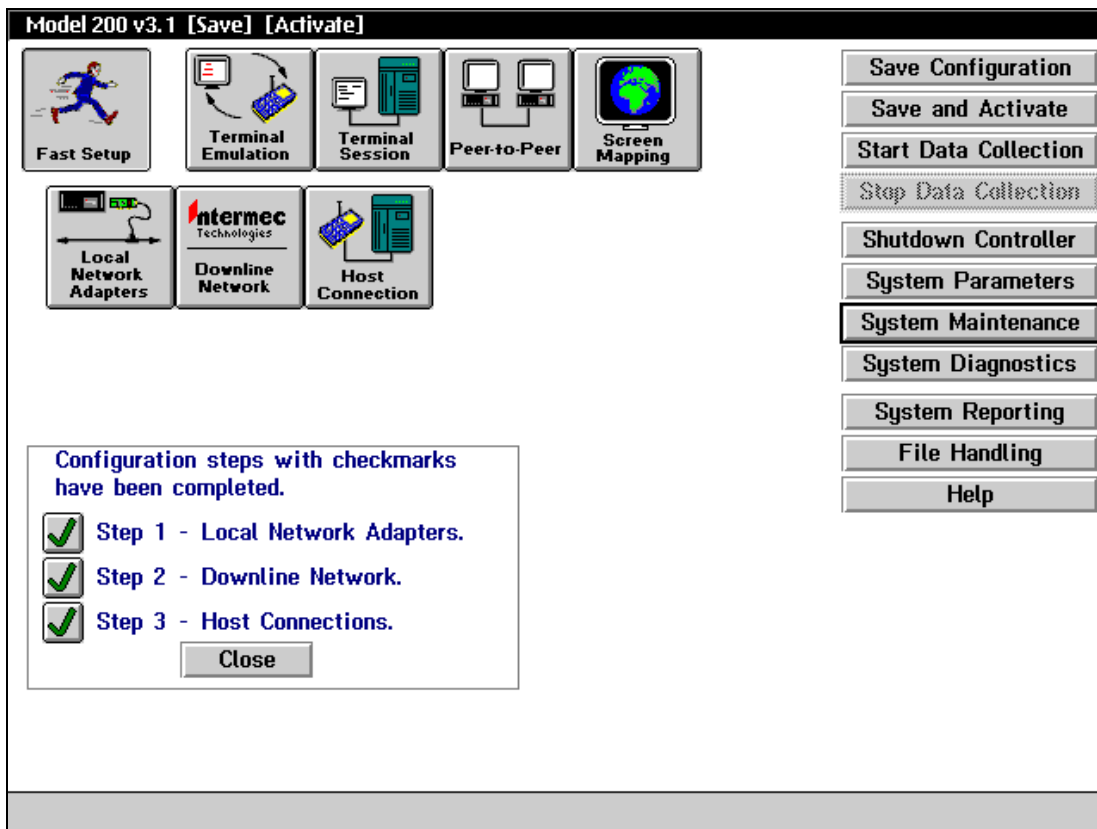
Note: If you are using 10Base2, make sure that you connect the cable to the port and connection before turning on the controller.

Turning on the Controller

When you turn on the controller for the first time, a dialog box appears that lists the network adapter cards, RF controller cards, and COM ports in your controller. Choose one of the following options:

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

The main menu appears. Choose Fast Setup. The Fast Setup main menu appears.



About the Fast Setup Main Menu

This main menu appears whenever you turn on the Model 200 Controller. In the title bar, [Save] and [Activate] appear when you make changes to the configuration that you need to save and activate. The Fast Setup main menu has three parts.

Toolbar Buttons

The buttons across the top of the main menu are grouped into two sections: Fast Setup and Advanced Setup. This quick reference guide (QRG) addresses how to use the first button, Fast Setup. For more information on Advanced Setup, see the *Model 200 Controller User's Manual*.

Sidebar Buttons

The buttons on the right side of the main menu perform system functions on the controller. This QRG explains how to use Save Configuration, Save and Activate, Start Data Collection, Stop Data Collection, Shutdown Controller, System Parameters, and some of the commands in the System Maintenance dialog box. For more information on the other buttons, see the *Model 200 Controller User's Manual*.

Checklist Box

The checklist box on the bottom left side of the main menu lists the three steps you complete to configure the controller in Fast Setup:

1. Local Network Adapters.

This box is checked after you enter the required parameters that identify the network adapter cards in the controller to the network.

2. Downline Network.

This box is checked after you configure the controller for your downline data collection network, including configuring any RF controller cards, the UDP Plus network, and any external Intermecc controllers.

3. Host Connections.

This box is checked after you configure the host connections for terminal emulation, peer-to-peer applications, or terminal sessions for screen mapping.

Step 4 - Set the System Parameters

When you set these system parameters, you are defining the operating parameters for the Model 200 Controller.

The screenshot shows a dialog box titled "System Parameters" with a checkmark icon in the top-left corner. The dialog contains several sections for configuring system parameters:

- Time Synchronization:** Includes a checked checkbox "Send to downline devices every" with a text input field containing "60" and the label "minutes (0-9999)".
- File Transfer Time:** Includes a text input field containing "180" and the label "seconds (0-9999)".
- Transaction Parameters:** Includes a label "ID delimiter:" followed by a dropdown menu showing a comma character. To the right is the text "The delimiter separates the transaction ID from the rest of the transaction's fields." Below this is a label "Bad ID response:" followed by an empty text input field.
- Peer-to-Peer Network Connection Parameters:** Includes a label "Maximum connections:" followed by a text input field containing "10" and the label "(1-256)". To the right is a label "Strip pad:" followed by a dropdown menu showing "<none>".
- Auto-Start:** Includes a checkbox "Auto-start data collection when the Model 200 Controller is booted." which is currently unchecked.
- Terminal Emulation Setup Screens:** Includes three checked checkboxes: "VT/ANSI", "5250", and "3270".

At the bottom of the dialog are three buttons: "OK", "Cancel", and "Help".

Fast Setup Quick Reference Guide

Field	Description	Value	Default
Send to downline devices every...	This check box determines if the Model 200 Controller sends its time to all external Intermec controllers.	Check, Clear	Check
...minutes	This field specifies how often in minutes the controller sends the time synchronization message.	0 to 9999	60
File Transfer Time	This box specifies how long in seconds the controller waits for a response from the data collection device when it is downloading files, before it times out.	0 to 9999	180
ID delimiter	The character that the data collection devices use to separate the transaction ID from the transaction fields.	Predefined	, (comma)
Bad ID response (Optional)	The message that the controller sends to the source of the transaction if the controller does not recognize the transaction ID.	1 to 39 characters	None
Max 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 controller to remove before sending the transaction.	Predefined	None
Auto-start data collection when the Model 200 Controller is booted.	This check box determines if the controller starts data collection when it is booted.	Check, Clear	Clear
Terminal Emulation Setup Screens	This box allows you to customize which terminal emulation buttons appear in the main menu.	VT/ANSI, 5250, 3270	All



To set the system parameters

1. From the main menu sidebar buttons, choose System Parameters. The System Parameters dialog box appears.
2. Enable or disable time synchronization. A check in the check box indicates that time synchronization is enabled. Enter how often you want the controller to send the time broadcast to all external Intermecc controllers and BRUs.
3. In the File Transfer Time box, enter how long you want the controller to wait for a response from a device when it is downloading files to that device, before it times out.
4. In the ID delimiter field, click the down arrow on the right side of the field. A list of available delimiters appears. Select the delimiter that you want to use to separate the transaction ID from the rest of the transaction fields in data coming from data collection devices.
5. (Optional) In the Bad ID response field, enter the message that you want sent back to the source of the transaction if the controller does not recognize the transaction ID.
6. In the Peer-to-Peer Network Connection Parameters box, enter the maximum number of connections for each NetComm process.
7. (Peer-to-peer applications, APPC only) In the Strip pad field, click the down arrow on the right side of the field. A list of characters that a host application may use to pad fixed-length transactions appears. Select the character that the controller removes before sending on the transaction.
8. In the Auto-Start box, enable or disable the controller from automatically starting data collection when it boots. A check in the check box indicates that the controller automatically starts data collection.
9. In the Terminal Emulation Setup Screens box, choose which type of terminal emulation you want displayed in the main menu.
10. Choose OK to save your changes and return to the main menu.

Step 5 - Set Up the Data Collection Environment

Worksheets available

- Model 200 Controller to RF Card Worksheet
- Model 200 Controller to TRAKKER Antares Terminals Worksheet
- Model 200 Controller to 9180 and CrossBar Worksheet
- Model 200 Controller to 9180 Worksheet
- Model 200 Controller to CrossBar Worksheet

You can use Fast Setup to define the parameters for any external Intermec controllers that exist downline from the Model 200 Controller, for RF controller cards that you may have inside the controller, and for the controller to communicate with the TRAKKER® Antares™ terminals using UDP Plus. Fast Setup assumes that any downline device that you add to the network is configured with factory defaults.

RF controller cards Fast Setup configures the controller to communicate with the first 9181 BRU on RF Card 1 and it enables this BRU. It also sets up this BRU to communicate with the first eight RF devices. If you have more than one RF card or more than one BRU, you will need to configure their RF parameters. For help configuring the other RF card, see Chapter 3, “Connecting to the Intermec RF Network” in the *Model 200 Controller User’s Manual*. For help configuring the BRU, see the *900 MHz RF Equipment User’s Manual*.

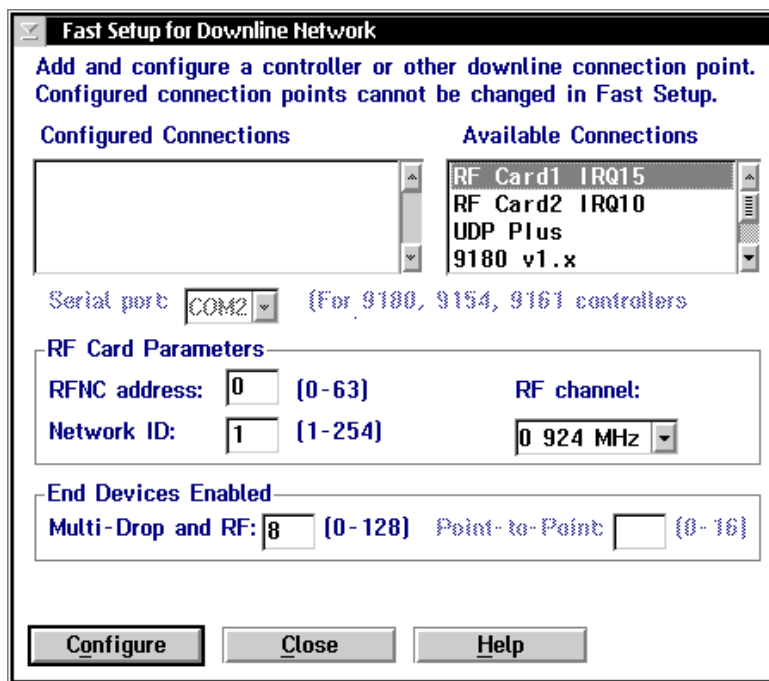
UDP Plus network Fast Setup configures the controller to communicate with JANUS devices and TRAKKER Antares terminals through the access points on an Ethernet or token ring network. You also need to define IP addresses for each of the terminals. Before you can verify your connection to the UDP Plus network, you must define an IP address for the Ethernet or token ring card. For help, see “Ethernet Adapter Card” and “Token Ring Adapter Card” later in this quick reference guide.

External Intermec controllers Fast Setup configures a few of the parameters that let the controller communicate with the external Intermec controller. However, you may still need to configure your external controller to send and receive transactions to the devices. Refer to your controller’s user’s manual.

Note: Once you define your external Intermec controllers, your RF controller cards, or UDP Plus and you choose Configure, Fast Setup does not let you edit the configuration. You need to use Advanced Setup to change any parameters.

Fast Setup Quick Reference Guide

To get to the Fast Setup for Downline Network dialog box, from the main menu choose Fast Setup and then choose Downline Network.



Field	Description	Value	Default
Configured Connections	The external Intermec controllers, RF controller cards, or UDP Plus that you have already configured.	None	None
Available Connections	The UDP Plus, RF controller cards, or any external Intermec controllers that are available to be configured.	If you have an open serial port, the direct connect controllers are listed. If you have an unconfigured RF card or UDP Plus, it is listed.	None

Fast Setup Quick Reference Guide

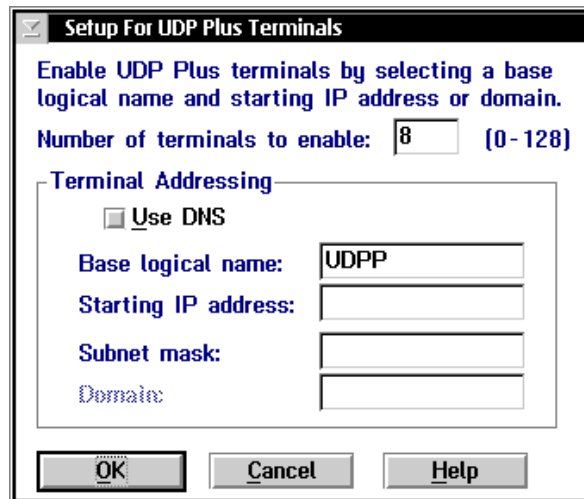
Field	Description	Value	Default
Serial port	The serial port on the controller that connects to the external Intermecc controller.	COM1, COM2	COM1
RFNC address	The radio frequency network address of the RF controller card. Devices use this address to communicate with the BRUs attached to this card.	0 to 63	0 If 0 is being used, the next available number is the default.
Network ID	The network ID of the RF controller card. Devices use this ID during a channel search to locate the RF controller card's RFNC address.	1 to 254	1 If 1 is being used, the next available value is used.
RF channel	The channel that the RF controller card will use.	0 to 6	0
Multi-Drop and RF	The number of device addresses to be enabled for the RF controller card, UDP Plus, or an external Intermecc controller.	Varies	8
Point-to-Point (9161 only)	The number of device addresses to be enabled on the 9161 controller.	Varies	9161-01 is 8 9161-02 is 0

Configuring an RF Card for Your Network

1. In the Available Connections list box, select the RF card you want to configure.
2. In the RF Card Parameters box, enter the RFNC address, network ID, and RF channel.
3. In the Multi-Drop and RF field, enter the number of device addresses you want to enable on the controller.
4. Choose Configure to save your changes. The RF card appears in the Configured Connections list box.
5. Choose Close to close the dialog box and return to the main menu.

Configuring a UDP Plus Network

1. In the Available Connections list box, select UDP Plus.
2. Choose Configure to save your changes. The Setup for UDP Plus Terminals dialog box appears.



To set up the UDP Plus devices using a DNS server

1. In the Number of terminals to enable field, enter the number of logical names that you want the controller to generate.
2. Check the Use DNS check box.

Note: Before you can use DNS, you must use Advanced Setup to configure a DNS server in the DNS Configuration dialog box.

3. In the Base logical name field, enter the base name that the controller uses to create a unique logical name for each terminal. The controller appends a sequential 3-digit number to this name for each terminal.

Fast Setup Quick Reference Guide

4. In the Domain field, enter the name of the domain that all of the terminals are in.

Note: If you enable 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.

5. Choose OK. The controller generates the logical names and you return to the Fast Setup for Downline Network dialog box.
6. Choose Close to close the dialog box and return to the main menu.

To set up the UDP Plus devices using the controller to generate IP addresses

1. In the Number of terminals to enable field, enter the number of IP addresses that you want the controller to generate.
2. Clear the Use DNS check box.
3. In the Base logical name field, enter the base name that the controller uses to create a unique logical name for each terminal. The controller appends a sequential 3-digit number to this name for each terminal.
4. In the Starting IP address field, enter the starting IP address. The IP address must be a valid IP v4 address.
5. In the Subnet mask field, enter the subnet mask that the server uses to validate the IP addresses. The controller verifies that they do not cross a subnet boundary.
6. Choose OK. The controller assigns valid sequential logical names and IP addresses to the terminals starting with the starting IP address and then you return to the Fast Setup for Downline Network dialog box.
7. Choose Close to close the dialog box and return to the main menu.



Configuring an Intermec Controller for Your Network

1. In the Available Connections list box, select the external Intermec controller you want to configure.
2. In the Serial port field, click the down arrow on the right side of the field. A list that contains the available serial ports appears. Choose the serial port on the Model 200 Controller that is connected to the external controller.
3. In the End Devices Enabled box, enter the number of Multi-Drop or Point-to-Point device addresses you want to enable on the controller.

Protocol	Controller	End Devices Enabled
Multi-Drop and RF	9180 v1.x, 9180 v2.x	0 through 128
	9154	0 through 32
	9161-02	0 through 128
Point-to-Point	9161-01	0 through 16
	9161-02	0 through 12

4. Choose Configure to save your changes. The controller appears in the Configured Connections list box.
5. Choose Close to return to the main menu.

Verify Your Data Collection Environment

Once you configure the Fast Setup for Downline Network dialog box, you may want to verify that you have a connection between the Model 200 controller and a device.

When sending a transaction to a device (destination), make sure that your device is ready to accept the transaction. If your device is not ready, the transaction is written to the Hot Standby file. If the device does not know how to interact with the Hot Standby file, subsequent transactions will also be written to the Hot Standby file. In this case, clear the Hot Standby file before sending another transaction to the device. For help, see "Clearing the Hot Standby Files" in Appendix A in the *Model 200 Controller User's Manual*.

Fast Setup Quick Reference Guide

Before you verify your data collection environment, make sure you activate your current configuration and start data collection.

To get to the Send Transaction dialog box, from the main menu sidebar buttons choose System Maintenance. The System Maintenance dialog box appears. Select Send Transactions and then choose Start. The Send Transaction dialog box appears.

Field	Description	Value	Default
Source ID (Optional)	This field can contain the destination 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 logical name of the device.	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 as either 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 characters	None

To verify your data collection environment

1. (Optional) In the Source ID field, enter a destination name that you want to use as the source of the transaction.
2. If you want to send the transaction to one device, in the Destination ID field enter the logical name of the device that you are using to verify the connection.

***Note:** If you are using the Send Transactions feature to verify your host connection, enter the name of the host application.*

Or, if you want to send the transaction to all the devices that are configured to accept it, in the Transaction ID field enter the unique name of the transaction.

3. In the Data or System field, enter D or S. This field defines the transaction as either a data or a system transaction.
4. (Optional) In the Data field, enter any data you want to send with the transaction ID.
5. Choose Send to send the transaction to the device.
6. Choose Close to close the dialog box and return to the System Maintenance dialog box.
7. Choose Close to return to the main menu.

Step 6 - Set Up the Host Communications Environment

To set up the host communications environment, you need to configure any network adapter cards in your Model 200 Controller. The network adapter cards that your controller may contain are:

- Ethernet
- token ring
- coaxial
- twinaxial
- SDLC

To configure the network adapter cards

1. From the main menu, choose Fast Setup.
2. Choose Local Network Adapter.

Note: Fast Setup grays out the buttons for any network adapter cards that are not installed in your controller.

3. Choose the button for the network adapter card you want to configure and follow the appropriate instructions in this section.

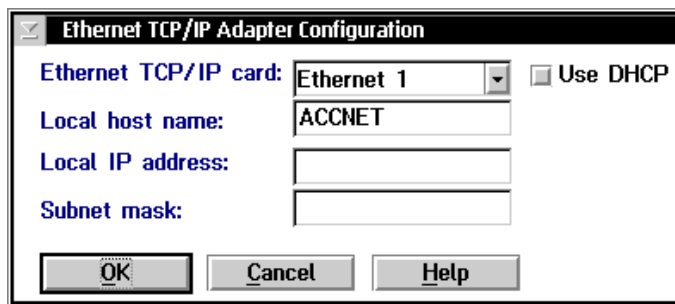
Ethernet Adapter Card

If you are using Ethernet adapter cards in the controller in a TCP/IP network, use Fast Setup to enter the parameters required for the TCP/IP protocol for each of the cards. Use the information from the Network Adapter Cards Worksheet to help you fill in the fields in this dialog box.

Note: The default setting for the Ethernet adapter card is 10BaseT. Contact your local Intermecc representative if you are using 10Base2 or 10Base5.

Note: If your controller contains two cards (two Ethernet cards or one Ethernet and one token ring card) that communicate using TCP/IP, each card must use a different subnet.

If you are not using the Ethernet adapter cards in a TCP/IP network, you do not need to configure them.



The screenshot shows a dialog box titled "Ethernet TCP/IP Adapter Configuration". It contains the following fields and controls:

- Ethernet TCP/IP card:** A dropdown menu with "Ethernet 1" selected.
- Use DHCP**
- Local host name:** A text field containing "ACCNET".
- Local IP address:** An empty text field.
- Subnet mask:** An empty text field.
- Buttons: **OK**, **Cancel**, and **Help**.

Fast Setup Quick Reference Guide

Field	Description	Value	Default
Ethernet TCP/IP card	The Ethernet card that you are configuring.	Ethernet 1 Ethernet 2	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 controller to the network.	1 to 12 alphanumeric characters	ACCNET
Local IP address	The IP address that identifies the Ethernet card. 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 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

To configure the Ethernet card

1. From the main menu, choose Fast Setup.
2. Choose Local Network Adapters.
3. Choose Ethernet. The Ethernet TCP/IP Adapter Configuration dialog box appears.
4. In the Ethernet TCP/IP Card field, click the down arrow on the right side of the field. A list of Ethernet cards that are installed in your controller appears. Select the card you want to configure.

***Note:** If you have two or more 10 Mbps Ethernet cards, Ethernet 1 is the Ethernet card that is in the slot the furthest left if you are facing the controller front panel. If you have a 100 Mbps Ethernet card, it is Ethernet 1.*

5. To enable DHCP, check the Use DHCP check box. Go to Step 9.
Or, to disable DHCP, clear the Use DHCP check box. Go to Step 6.

6. (Optional) In the Local host name field, enter a meaningful TCP/IP host name for the controller.
7. In the Local IP address field, enter the address that identifies this Ethernet card in the controller (host) to the network. This IP address must be a valid IP v4 address.
8. In the Subnet mask field, enter the mask used in the IP protocol layer to separate the subnet address from the local IP address.
9. Choose OK to save your changes and return to main menu.

Token Ring Adapter Card

If you are configuring the token ring card in the controller for a TCP/IP network, you need to use Advanced Setup. For help, see Chapter 5, "Connecting to an Ethernet/Token Ring Network" in the *Model 200 Controller User's Manual*.

If you are not using your token ring card in a TCP/IP network, you do not need to set any parameters for a token ring adapter connection. All parameters are set to default values. If you choose Token Ring, a message box appears.

Choose OK to close the message box and return to the main menu.

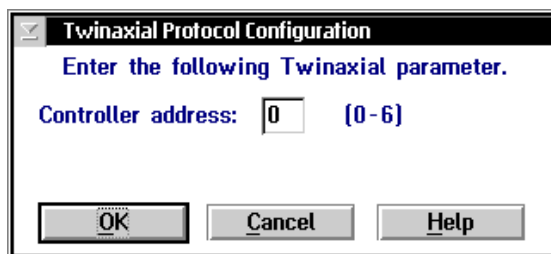
Coaxial Adapter Card

You do not need to set any parameters for a coaxial adapter connection. All parameters are set to default values. If you choose Coaxial, a message box appears.

Choose OK to close the message box and return to the main menu.

Twinaxial Adapter Card

If you have a twinaxial adapter card in the controller, you can use Fast Setup to establish a twinaxial connection between the controller and your host. Use the information from the Network Adapter Cards Worksheet to help you fill in the Controller address field in this dialog box.



Field	Description	Value	Default
Controller address	The unique host connection address.	0 to 6	0

To set the controller address

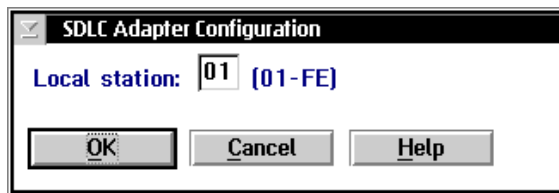
1. Choose Twinaxial. The Twinaxial Protocol Configuration dialog box appears.
2. In the Controller address field, enter the host connection address. Each twinaxial device on a twinaxial line must have a unique address.
3. Choose OK to save your changes and return to the main menu.



SDLC Adapter Card

If you have an SDLC adapter card in the controller, you can use Fast Setup to establish an SDLC connection between the controller and your host. Use the information from the Network Adapter Cards Worksheet to help you fill in the Local station field in this dialog box.

Fast Setup assumes that you are using a leased line for your SDLC configuration. To change this parameter, you must use Advanced Setup. For help, see Chapter 7, "Connecting to an SDLC Network" in the *Model 200 Controller User's Manual*.



Field	Description	Value	Default
Local station	The address of the controller on the SDLC network.	01 to FE	01

To configure the SDLC adapter

1. Choose SDLC. The SDLC Adapter Configuration dialog box appears.
2. In the Local station field, enter the controller station address. This address must match the controller workstation address defined on the host.
3. Choose OK to save your changes and return to the main menu.

Step 7 - Configure the Host Environment Parameters

You need to define the host environment parameters that tell the Model 200 Controller how to communicate with the host. Perform one of these procedures:

- Set up VT100/220/320, ANSI, 5250, or 3270 terminal emulation.
- Set up peer-to-peer links to run remote TCP/IP or APPC applications.
- Set up VT100/220/320, ANSI, 5250, or 3270 terminal sessions for screen mapping.

Note: Once you define your hosts and you choose OK, Fast Setup does not let you edit the configuration. You need to use Advanced Setup to change any parameters.

To configure the host environment parameters

1. From the main menu, choose Fast Setup.
2. Choose Host Connection.
3. Choose the button for the type of communications you want to configure and follow the appropriate instructions in this section.

Setting Up Telnet Terminal Emulation

You can use Fast Setup to set up VT100/220/320 or ANSI terminal emulation (TE) between JANUS™ devices and TRAKKER Antares terminals and your TCP/IP hosts. You can also set up TN5250 or TN3270 TE between your JANUS 2.4 GHz RF devices that are running UDP Plus and your JANUS 900 MHz RF devices and an IBM host that supports Telnet. You need to identify all remote host names and their IP addresses.

You also need to decide which terminals from the Available Terminals list box you want to explicitly link to a host. If an explicit link is set up between a terminal and a host, it means that the terminal can only start TE sessions with that host. If no explicit link is set up, the terminal can start a TE session with any host in the Host Name list. The controller starts a TE session with the host that is configured on the terminal.

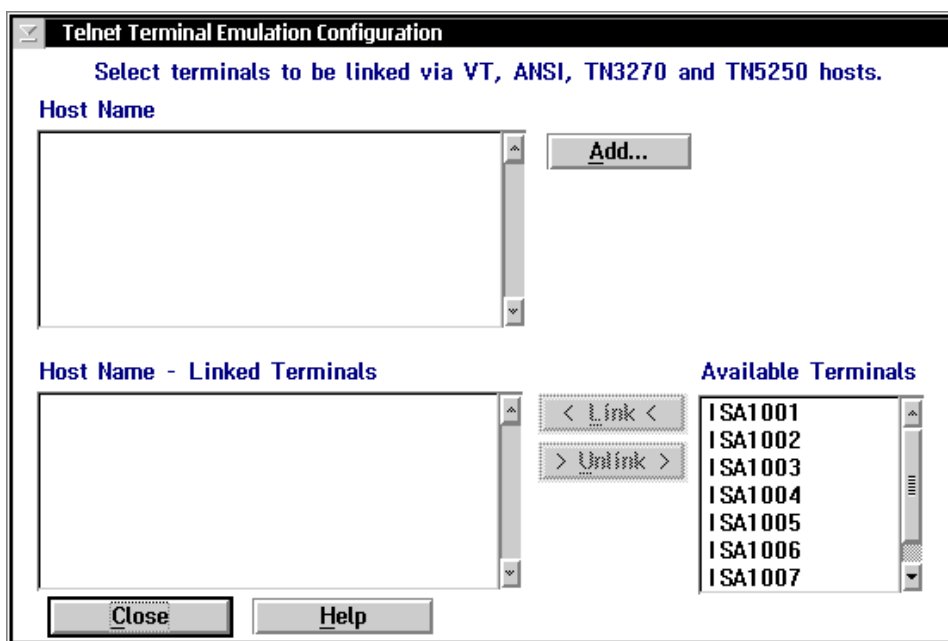
You can link as many device addresses as you want. However, the number of terminals that can simultaneously communicate through the controller depends on

- the number of devices you enabled in the Fast Setup for Downline Network dialog box.
- the number of terminals in your terminal license.

***Note:** You may need to load the correct TE software on all of the JANUS devices that you will be using as terminals. This software is available on the Model 200 Controller. Refer to Chapter 8, “Using Terminal Emulation” in the Model 200 Controller User’s Manual.*

Use the information from the Telnet Terminal Emulation Worksheet to help you fill in this dialog box.

Fast Setup Quick Reference Guide



Field	Description	Value	Default
Host Name	This list box contains the names of the defined TCP/IP hosts.	Predefined	None
Host Name - Linked Terminals	The list of terminals that are linked to a selected host.	None	None
Available Terminals	The list of all the terminals that are available to link to a host.	Predefined	None



To set up Telnet terminal emulation

1. Choose Telnet Terminal Emulation. The Telnet Terminal Emulation Configuration dialog box appears.
2. Make sure you have added all the Telnet hosts that the terminals will access. The Host Name list box contains all the defined host names.
To add a host, follow the instructions in “Adding a TCP/IP Host” in the next section.
3. (Optional) Create any explicit links between hosts and terminals.
 - a. In the Host Name list box, select the host that you want to link to a terminal.
 - b. In the Available Terminals list box, select the logical name of the terminal you want to link to the host.
 - c. Choose Link. The host name and the logical name appear in the Host Name - Linked Terminals list box.
4. (Optional) Unlink any explicit links between hosts and devices.
 - a. In the Host Name - Linked Terminals list box, select the terminal that you want to unlink from a host.
 - b. Choose Unlink. The host name and the logical name are removed from the Host Name - Linked Terminals list box.
5. Choose Close to close this dialog box and return to the main menu.

Fast Setup Quick Reference Guide

Adding a TCP/IP Host

To communicate with TCP/IP hosts, the Model 200 Controller must know their IP addresses. You can either use DNS to resolve these IP addresses or you can enter them in manually.

TCP/IP Host Connection

Enter the parameters for the TCP/IP host configuration.
(If you are using a DNS server, you can verify that this name resolves by pressing Resolve.)

Host name: Use DNS

IP address:

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.	Check, Clear	Clear
IP address	The address that identifies the TCP/IP host to the network.	xxx.xxx.xxx.xxx where xxx is a value between 0 and 255.	None

To determine the host IP address using DNS

1. From the Telnet Terminal Emulation Configuration dialog box, choose Add. The TCP/IP Host Connection dialog box appears.
2. In the Host name field, enter the abbreviated or long host name. If you enter the abbreviated name, the controller searches the domain names in the DNS Configuration dialog box to determine the long host name.
3. Enable the Use DNS check box.

Note: Before you enable this check box, you must first configure a DNS server in the DNS Configuration dialog box.

4. (Optional) Choose Resolve. The controller searches in the domains that are listed in the DNS Configuration dialog box for the host name and resolves the IP address.
5. Choose OK to save your changes and return to the Telnet Terminal Emulation Configuration dialog box.

To configure the host IP address manually

1. From the Telnet Terminal Emulation Configuration dialog box, choose Add. The TCP/IP Host Connection dialog box appears.
2. In the Host name field, enter the host name.
3. Make sure the Use DNS check box is disabled.
4. In the IP address field, enter the host's IP address.
5. Choose OK to save your changes and return to the Telnet Terminal Emulation Configuration dialog box.

Setting Up 5250 SNA Terminal Emulation

You can use Fast Setup to set up 5250 SNA terminal emulation (TE) between your JANUS 900 MHz RF devices or your TRAKKER Antares terminals and SNA hosts. You need to identify all remote host names.

You also need to decide which terminals from the Available Terminals list box you want to explicitly link to a host. If an explicit link is set up between a terminal and a host, it means that the terminal can start a TE session only with that host. If no explicit link is set up, the terminal can start a TE session with any host in the Host Name list. It will start a TE session with the host that is configured on the terminal.

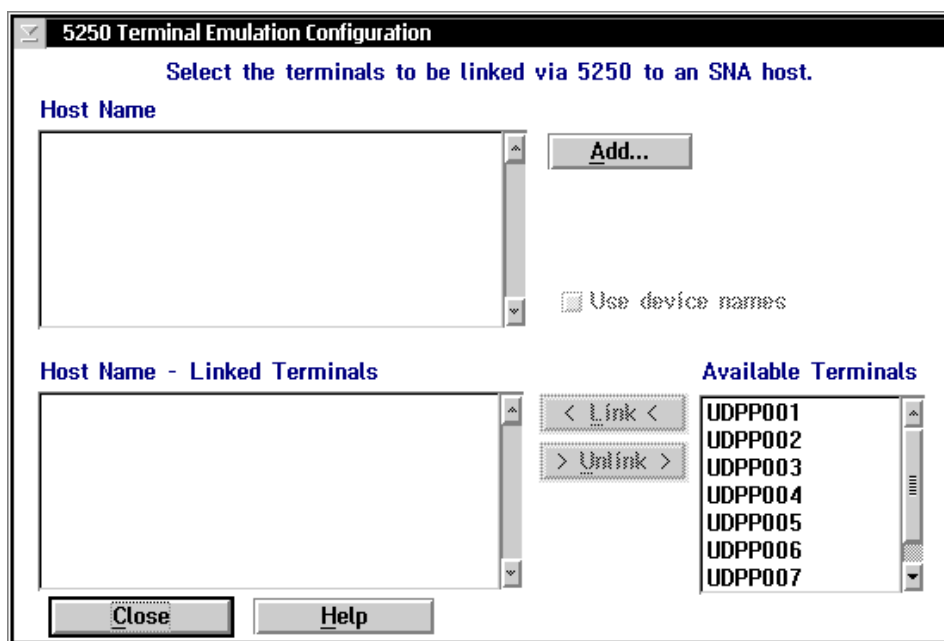
You can link as many terminals as you want. However, the number of terminals that can simultaneously communicate through the controller depends on

- the number of devices you enabled in the Fast Setup for Downline Network dialog box.
- the mode you are using to define the terminal session characteristics between the controller and the SNA host. The default mode is #INTER. For help, see “Creating Terminal Sessions” in Chapter 10 in the *Model 200 Controller User’s Manual*.
- the number of terminals in your terminal license.
- the maximum number of virtual devices the AS/400 5250 Display Station Pass-Through program supports.

Note: Your JANUS 900 MHz RF devices and your TRAKKER Antares terminals come with the 5250 TE software already loaded. However, this software is also available on the Model 200 Controller.

Also, you must configure your terminals to use the SNA protocol.

Use the information from the 5250 Terminal Emulation Worksheet to help you fill in this dialog box.



Field	Description	Value	Default
Host Name	This list box contains the names of the defined SNA hosts.	Predefined	None
Use device names	This check box determines if the selected host in the Host Name list box uses the logical name of the devices when establishing terminal sessions.	Check, Clear	Clear
Host Name - Linked Terminals	The list of terminals that are linked to a selected host.	None	None
Available Terminals	The list of all terminals that are available to link to a host.	Predefined	None

Fast Setup Quick Reference Guide

To set up 5250 terminal emulation

1. Choose 5250 Terminal Emulation. The 5250 Terminal Emulation Configuration dialog box appears.
2. Make sure you have added all the SNA hosts that the terminals will access for terminal emulation. The Host Name list box contains all the defined host names.

To add a host, follow the instructions in “Adding an IBM SNA Host” in the next section.

3. Check the Use device names check box if you want the selected host to use the logical name of the devices when establishing terminal sessions. A Yes appears next the host name under the Names column.
4. (Optional) Create any explicit links between hosts and terminals.
 - a. In the Host Name list box, select the host that you want to link to a terminal.
 - b. In the Available Terminals list box, select the terminal you want to link to the host.
 - c. Choose Link. The terminal appears in the Host Name - Linked Terminals list box.
5. (Optional) Unlink any explicit links between hosts and terminals.
 - a. In the Host Name - Linked Terminals list box, select the terminal you want to unlink from a host.
 - b. Choose Unlink. The host name and logical name are removed from the Host Name - Linked Terminals list box.
6. Choose Close to close this dialog box and return to the main menu.



Adding an IBM SNA Host

Field	Description	Value	Default
Host name	A 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, 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	Controller's network ID from the SNA local node definition
Host LU	The LU name that identifies the host. This field 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.	8 uppercase alphanumeric or special characters	SNA node name + 2-digit suffix, starting with 01
Address (Ethernet or token ring only)	The LAN adapter address of the host.	Token ring MAC address format	None

Fast Setup Quick Reference Guide

To add an IBM SNA host

1. From the 5250 Terminal Emulation Configuration dialog box, choose Add. The Host Connection Configuration dialog box appears.
2. In the Host name field, enter a meaningful name for the host.
3. In the Adapter card field, click the down arrow on the right side of the field. A list that contains the available adapter cards appears. Select the adapter card you are using to connect to the host.
4. In the Network ID field, enter the network ID of the network on which the host resides.
5. In the Host LU field, enter the LU (logical unit) name that identifies the host. This field must match the control point (CP) name or node name of the host.
6. (Ethernet or token ring only) In the Local PU field, enter a unique PU (physical unit) name for the host. The default name is the local SNA node name plus a 2-digit suffix.
7. (Ethernet or token ring only) In the Address field, enter the LAN adapter address of the remote host.
8. Choose OK to save your changes and return to the 5250 Terminal Emulation Configuration dialog box.

Setting Up 3270 SNA Terminal Emulation

You can use Fast Setup to set up 3270 SNA terminal emulation (TE) between your JANUS 900 MHz RF devices or your TRAKKER Antares terminals and SNA hosts. You need to identify all remote host names.

You also need to decide which terminals from the Available Terminals list box you want to explicitly link to a host. If an explicit link is set up between a terminal and a host, it means that the terminal can start a TE session only with that host. If no explicit link is set up, the terminal can start a TE session with any host in the Host Name list, as long as the host has NAU addresses available. It will start a TE session with the host that is configured on the terminal.

You can link as many terminals as you want. However, the number of terminals that can simultaneously communicate through the controller depends on

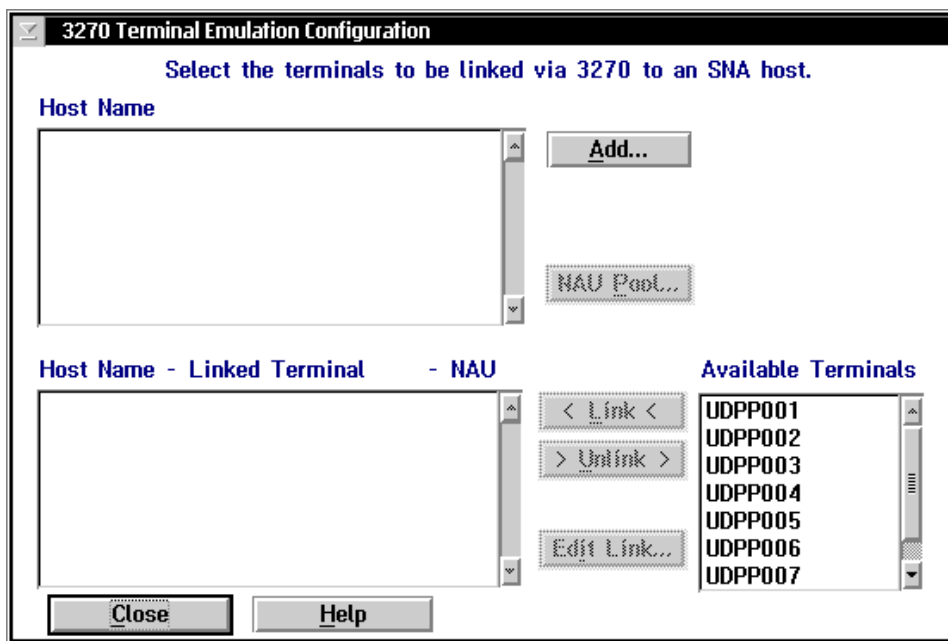
- the number of devices you enabled in the Fast Setup for Downline Network dialog box.
- the number of terminals in your terminal license.
- the NAUs available on the remote hosts. You need to define these NAUs on the controller. You can add these NAUs to an NAU pool. Then, terminals that want to communicate with a host can dynamically link with them. Or, you can explicitly link an NAU to a terminal and a host.

Note: Your JANUS 900 MHz RF devices and your TRAKKER Antares terminals come with the 3270 TE software already loaded. However, this software is also available on the Model 200 Controller.

Also, you must configure your terminals to use the SNA protocol.

Use the information from the 3270 Terminal Emulation Worksheet to help you fill in this dialog box.

Fast Setup Quick Reference Guide



Field	Description	Value	Default
Host Name	This list box contains the names of the defined SNA hosts.	Predefined	None
Host Name - Linked Terminal - NAU	The list of terminals and their NAUs that are linked to a selected host.	None	None
Available Terminals	The list of all terminals that are available to link to a host.	Predefined	None



To set up 3270 terminal emulation

1. Choose 3270 Terminal Emulation. The 3270 Terminal Emulation Configuration dialog box appears.
2. Make sure you have added all the SNA hosts that the terminals will access for terminal emulation. The Host Name list box contains all the defined host names.

To add a host, follow the instructions in “Adding an IBM SNA Host” later in this section.

3. Decide how to set up NAUs for the terminals:
 - Fill the NAU pool for each of the hosts, but do not explicitly link any terminals to hosts.
 - Do not fill the NAU pool for any of the hosts. When you explicitly link terminals to hosts, the controller generates NAUs starting at 002.
 - 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” later in this section.

4. (Optional) Create any explicit links between hosts, terminals, and NAUs.
 - a. In the Host Name list box, select the host that you want to link to a terminal.
 - b. In the Available Terminals list box, select the terminal you want to link to the host.
 - c. Choose Link. The host, terminal, and first available NAU appear in the Host Name - Linked Terminal - NAU list box.

To change the NAU that the controller assigns to the terminal, follow the instructions in “Editing a Link” later in this section.

5. (Optional) Unlink any explicit links between hosts, terminals, and NAUs.
 - a. In the Host Name - Linked Terminal - NAU list box, select the terminal you want to unlink from a host.
 - b. Choose Unlink. The host, terminal, and NAU are removed from the Host Name - Linked Terminal - NAU list box.
6. Choose Close to close this dialog box and return to the main menu.

Adding an IBM SNA Host

Field	Description	Value	Default
Host name	A 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 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.	8 uppercase alphanumeric or special characters	SNA node name + 2-digit suffix, starting with 01
Address (Ethernet or token ring only)	The LAN adapter address of the host.	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 controller.	8 hexadecimal characters	05D00000

To add an IBM SNA host

1. From the 3270 Terminal Emulation Configuration dialog box, choose Add. The Host Connection Configuration dialog box appears.
2. In the Host name field, enter a meaningful name for the host.
3. In the Adapter card field, click the down arrow on the right side of the field. A list that contains the available adapters appears. Select the adapter you are using to connect to the host.
4. (Ethernet or token ring only) In the Local PU field, enter a unique PU (physical unit) name for the host. The default name is the local SNA node name plus a 2-digit suffix.
5. (Ethernet or token ring only) In the Address field, enter the LAN adapter address of the remote host.
6. In the Node ID field, enter the last eight characters in the XID that establish a host connection. The Node ID is the same as the XID.

Note: When establishing a connection, the host or controller with the higher Node ID number is the primary workstation.

7. Choose OK to save your changes and return to the 3270 Terminal Emulation Configuration dialog box.

Filling the NAU Pool



Fast Setup Quick Reference Guide

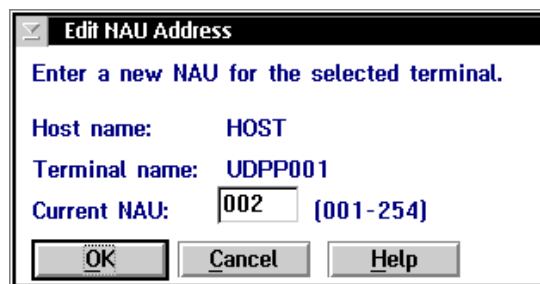
1. From the 3270 Terminal Emulation Configuration dialog box, choose NAU Pool. The 3270 NAU Pool dialog box appears.
2. Add all the NAUs to the NAU pool.

Note: Once an NAU is in the pool, you cannot use it in an explicit link.

- a. In the New NAU field, type in the address.
 - b. Choose Add. The NAU is added to the Unlinked NAUs pool.
3. Remove any NAUs that you do not want in the pool or that you want to use in an explicit link.
 - a. In the Unlinked NAUs pool, choose the NAU to remove.
 - b. Choose Delete. The NAU is removed from the pool. You can now use this NAU in an explicit link.

Editing a Link

1. From the 3270 Terminal Emulation Configuration dialog box in the Host Name - Linked Terminal - NAU list box, select the NAU to change.
2. Choose Edit Link. The Edit NAU Address dialog box appears.



3. In the Current NAU field, enter a new NAU for the terminal.
4. Choose OK to save your changes and return to the 3270 Terminal Emulation Configuration dialog box.

Setting Up Peer-to-Peer Links

To run TCP/IP or APPC applications in your data collection network, you must define all the destination names in the Model 200 Controller. The controller puts these names in a peer-to-peer destination list. You must also specify which transactions the controller routes to each application.

The Peer-to-Peer Destination Parameters dialog box also lets you set the Hot Standby timeout and delivery response messages.

The screenshot shows the 'Peer-to-Peer Destination Parameters' dialog box. The title bar reads 'Peer-to-Peer Destination Parameters'. Below the title bar, the text 'Configure this peer-to-peer destination and its transactions.' is displayed. The dialog contains several input fields and controls:

- Destination name:** A text input field.
- Hot Standby timeout:** A numeric input field containing '20', followed by the text 'seconds (1-9999)'.
- Transactions held in volatile memory:** Three radio buttons: 'None', 'Unlimited', and 'Maximum'. The 'Maximum' option is selected. To the right of the 'Maximum' radio button is a numeric input field containing '50' and the text '(1-9999)'.
- International text pass-through:** A checkbox that is currently unchecked.
- Transactions:** A section with two list boxes. The left list box is labeled 'Selected' and is currently empty. Below it is an 'Add...' button. The right list box is labeled 'Available' and is also empty. Between the two list boxes are two buttons: '< Select <' and '> Remove >'. Both list boxes have vertical scroll bars.
- Delivery Responses (if any):** A section with two text input fields. The first is labeled 'Interactive response:' and the second is labeled 'Hot Standby:'.
- Buttons:** At the bottom of the dialog are three buttons: 'OK', 'Cancel', and 'Help'.

Fast Setup Quick Reference Guide

Field	Description	Value	Default
Destination name	The name of the destination (application).	1 to 16 alphanumeric characters	None
Hot Standby timeout	The number of seconds the controller waits for a response from a destination before it places the transactions going to that destination in a Hot Standby file.	0 to 9999	20
Transactions held in volatile memory	The number of transactions the controller keeps in RAM before it writes them to a Hot Standby file.	None, Unlimited, Maximum	Maximum 50
International text pass-through	This check box determines how much of the transaction is converted. Check this box to enable this feature. The server converts only the transaction header. Clear this box to use limited EBCDIC mapping. The server converts the entire transaction.	Check, Clear	Clear
Selected	This list box contains the transaction IDs that are routed to this destination.	None	None
Available	This list box contains all the transaction IDs that are available to add to the Selected list box.	Predefined	None
Interactive response (Optional)	The message that is sent to the source of the transaction when the transaction for the destination is delivered successfully.	1 to 39 characters	None
Hot standby (Optional)	The message that is sent to the source of the transaction when the transaction for the destination is written to a Hot Standby file.	1 to 39 characters	None



To set up your peer-to-peer link

1. Choose Peer-to-Peer. The Peer-to-Peer Destination Parameters dialog box appears.
2. In the Destination name field, enter the name of the destination (application) that will accept the transactions in the Transaction box.

Note: You need to add the name of each data collection device in a 2.4 GHz RF network that will communicate with the Model 200 Controller.

3. In the Hot Standby timeout field, enter the number of seconds the controller waits for an acknowledgment from the destination before it places the transactions going to that destination in a Hot Standby file.
4. Choose the number of transactions you want the controller to keep in RAM before it writes them 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 controller stores in RAM before it writes them to a file.
5. Enable or disable international text pass-through. A check in the check box means that international text pass-through is enabled.
6. Add all transaction IDs that you want routed to the destination to the Selected list box.
 - a. From the Available list box, select a transaction to be added to the Selected list box.
 - b. Choose Select. The transaction ID appears in the Selected list box.
7. Remove any transactions that you do not want routed to the destination from the Selected list box.
 - a. From the Selected list box, select a transaction to be removed.
 - b. Choose Remove. The transaction ID is removed from the Selected list box.

Fast Setup Quick Reference Guide

8. Add any transaction IDs that are not listed in the Available list box. Follow the instructions in the next section, "Adding a Transaction."
9. (Optional) In the Delivery Responses box, enter the messages you want to send to the transaction source.
 - In the Interactive response field, enter the message you want to send to the source of the transaction when the transaction for the destination is successfully delivered in Interactive mode.
 - In the Hot standby field, enter the message you want to send to the source of the transaction when the transaction for the destination is not successfully delivered and is written to a Hot Standby file.
10. Choose OK to save your changes and return to the main menu.

Adding a Transaction

You need to define transaction IDs so the controller can route them to their proper destination.

Transaction Parameters

Define a transaction ID and its fields. You must define fields whenever screen mapping from a transaction is required.

Transaction ID:

Hot Standby message (if any):

Transaction Field Parameters

	Value	Field Name
Delimiter: <input type="text" value=","/>	<input type="text"/>	<input type="text"/>



Field	Description	Value	Default
Transaction ID	The unique name 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 controller places the transactions for the destination in a Hot Standby file.	1 to 39 characters	None
Delimiter	The character that separates the fields in the transaction.	Predefined	, (comma)

To add a transaction

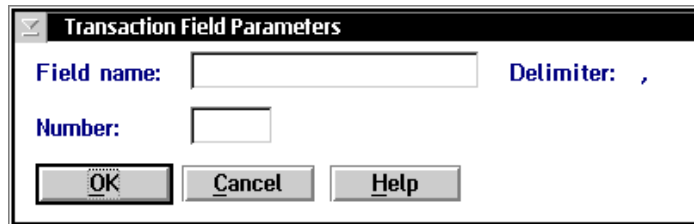
1. From the Peer-to-Peer Destination Parameters dialog box, choose Add. The Transaction Parameters dialog box appears.
2. In the Transaction ID field, enter the unique ID for the transaction.
3. (Optional) In the Hot Standby message field, enter the message that the controller sends to the source of the transaction when it places the transactions for the destination in a Hot Standby file.
4. In the Delimiter field, click the down arrow on the right side of the field. A list of delimiter characters appears. Choose one.

Note: This delimiter may differ from the delimiter set in the System Parameters dialog box.

5. (Optional) Add, edit, or delete transaction fields from the list box. For help, see the next sections.
6. Choose OK to save your changes and return to the Peer-to-Peer Destination Parameters dialog box.

Fast Setup Quick Reference Guide

To add transaction fields



Transaction Field Parameters

Field name: Delimiter: ,

Number:

OK Cancel Help

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

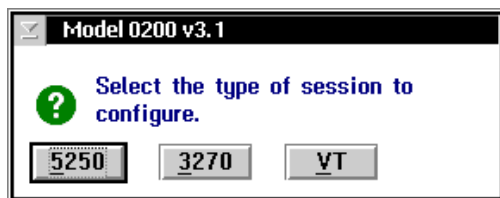
1. From the Transaction Parameters dialog box, choose Add. The Transaction Field Parameters dialog box appears.
2. In the Field name field, enter a name for the transaction field.
3. In the Number field, enter the order or position of the field in the transaction. The first field in the transaction is at position 1.
4. Choose OK to save your changes and return to the Transaction Parameters dialog box.

Setting Up a Terminal Session

You can use Fast Setup to establish VT, ANSI, 5250, or 3270 terminal sessions between the controller and your host. Use these sessions to access your host directly from the controller. By accessing your host, you can verify your host connection and you can start remote applications. Later, using Advanced Setup, you can use this session to configure and run screen mapping.

To set up a terminal session

1. Choose Terminal Session. This message box appears.



2. Choose the button for the type of terminal session you want to configure and follow the appropriate instructions for configuring this terminal session.

Configuring a VT/ANSI Terminal Session

Field	Description	Value	Default
Name	A meaningful name for this terminal session.	1 to 8 alphanumeric characters	None
Terminal mode	The type of terminal mode 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.	Predefined	None
Number of sessions	The number of terminal sessions you want to run on the controller.	1 to 228	1
Port number	The port number on which this session will communicate with the Telnet daemon on the host.	0 to 65535	23



To configure a VT/ANSI terminal session

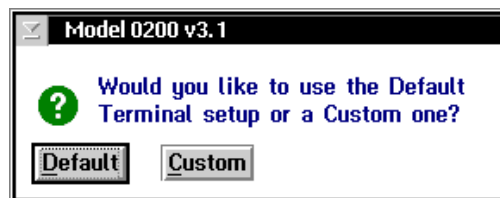
1. Choose VT. The Terminal Session Definition dialog box appears.
2. In the Session box, enter a meaningful name for the session.
3. In the Terminal mode field, click the down arrow on the right side of the field. A list that contains the different terminal modes appears. Select the type of terminal mode you want to use for this terminal session.
4. In the Host Name box, click the down arrow on the right side of the field. A list that contains existing TCP/IP host names appears. Select the host that you want to connect with for this session.

Or, add a new host. For help, see “Adding a TCP/IP Host” earlier in this quick reference guide.

5. In the Number of sessions field, enter the number of terminal sessions that you want to run on the controller.
6. In the Port number field, enter the host port number on which this session will communicate.

Note: Telnet uses port number 23 (default).

7. Choose OK to save your changes. A message box appears.

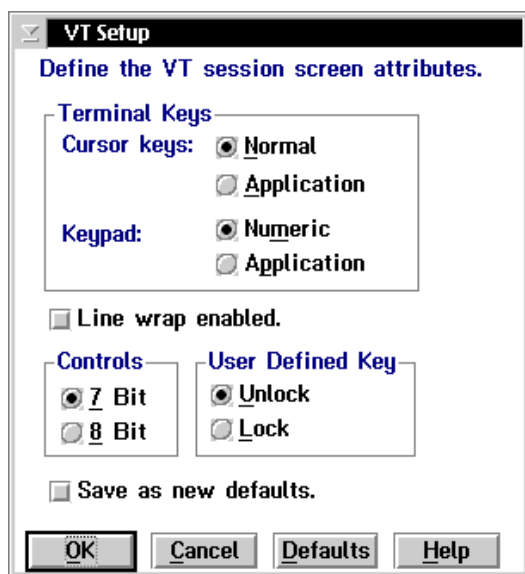


8. Choose Default to use the default terminal setup. The message box closes and you return to the main menu.

Or, choose Custom to customize the terminal setup. The VT Setup dialog box appears. For help, see “Customizing the VT Terminal Setup” later in this section.

Customizing the VT Terminal Setup

When you add a new VT or ANSI terminal session and you choose Custom, the VT Setup dialog box automatically 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.





Field	Description	Value	Default
Cursor keys	Determines whether the arrow keys on the terminal control cursor movement or they send their application control functions.	Normal, Application	Normal
Keypad	Determines whether the number keys on the terminal send their keycap characters or they send their programming functions.	Numeric, Application	Numeric
Line wrap enabled	This check box determines if text automatically wraps to the next line when it reaches the right margin.	Check, Clear	Clear
Controls	Defines the type of control characters that your terminal uses.	7 bit, 8 bit	7 bit
User-Defined Key	Determines whether or not the host can change the user-defined keys.	Unlock, Lock	Unlock
Save as new defaults	This check box determines if the current parameter settings are the default parameter settings.	Check, Clear	Clear

Fast Setup Quick Reference Guide

To customize the terminal setup

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

1. In the Terminal Keys box, choose Normal if you want to use the terminal cursor keys to move the cursor.
Choose Application if you want the cursor keys to send their application control function.
2. In the Terminal Keys box, choose Numeric if you want the terminal number keys to send their numbers.
Choose Application if you want the terminal number keys to send their programming functions.
3. Check or clear the text to automatically wrap to the next line when it reaches the right margin.
If line wrap is cleared, 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.
4. In the Controls box, choose 7-bit if you want the terminal to use all the VT320 features. This mode also supports 8-bit graphic display characters and 7-bit control characters. Choose this setting for all VT220 applications.
Choose 8-bit if you want the terminal to use all the VT320 features in an 8-bit environment with 8-bit control characters. Choose this setting for VT220 applications that use 8-bit control characters.
5. In the User-Defined Key box, choose Lock if you do not want the host to change the user-defined key definitions.
Choose Unlock if you want the host to be able to add or to change the user-defined key definitions.
6. Check the Save as new defaults check box if you want to use the current custom terminal configuration as the default for all other terminals of the same type.
7. Choose OK to save your changes and to return to the main menu.



Configuring a 5250 Terminal Session

The screenshot shows a dialog box titled "Terminal Session Definition" with a close button in the top-left corner. The main text inside the dialog reads "Enter the terminal session parameters." Below this, there are several input fields and controls:

- Session... Name:** A text input field.
- Session type:** A text input field containing the value "5250".
- Host Name:** A dropdown menu with a small downward arrow on the right. Below it is an "Add..." button.
- Mode name:** A dropdown menu containing the value "#INTER".
- Host user ID:** A text input field.
- Password:** A text input field with a "Show" checkbox to its right.
- Number of sessions:** A text input field with "[1-15]" to its right.

At the bottom of the dialog, there are three buttons: "OK", "Cancel", and "Help".

Fast Setup Quick Reference Guide

Field	Description	Value	Default
Name	A meaningful name for this terminal session.	1 to 8 alphanumeric characters	None
Host Name	The name of the SNA host to which the terminal session connects.	Predefined	None
Mode name	This name describes the class of service and other session characteristics that you may want for your network.	Predefined	#INTER
Host user ID	The user ID that lets you log into the remote host.	1 to 10 alphanumeric characters	None
Password	The password that goes with the user ID that lets you log into the remote host.	1 to 10 alphanumeric characters	None
Show	Determines if your password appears in the field as you enter it. Clear this check box to show asterisks for each character you type instead of the actual characters.	Check, Clear	Clear
Number of sessions	The number of terminal sessions you want to configure to this host.	15	1



To configure a 5250 terminal session

1. Choose 5250. The Terminal Session Definition dialog box appears.
2. In the Session box, enter a meaningful name for the session.
3. In the Host Name box, click the down arrow on the right side of the field. A list that contains existing host names appears. Select the host that you want to connect with for this session. For help, see “Adding an IBM SNA Host” earlier in this document.
4. In the Mode name field, click the down arrow on the right side of the field. A list of communication modes appears. Select the mode that you want to use to communicate with your SNA host.
5. In the Host user ID field, enter the ID that allows you to log in to the AS/400. In the Password field, enter the password that goes with your user ID that allows you to log into the AS/400.

Enable the Show check box to show asterisks instead of the characters you are typing.

Disable the Show check box to show the characters that you are typing in the field.
6. In the Number of sessions field, enter the number of terminal sessions you want to run on the controller. You can enter up to 15 sessions.
7. Choose OK to save your changes and return to the main menu.

Configuring a 3270 Terminal Session

Field	Description	Value	Default
Name	A meaningful name for this terminal session.	1 to 8 alphanumeric characters	None
Host Name	The name of the SNA host to which the terminal session connects.	Predefined	None
Number of sessions	The number of terminal sessions you want to configure to this host.	See table in Step 4	1
NAU address	The network addressable unit (NAU) that is specified for the workstation LU name.	1 to 254	None



To configure a 3270 terminal session

1. Choose 3270. The Terminal Session Definition dialog box appears.
2. In the Session box, enter a meaningful name for the session.
3. In the Host Name box, click the down arrow on the right side of the field. A list that contains existing host names appears. Select the host that you want to connect with for this session. For help, see “Adding an IBM SNA Host” earlier in this document.
4. In the Number of sessions field, enter the number of terminal sessions you want to run on the controller.

Session Type	Coaxial	Non-Coaxial
3270	5	26

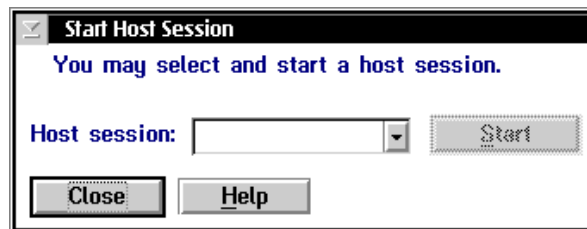
5. (non-coaxial only) In the NAU address field, enter the NAU address that is specified for the workstation LU name.
6. Choose OK to save your changes and return to the main menu.

Starting a Host Session

Once you have set up your terminal sessions on the controller, you can start the host session from the controller.

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 Sessions 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 one 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.

Verify Your Host Connection

Once you configure the network adapter cards and your host connection, you may want to use the Send Transactions feature to verify that you have a connection between the Model 200 Controller and your host. For help, see “Verifying Your Data Collection Environment” earlier in this quick reference guide.

When sending a transaction to your host application (destination), make sure that your application is ready to accept the transaction. If your application is not ready, the transaction is written to the Hot Standby file. If the application does not know how to interact with the Hot Standby file, subsequent transactions will also be written to the Hot Standby file. In this case, clear the Hot Standby file before sending another transaction to the application. For help, see “Viewing and Clearing the Hot Standby Files” in Appendix A in the *Model 200 Controller User’s Manual*.

Before you verify your host connection, make sure you activate your current configuration and start data collection.

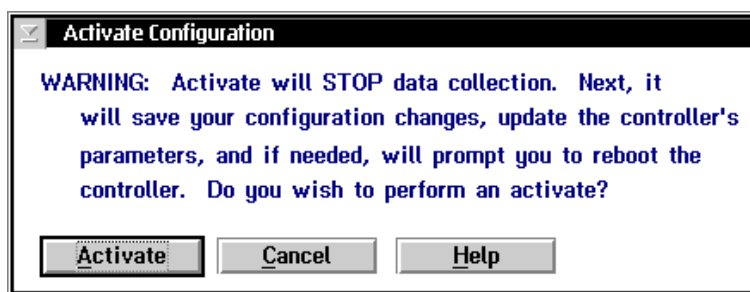
Step 8 - Start the Controller

Before you start the Model 200 Controller, make sure you have performed these tasks:

1. Connected and configured all external Intermecc controllers and devices.
2. Connected the Model 200 Controller to the host and the data collection network.
3. Used Fast Setup to configure the data collection environment.
4. Used Fast Setup to configure the host communications environment.
5. Used Fast Setup to configure terminal emulation, peer-to-peer applications, or terminal sessions.

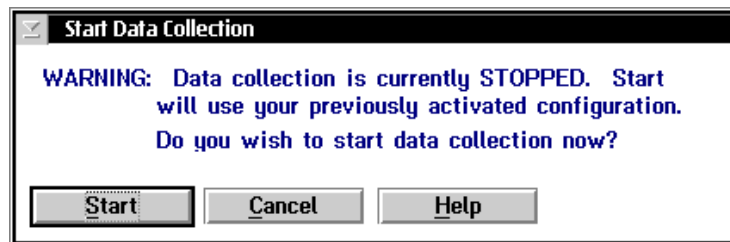
To start the controller

1. From the main menu sidebar buttons, choose Save and Activate Configuration. A message box appears confirming that you want to save your changes and activate the configuration.



2. Choose Activate. You may be asked to shutdown the controller and press **Ctrl-Alt-Del** to boot it. If not, a message box appears informing you when your activate is successful.

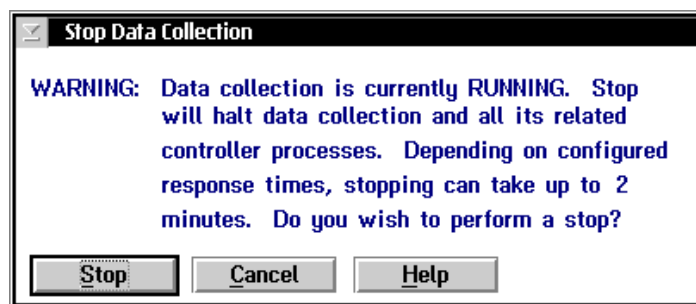
3. From the main menu on the controller, choose Start Data Collection. A message box appears confirming that you want to start data collection.



4. Choose Start.
5. Start the applications on the host.
6. Start the applications on the devices.

To stop the controller

1. From the main menu sidebar buttons, choose Stop Data Collection. A message box appears confirming that you want to stop data collection.



2. Choose Stop. When the controller is done stopping data collection, the main menu appears.

Where Do You Go From Here?

Now that your controller is installed in your network, you can perform terminal emulation or send transactions from your Intermec data collection devices to your host. If you need to perform Advanced Setup to edit or delete some of the parameters, or if you need to configure screen mapping, see the *Model 200 Controller User's Manual*.



Index

Numbers

- 2.4 GHz RF network, 5, 7. *See also* UDP Plus network. *See also* UDP Plus network
- 3270 NAU Pool dialog box, 45
 - New NAU field, 46
 - Unlinked NAUs pool, 46
- 3270 screen mapping, *See* 3270 terminal sessions
- 3270 SNA terminal emulation
 - setting up, 30, 41
- 3270 Terminal Emulation Configuration dialog box, 42
 - Available Terminals list box, 42
 - Edit Link button, 46
 - Host Name - Linked Terminal - NAU list box, 42
 - Host Name list box, 42
 - NAU Pool button, 45
- 3270 Terminal Emulation Worksheet, 41
- 3270 terminal sessions, 5
 - setting up, 30, 53, 62
 - starting, 64
- 5250 screen mapping, *See* 5250 terminal sessions
- 5250 SNA terminal emulation
 - setting up, 30, 36
- 5250 Terminal Emulation Configuration dialog box, 37
 - Available Terminals list box, 37
 - Host Name - Linked Terminals list box, 37
 - Host Name list box, 37
 - Use device names check box, 37
- 5250 Terminal Emulation Worksheet, 36
- 5250 terminal sessions, 5
 - setting up, 30, 53, 59
 - starting, 64
- 900 MHz RF network, 5, 7

A

- access points, 16
- accessories
 - keyboard, 8, 9
 - monitor, 8, 9
 - mouse, 8, 9
 - power cord, 9
 - power supply, 8

- activating your configuration, 12
- Adapter card field, 39, 44
- adapter cards, *See* local network adapter
- adding a TCP/IP host, 34
- adding a transaction, 50
- adding an IBM SNA host, 39, 44
- adding transaction fields, 52
- Address field, 39, 44
- ANSI screen mapping, *See* VT/ANSI terminal sessions
- ANSI terminal emulation, *See* Telnet terminal emulation
- APPC applications
 - setting up, 30
- Auto-Start box, 14
- Available Connections list box, 17
- Available list box, 48
- Available Terminals list box, 32, 37, 42

B

- Bad ID response field, 14
- BRU, 16

C

- cards, *See* local network adapter
- checklist box, 12
- coaxial adapter card, configuring, 27
- COM ports, *See* serial ports
- communications environment, *See* host communications environment
- Configure button, 16
- Configured Connections list box, 17
- configuring a 3270 terminal session, 62
- configuring a 5250 terminal session, 59
- configuring a UDP Plus network, 19
- configuring a VT/ANSI terminal session, 54
- configuring an RF card, 18
- configuring external Intermec controllers, 21
- configuring the host environment parameters, 30
- configuring the local network adapter cards, 24
- connecting to your data collection network, 10
- connecting to your host environment, 10
- Controller address field, 28

Fast Setup Quick Reference Guide

controllers, configuring external Intermecc, 16, 21
Controls option buttons, 57
CrossBar network, 7
Current NAU field, 46
Cursor keys option buttons, 57
customizing the VT terminal setup, 56

D

data collection
 starting, 66
 stopping, 67
data collection network
 configuring, 16
 connecting to, 10
 figure, 7
 verifying connection, 21
Data field, 22
Data or system field, 22
Delimiter field, 51
delivery response messages, 47
Destination ID field, 22
Destination name field, 48

E

Edit Link button, 46
Edit NAU Address dialog box, 46
 Current NAU field, 46
editing a link, 46
environment parameters, *See* host environment parameters
Ethernet adapter card
 configuring, 25
 default setting, 25
Ethernet TCP/IP Adapter Configuration dialog box, 25
 Ethernet TCP/IP card field, 26
 Local host name field, 26
 Local IP address field, 26
 Subnet mask field, 26
 Use DHCP check box, 26
Ethernet TCP/IP card field, 26
explicit links
 editing an NAU, 46
 setting up, 31, 36, 41

external Intermecc controllers, 16
 configuring, 21

F

Fast Setup for Downline Network dialog box, 17
 Available Connections list box, 17
 Configured Connections list box, 17
 Multi-Drop and RF field, 18
 Network ID field, 18
 Point-to-Point field, 18
 RF channel field, 18
 Serial port field, 18
Fast Setup for Intermecc Hardware dialog box, 16
 Configure button, 16
Fast Setup toolbar button, 11
Field name field, 52
File Transfer Time box, 14
filling the NAU pool, 45

H

help, using, 6
Hide at Boot Time button, 11
host
 adding, 34
 adding an IBM SNA host, 39, 44
 types of, 5
 verifying your connection, 65
host communications environment, setting up, 24
Host Connection Configuration dialog box, 39, 44
 Adapter card field, 39, 44
 Address field, 39, 44
 Host LU field, 39
 Host name field, 39, 44
 Local PU field, 39, 44
 Network ID field, 39
 Node ID field, 44
Host Connections step, 12
host environment parameters, configuring, 30
host environment, connecting to, 10
Host LU field, 39

Host Name - Linked Terminal - NAU list box, 42
 Host Name - Linked Terminals list box, 32, 37
 Host Name box, 54, 60, 62
 Host name field, 34, 39, 44
 Host Name list box, 32, 37, 42
 Host session field, 64
 Host user ID field, 60
 Hot standby field, 48
 Hot Standby message field, 51
 Hot Standby timeout, 47
 Hot Standby timeout field, 48

I

IBM host, using with Telnet terminal emulation, 31
 IBM SNA host, adding, 39, 44
 ID delimiter field, 14
 installing the controller, 10
 Interactive response field, 48
 Intermec Hardware step, 12
 International text pass-through check box, 48
 introduction to Fast Setup, 5
 IP address field, 34

J

JANUS devices
 using with 3270 SNA terminal emulation, 41
 using with 5250 SNA terminal emulation, 36
 using with Telnet terminal emulation, 31

K

keyboard, 8, 9
 Keypad option buttons, 57

L

Line wrap enabled check box, 57
 links, *See* explicit links
 Local host name field, 26
 Local IP address, 26
 local network adapter
 coaxial adapter card, 27
 configuring, 24
 downline cards, 5

Ethernet adapter card, 25
 SDLC adapter card, 29
 token ring adapter card, 27
 twinaxial adapter card, 28
 upline cards, 5
 Local Network Adapters step, 12
 Local PU field, 39, 44
 Local station field, 29

M

main menu, 11, 12
 checklist box, 12
 sidebar buttons, 12
 title bar, 12
 toolbar buttons, 12
 Max connections field, 14
 Mode name field, 60
 Model 200 Controller to 9180 and CrossBar Worksheet, 16
 Model 200 Controller to 9180 Worksheet, 16
 Model 200 Controller to CrossBar Worksheet, 16
 Model 200 Controller to RF Card Worksheet, 16
 Model 200 Controller to TRAKKER Antares Terminals Worksheet, 16
 monitor, 8, 9
 mouse, 8, 9
 Multi-Drop and RF field, 18

N

Name field, 54, 60, 62
 NAU address field, 62
 NAU Pool button, 45
 NAU pool, filling, 45
 network adapter cards, *See* local network adapter
 Network Adapter Cards Worksheet
 using with the Ethernet card, 25
 using with the SDLC card, 29
 using with the twinaxial card, 28
 Network ID field, 18, 39
 New NAU field, 46
 Node ID field, 44
 Number field, 52
 Number of sessions field, 54, 60, 62
 Number to enable field, 19, 20

Fast Setup Quick Reference Guide

O

online help, using, 6

P

parameters

- setting host environment, 30
- setting system, 13

Password field, 60

peer-to-peer applications

- setting up, 30
- setting up links, 47

Peer-to-Peer Destination Parameters dialog box, 47

- Available list box, 48
- Destination name field, 48
- Hot standby field, 48
- Hot Standby timeout field, 48
- Interactive response field, 48
- International text pass-through check box, 48
- Selected list box, 48
- Transactions held in volatile memory field, 48

Peer-to-Peer Network Connection Parameters box, 15

Point-to-Point field, 18

Port number field, 54

power button, 11

power cord, 9

powering on the controller, 11

R

rear panel, figure, 8

Resolve button, 35

RF card, configuring, 18

RF channel field, 18

RF controller card, 16

RFNC address field, 18

S

Save and Activate sidebar button, 66

Save as new defaults check box, 57

saving your configuration, 12

screen mapping, 5, 53

SDLC adapter card

configuring, 29

default setting, 29

SDLC Adapter Configuration dialog box, 29

Local station field, 29

Selected list box, 48

Send Transaction dialog box, 22

Data field, 22

Data or System field, 22

Destination ID field, 22

Source ID field, 22

Transaction ID field, 22

Serial port field, 18

serial ports, 6

setting the system parameters, 13

setting up 3270 SNA terminal emulation, 41

setting up 5250 SNA terminal emulation, 36

setting up a terminal session, 53

setting up peer-to-peer links, 47

setting up Telnet terminal emulation, 31

setting up the controller, 8

setting up the data collection environment, 16

setting up the host communications environment, 24

Setup for UDP Plus Terminals dialog box, 19, 20

Number to enable field, 19, 20

Starting IP address field, 20

Show at Boot Time button, 11

Show check box, 60

sidebar buttons, 12

Save and Activate, 66

Start Data Collection, 67

Stop Data Collection, 67

System Parameters dialog box, 13

SNA host

setting up explicit links with terminals, 36, 41

using with 3270 terminal emulation, 41

using with 5250 terminal emulation, 36

Source ID field, 22

Start button, 64

Start Data Collection sidebar button, 67

Start Host Session dialog box, 64

Host session field, 64

Start button, 64

Start Host Sessions, 64

starting a host session, 64

- starting data collection, 66
 - Starting IP address field, 20
 - steps, configuring controller
 - Host Connections, 12
 - Intermec Hardware, 12
 - Local Network Adapters, 12
 - Stop Data Collection sidebar button, 67
 - stopping data collection, 67
 - Strip pad field, 14
 - Subnet mask, 26
 - System Maintenance sidebar button
 - Send Transactions, 22
 - Start Host Sessions, 64
 - System Parameters dialog box
 - Auto-Start box, 14
 - Bad ID response field, 14
 - File Transfer Time box, 14
 - ID delimiter field, 14
 - Max connections field, 14
 - Peer-to-Peer Network Connection Parameters box, 15
 - Terminal Emulation Setup Screens box, 14
 - Time Synchronization box, 14
 - system parameters, setting, 13
- T**
- TCP/IP applications, setting up, 30
 - TCP/IP host
 - adding, 34
 - setting up explicit links with terminals, 31
 - using with Telnet terminal emulation, 31
 - TCP/IP Host Connection dialog box, 34
 - Host name field, 34
 - IP address field, 34
 - Resolve button, 35
 - Use DNS check box, 34
 - Telnet terminal emulation
 - setting up, 30, 31
 - Telnet Terminal Emulation Configuration dialog box, 32
 - Available Terminals list box, 32
 - Host Name - Linked Terminals list box, 32
 - Host Name list box, 32
 - Telnet Terminal Emulation Worksheet, 31
 - terminal emulation, *See also* 3270 SNA terminal emulation. *See also* 5250 SNA terminal emulation. *See also* Telnet terminal emulation
 - loading software, 31
 - Terminal Emulation Setup Screens box, 14
 - terminal license, 31, 36, 41
 - Terminal mode field, 54
 - Terminal Session Definition dialog box, 54, 59, 62
 - Host Name box, 54, 60, 62
 - Host user ID field, 60
 - Mode name field, 60
 - Name field, 54, 60, 62
 - NAU address field, 62
 - Number of sessions field, 54, 60, 62
 - Password field, 60
 - Port number field, 54
 - Show check box, 60
 - Terminal mode field, 54
 - terminal sessions, *See* VT/ANSI terminal sessions. *See* 3270 terminal sessions. *See* 5250 terminal sessions
 - terminals, setting up explicit links with hosts, 31, 36, 41
 - Time Synchronization box, 14
 - title bar, 12
 - TN3270 terminal emulation, *See* Telnet terminal emulation
 - TN5250 terminal emulation, *See* Telnet terminal emulation
 - token ring adapter card
 - configuring, 27
 - default setting, 27
 - toolbar buttons, 12
 - TRAKKER Antares terminals, 16
 - using with 3270 SNA terminal emulation, 41
 - using with 5250 SNA terminal emulation, 36
 - using with VT/ANSI terminal emulation, 31
 - Transaction Field Parameters dialog box, 52
 - Field name field, 52
 - Number field, 52
 - transaction fields, adding, 52
 - Transaction ID field, 22, 51

Fast Setup Quick Reference Guide

- Transaction Parameters dialog box, 50
 - Delimiter field, 51
 - Hot Standby message field, 51
 - Transaction ID field, 51
- Transactions held in volatile memory field, 48
- transactions, adding, 50
- turning on the controller, 11
- twinaxial adapter card, configuring, 28
- Twinaxial Protocol Configuration dialog box, 28
 - Controller address field, 28

U

- UDP Plus network, 16
 - configuring, 19
- Unlinked NAUs pool, 46
- Use device names check box, 37
- Use DHCP check box, 26
- Use DNS check box, 34
- User-Defined Key option buttons, 57

V

- verifying your data collection environment, 21
- verifying your host connection, 65
- voltage select switch, 9
- VT screen mapping, *See* VT/ANSI terminal sessions
- VT Setup dialog box, 56
 - Controls option buttons, 57
 - Cursor keys option buttons, 57
 - Keypad option buttons, 57
 - Line wrap enabled check box, 57
 - Save as new defaults check box, 57
 - User-Defined Key option buttons, 57
- VT terminal emulation, *See* Telnet terminal emulation
- VT terminal, customizing the setup, 56
- VT/ANSI terminal sessions, 5
 - configuring, 54
 - setting up, 30, 53
 - starting, 64

W

- warranty, 2
- worksheets, 8

User's Manual

Model 200 Controller

 **ntermec**

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.

The information contained herein is proprietary and is provided solely for the purpose of allowing customers to operate and/or service Intermec manufactured equipment and is not to be released, reproduced, or used for any other purpose without written permission of Intermec.

Information and specifications in this manual are subject to change without notice.

© 1998 by Intermec Technologies Corporation
All Rights Reserved

The word Intermec, the Intermec logo, JANUS, IRL, TRAKKER, Antares, Adara, Duratherm, EZBuilder, Precision Print, PrintSet, Virtual Wedge, and CrossBar are either trademarks or registered trademarks of Intermec Corporation.

Throughout this manual, trademarked names may be used. Rather than put a trademark (™ or ®) symbol in every occurrence of a trademarked name, we state that we are using the names only in an editorial fashion, and to the benefit of the trademark owner, with no intention of infringement.

Contents

Before You Begin xvii
 Warranty Information xvii
 Safety Summary xvii
 Warnings and Cautions xviii
 About This Manual xix
 Other Intermec Manuals xxii

1

Learning About the Controller

Chapter Checklist 1-3

Features 1-4

What's New for Release 3.1? 1-5

Unpacking the Controller 1-7

Description 1-9

Understanding the Front Panel 1-9

Understanding the Rear Panel 1-10

About the Graphical User Interface 1-11

Using Help 1-12

Navigating Through Dialog Boxes 1-13

Understanding the Dialog Box Buttons 1-14

How the Controller Works 1-15

About Transactions 1-17

Data Transactions 1-17

System Transactions 1-17

How the Controller Routes Transactions 1-18

Routing Transactions From Applications 1-18

Routing Transactions From Devices 1-21

Model 200 Controller User's Manual

How the Controller Acknowledges Transactions 1-25

How the Controller Ensures Data Integrity 1-25

Interactivity With Data Collection Devices 1-25

Fully Interactive System 1-26

Partially Interactive System 1-27

Noninteractive System 1-27

Data Integrity Modes 1-28

Faster Mode 1-28

Safer Mode 1-28

Retaining Transactions in Memory 1-29

How the Controller Sets Application Status 1-30

Active Applications 1-31

Nonactive Applications 1-31

Sending Hot Standby Messages 1-32

Changing from Nonactive to Active Status 1-33

Active Recovery Mode 1-33

2

Setting Up the Controller

Chapter Checklist 2-3

Plugging In the Power Cord 2-4

Plugging In the Keyboard 2-5

Plugging In the Mouse 2-6

Connecting the Monitor 2-7

Connecting an Uninterruptable Power Supply 2-8

Connecting a Modem 2-11

Setting the System Parameters 2-14

About the Configuration Files 2-17

Restoring Default Configuration 2-17

Backing Up the Controller Configuration 2-18

Backing Up Your System Files and Run-Time Configuration 2-18

Backing Up Your User Files 2-19

Restoring the Controller Configuration 2-20

Restoring Your System Files and Run-Time Configuration 2-20

Restoring Your User Files 2-21

Deleting User Files 2-23

Using the Controller 2-24

Starting Data Collection 2-24

Stopping Data Collection 2-25

Turning Off the Controller 2-25

Accessing a Command Prompt 2-26

3

Connecting to the Intermec RF Network

Chapter Checklist 3-3

Connecting the Controller to the 900 MHz RF Network 3-4

Configuring RF Controller Cards 3-6

Adding RF Controller Card and BRUs 3-7

Setting the Time Parameters 3-11

Identifying the RF Devices 3-15

Editing an RF Device 3-17

Connecting the Controller to the 2.4 GHz RF Network 3-19

Configuring a UDP Plus Network 3-21

Adding a UDP Plus Network 3-22

Setting Up the UDP Plus Devices 3-25

Setting the Time Parameters 3-28

Identifying the UDP Plus Devices 3-31

Editing a UDP Plus Device 3-33
Determining a UDP Plus Device's IP Address 3-36
Editing a UDP Plus Device's IP Address 3-37

Saving Your Run-Time Configuration 3-37

4

Connecting to the 9180 and the Intermec CrossBar Network

Chapter Checklist 4-3

Configuring an External Intermec Controller 4-4

Adding a Controller 4-5
About the Controller Parameters 4-6
Adding a 9154 Controller 4-7
Adding a 9161 Controller 4-10
Adding a 9180 Controller 4-13
Setting the Time Parameters 4-15

Identifying the CrossBar Devices 4-19

Editing a CrossBar Device 4-21

Saving Your Run-Time Configuration 4-23

5

Connecting to an Ethernet/Token Ring Network

Chapter Checklist 5-3

Installing the Controller in an Ethernet Network 5-4

Installing the Controller in a Token Ring Network 5-5

Configuring the Network Adapter Card for TCP/IP 5-6

Using DNS 5-10

Clearing the IP Address and Subnet Mask 5-12

Using the Routing Daemon 5-12

Configuring Routing Tables 5-14

Configuring the Network Adapter Card for IEEE 802.2 5-16

Saving Your Run-Time Configuration 5-19

6

Connecting to a Coaxial/Twinaxial Network

Chapter Checklist 6-3

Installing the Controller 6-4

Configuring the Coaxial Adapter Card 6-5

Configuring the Twinaxial Adapter Card 6-6

Saving Your Run-Time Configuration 6-7

7

Connecting to an SDLC Network

Chapter Checklist 7-3

Installing the Controller 7-4

Configuring the Network Adapter Card 7-5

Configuring Advanced SDLC Parameters 7-6

Saving Your Run-Time Configuration 7-8

8

Using Terminal Emulation

Chapter Checklist 8-3

About Terminal Emulation 8-5

JANUS TE Application 8-6

TRAKKER Antares TE Application 8-7

Setting Up Telnet Terminal Emulation 8-7

Configuring the Controller 8-7

Adding a TCP/IP Host 8-10

Setting Up 5250 SNA Terminal Emulation 8-12

Configuring the Host 8-12

Configuring the Controller 8-12

Adding an IBM SNA Host 8-15

Configuring the Controller SNA Node 8-17

Selecting an IBM Mode 8-18

Setting and Removing the User ID and Password 8-19

Performing a Double Pass-Through on the IBM AS/400 Host 8-21

Setting Up 3270 SNA Terminal Emulation 8-22

Configuring the Host 8-22

Configuring the Controller 8-22

Adding an IBM SNA Host 8-25

Filling the NAU Pool 8-28

Editing a Link 8-29

Saving and Activating Your Run-Time Configuration 8-29

Configuring Your JANUS Devices 8-30

Configuring for 900 MHz RF Communications 8-30

Configuring for UDP Plus Communications 8-31

Downloading the JANUS TE Application 8-31

Using the Download Server to Download the JANUS TE Application 8-33

Using FTP to Load the JANUS TE Application 8-34

Accessing the TE Configuration Menu 8-35

Exiting the TE Configuration Menu 8-36

Starting TE 8-36

Ending TE 8-37

About Running TE 8-37

About the Auto-Login Feature 8-38

Displaying International Characters 8-39

Configuring Your TRAKKER Antares Terminals 8-40

Configuring for Communications 8-40

Downloading the TRAKKER Antares TE Application 8-41

Accessing the TE Configuration Menu 8-43

Exiting the TE Configuration Menu 8-44

About Running TE on Your Terminals 8-45

About the Auto-Login Feature 8-45

Displaying International Characters 8-45

Setting Security for the TE Configuration Menu 8-46

Verifying That Security Is Set 8-49

9

Using Peer-to-Peer Applications

Chapter Checklist 9-3

About Peer-to-Peer Applications 9-4

Configuring the Host for Peer-to-Peer Applications 9-5

TCP/IP Applications 9-5

APPC Applications 9-5

Setting Up Peer-to-Peer Links on the Controller 9-6

Adding a Destination 9-8

Using International Text Pass-Through 9-11

Adding a Transaction 9-13

Adding a Transaction Field 9-14

Saving and Activating Your Run-Time Configuration 9-15

Communicating With TCP/IP Applications 9-16

How the Controller Communicates With Applications 9-18

Understanding Transaction Routing in a TCP/IP Network 9-20

Communicating Through the Direct TCP/IP Socket Interface 9-23

Direct TCP/IP API vs. NetComm API 9-25

About the \$IPT Transaction ID 9-26

About the Host Application Requirements 9-26

Using International Text Pass-Through 9-27

Communicating With APPC Applications 9-28

APPC Verbs 9-29

IMS Applications 9-30

NetComm Pairs 9-30

10

Using Terminal Sessions

Chapter Checklist 10-3

About Terminal Sessions 10-4

Configuring the Host for Terminal Sessions 10-5

Setting Up 5250 Terminal Sessions Using SDLC 10-5

Setting Up 3270 Terminal Sessions Using Ethernet 10-5

Setting Up 3270 Terminal Sessions Using SDLC 10-6

Creating Terminal Sessions 10-6

Adding a VT/ANSI Terminal Session 10-8

Adding a TCP/IP Host 10-10

Customizing the VT Terminal Setup 10-12

Adding a 5250 Terminal Session 10-15

Adding an IBM SNA Host 10-18

Configuring the Controller SNA Node 10-20

Adding a 3270 Terminal Session 10-21

Adding an IBM SNA Host 10-23

Saving and Activating Your Run-Time Configuration 10-25

Starting a Host Session 10-26

Mapping Terminal Keyboards to the Model 200 Controller Keyboard 10-27

11

Using Screen Mapping

Chapter Checklist 11-3

About Screen Mapping 11-5

About Script Files 11-7

Preparing to Use the Script Builder Tool 11-7

Single Transaction Script Files vs. Multiple Transaction Script Files 11-8

Identifying Key Elements for the Script File 11-10

Example 1 - Single Transaction Script File 11-10

Example 2 - Multiple Transaction Script File 11-12

Understanding How the Script Builder Tool Flows 11-14

Using the Script Builder Tool 11-16

Creating a New Script File 11-17

Opening an Existing Script File 11-18

Saving the Script File 11-18

Copying a Script File 11-19

Deleting a Script File 11-21

Setting Options for the Script File 11-22

About the Data Response Timeout (VT/ANSI) 11-25

Creating Host Access Sequences 11-26

Creating a Logon Sequence 11-27

Creating a Normal Logoff Sequence 11-29

Creating an Abnormal Logoff Sequence 11-31

Editing the Captured Keystrokes 11-33

Deleting Lines in the Captured Keystrokes Box 11-33

Changing Lines in the Captured Keystrokes Box 11-33

Inserting New Lines in the Captured Keystrokes Box 11-33

Selecting Transactions for the Script 11-34

Selecting Host Screens for the Current Transaction 11-36

- Defining Next Screen Sequences for Host Screens 11-37*
- Selecting Host Screen Fields for the Current Host Screen 11-39*
 - Adding a Host Screen Field 11-40*
 - Getting Host Screen Field Attributes From a Host Screen 11-42*
- Selecting Regions for the Current Host Screen 11-43*
 - Adding a Region 11-44*
 - Getting a Region From a Host Screen 11-49*
 - Capturing Keystrokes 11-50*
 - Defining Next Host Screen Sequences for Regions 11-51*
- Creating Screen and Region Messages 11-53*
 - Adding a Message 11-55*
 - About Message Types (Status vs. Transaction) 11-57*
- Changing the Order of Screen Events 11-59*
- Maintaining the Host Screens 11-61*
 - Adding a Host Screen 11-63*
 - Getting the Screen Identifier From the Host Screen 11-64*

Defining User Blocks 11-65

- Adding a User Block 11-68*

Viewing the Script 11-69

Checking a Script File 11-70

- Verifying the Script File Syntax 11-70*
- Verifying the Script File Logic 11-71*

Setting Up Screen Mapping Sessions 11-76

- Adding a Screen Mapping Session 11-77*
- Mapping Transaction Fields 11-80*
 - Adding a Screen Mapping Field Placement Entry 11-82*

Saving and Activating Your Run-Time Configuration 11-83

Building Terminal Screens for Data Collection Devices 11-83

Adding a Terminal Screen 11-87

Adding a Terminal Field 11-89

Validating a Terminal Field 11-93

Getting Terminal Field Attributes From a Host Screen 11-95

Getting Terminal Field Attributes From the Script File 11-96

Defining Next Screen Sequence for Terminal Screens 11-97

Copying a Terminal Screen 11-99

Building Menus From Screens 11-100

Adding a Menu 11-101

Generating Menus Into Templates 11-102

Saving and Activating Your Run-Time Configuration 11-103

Script Builder Tool Limitations 11-103

VT/ANSI Screen Mapping Limitations 11-105

VT Keyboard Mapping and Script Keystroke Names 11-106

Keystrokes 11-108

Configuring Your JANUS Devices 11-109

Configuring Communications 11-109

Configuring for 900 MHz RF Communications 11-109

Configuring for UDP Plus Communications 11-109

Downloading the Terminal Template Application 11-110

Downloading the Template 11-113

Loading a Validation File 11-116

Running the Application 11-117

Configuring Your TRAKKER Antares Terminals 11-118

Configuring the Terminals for the First Time 11-118

Downloading the Template 11-119

Loading a Validation File 11-122

Running the Application 11-123

A

Troubleshooting

General Troubleshooting A-3

Using the System Reporting Tools A-5

Viewing the Configuration A-5

Viewing and Clearing the Hot Standby Files A-7

Message Box Error Messages A-9

Error Log Error Messages A-26

Viewing the Error Messages A-26

Using the Status Monitor A-26

Using the Error Log A-28

Understanding the Error Messages A-29

Using the System Diagnostics Tools A-59

Using the Message Log Formatter A-60

Using SNA Subsystem Management A-61

Using the Trace Utility A-62

Adding a Network Trace A-64

Adding a Screen Mapping Trace A-65

Adding a System Trace A-66

Understanding the Monitor Message Handler Transactions Dialog Box A-67

B

Helpful Information

System Cabling Specifications B-3

Converting Ethernet Addresses to Token Ring MAC Format B-5

Using the Controller to Verify Your Network Connections B-7

Sending Transactions B-7

Receiving Transactions B-9

Using the Controller to Transfer Files B-11

Limitations when Downloading IRL Programs B-12

Adding a Group in the Download Server B-13

Copying Information Between Terminals or Groups B-15

Using the Download Server to Transfer Files B-16

Using Download Server Commands to Transfer Files B-18

Using the Controller to Configure TRAKKER Antares Terminals B-20

C

Using Remote Console

About Remote Console C-3

Configuring the NetOp Host (Model 200 Controller) C-3

Configuring for TCP/IP or Dial-Up SLIP C-4

Configuring for APPC C-6

Configuring Security C-8

Configuring the NetOp Guest (Remote PC) C-11

Using NetOp Guest for Windows C-11

Using NetOp Guest for OS/2 C-13

D

Upgrading Your Controller and Devices

Upgrading Your Licenses D-3

Upgrading Your Terminal License D-3

Upgrading to Screen Mapping D-4

Upgrading to Remote Console D-5

Using the Controller to Upgrade TRAKKER Antares Terminals D-6

Adding Upgrade Events D-8

Loading Firmware and Applications From a Disk D-12

Defining a Group D-14

Renaming a Group D-16

Performing the Upgrade D-16

Model 200 Controller User's Manual

Managing System Firmware and Applications D-17

Viewing Upgrade Event Details D-18

Viewing the Event Log D-20



Worksheets



Glossary



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 manipulant 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 Model 200 Controller is in this manual. Information in this manual should be used by the person who will be installing and configuring the controller. Many of the parameters need to be set by the network administrator. This manual assumes that you are familiar with your network and data communications.

Terms

- The Model 200 Controller is usually referred to as “the controller.”
- “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, respectively, 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 the UDP Plus protocol, instead of TCP/IP.
- “Data collection devices” and “devices” refers to the JANUS devices, TRAKKER Antares terminals, and other devices that communicate through the Model 200 Controller.

Conventions

This manual uses these conventions to explain how to use your mouse and to emphasize input from a PC keyboard, a data collection 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.

Model 200 Controller User's Manual


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 Data Collection Device Keypad

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

Input From a Bar Code

You can use your data collection 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.

Change Configuration ——— *Name*
 ——— *Bar code (Code 39)*
* \$ + * ——— *Human-readable interpretation*

200.103

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 *BVdata* 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 Model 200 Controller 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.

This list contains only some of the manuals for Intermec's more recent products that can communicate through the controller.

Manual	Intermec Part No.
<i>DCS 300 Technical Reference Manual</i>	067717
<i>Data Communications Reference Manual</i>	044737
Intermec 900 MHz Products	
<i>RF System/9180 Controller User's Manual</i>	054292
<i>900 MHz RF Equipment User's Manual</i>	066163
<i>900 MHz RF Gateway User's Manual</i>	066164
<i>JANUS 2010 Hand-Held Computer User's Manual (4MB)</i>	065714
<i>JANUS 2020 Hand-Held Computer User's Manual (4MB)</i>	065715
<i>JANUS 2050 Vehicle Mount Computer User's Manual (4MB)</i>	065716
Intermec 2.4 GHz Products	
<i>0110/0111/0115 Access Point User's Manual</i>	065053
<i>2100 Universal Access Point User's Manual</i>	067150
<i>TRAKKER Antares 2420 and 2425 Hand-Held Terminal User's Manual</i>	064024
<i>TRAKKER Antares 248X Stationary Terminal User's Manual</i>	066960
<i>TRAKKER Antares Terminal Emulation User's Guide</i>	066694
<i>JANUS 2020 Hand-Held Computer User's Manual (4MB)</i>	065715
<i>JANUS 2050 Vehicle Mount Computer User's Manual (4MB)</i>	065716
<i>JANUS 2.4 GHz Installation Utility Kit for 4MB Devices</i>	064672

Before You Begin



Other Intermec Manuals (continued)

Manual	Intermec Part No.
Intermec CrossBar Products	
<i>9154 Multi-Drop Line Controller System Manual</i>	048517
<i>9160A Installation Manual</i>	044170
<i>9161A Operator Guide</i>	046070
<i>9161B Programmer/Operator Guide</i>	049574
<i>9161B Installation Manual</i>	049572

1

Learning About the Controller

This chapter helps you learn about the features of the Model 200 Controller and how the controller works with your LAN and Intermec's data collection network.

Chapter Checklist

Done?	Task	Page
<input type="checkbox"/>	Understand the features of your Model 200 Controller.	1-4
<input type="checkbox"/>	Unpack the controller.	1-7
<input type="checkbox"/>	Identify the components on the front and rear panels.	1-9
<input type="checkbox"/>	Understand the main menu, online help, how to navigate through dialog boxes, and the most common buttons in the graphical user interface (GUI).	1-11
<input type="checkbox"/>	Understand how the controller works and how transactions are routed in your data collection network.	1-15

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

Features

The Model 200 Controller is a network controller that connects Intermec's wired and wireless products either to your local area network or directly to a host. Your controller has many important features that make it easy to integrate it into your data collection system. These features include:

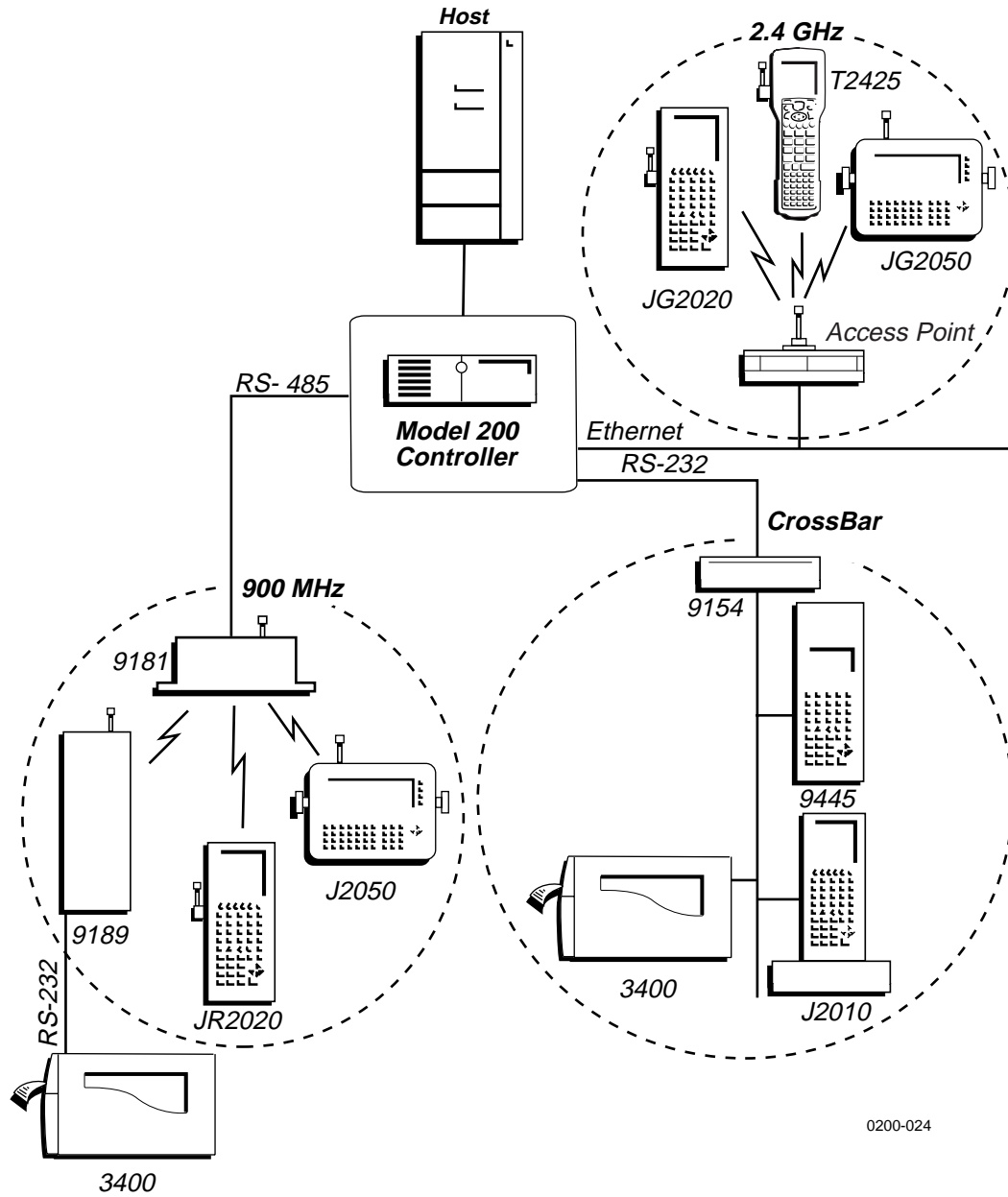
- An easy-to-use Fast Setup program with a graphical user interface (GUI). Fast Setup uses default values to help you get the controller quickly connected to your network.
- An Advanced Setup program that uses a GUI to help you customize the controller.
- Network adapter cards that support connections to hosts: Ethernet, token ring, twinaxial, coaxial, and SDLC networks.
- VT/ANSI terminal emulation for JANUS® devices and TRAKKER® Antares™ terminals to TCP/IP hosts.
- TN5250/TN3270 for JANUS 2.4 GHz RF devices and TRAKKER Antares terminals to TCP/IP hosts that support Telnet.
- 5250/3270 terminal emulation for JANUS devices and TRAKKER Antares terminals to SNA hosts.
- Peer-to-peer communications for APPC/LU6.2 and TCP/IP.
- Direct TCP/IP socket interface between data collection devices and hosts.
- Optional Script Builder tool that allows you to create custom screens and script files so that you can run VT, ANSI, 5250, or 3270 screen mapping.
- Optional RF controller 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 data collection devices to your hosts.
- Local management of external Intermec controllers and other data collection devices.

- Routing of transactions to one or multiple hosts.
- Localized language support for single-byte character sets in data collection devices that are running terminal emulation.
- Firmware Upgrade Utility that allows you to upgrade the firmware on your TRAKKER Antares terminals.

What's New for Release 3.1?

- Dynamic Host Configuration Protocol (DHCP) client support for the Model 200 Controller.
- Domain Naming Services (DNS) client support for the Model 200 Controller.
- Support for international text pass-through for peer-to-peer and direct TCP/IP applications.
- Support for double-byte character sets (DBCS) and data streams.
- Support for remote access to the Model 200 Controller using a third party remote console package.
- Ability to print to a printer attached to a terminal serial port that is within all terminal emulation clients.
- New system diagnostics tools: message log formatter, SNA subsystem management, and trace utility.
- New VT/ANSI screen mapping functionality to equal IBM screen mapping functionality. See the *DCS 300 Technical Reference Manual*.
- New screen mapping functionality. See the *DCS 300 Technical Reference Manual*.

Connecting the Model 200 Controller to Intermec's Data Collection Network



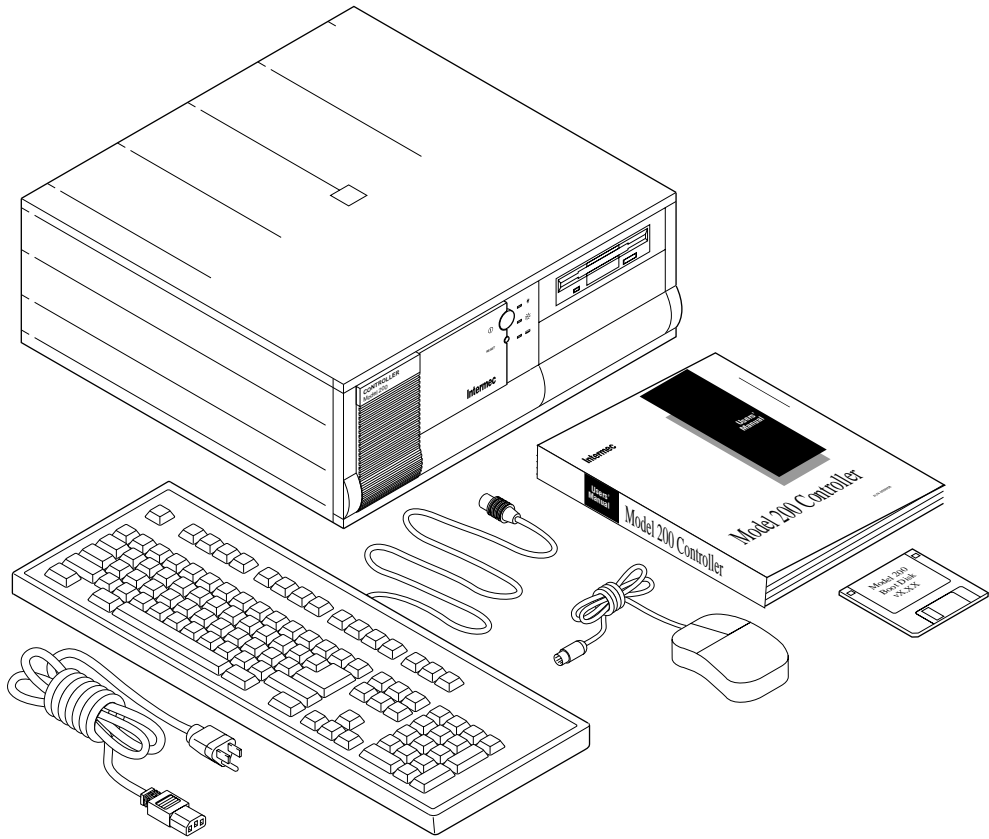
0200-024

Unpacking the Controller

1. Set the controller on a clean, stable, flat surface and remove the accessories, packing material, and the Model 200 Controller from the shipping container.
2. Save the shipping container and packing material in case you need to move or ship your controller.
3. Verify the contents of the shipping container against the list below. If any parts are missing, contact your local Intermec representative.
 - Model 200 Controller
 - AC power cord
 - Keyboard
 - Mouse
 - 3.5-inch disk to use for backing up your system files and run-time configuration
 - *Model 200 Controller Manual Supplement*
 - *Model 200 Controller System Manual*, which includes the *Fast Setup Quick Reference Guide* and the *Model 200 Controller User's Manual*
4. Report any damage or defects. Intermec thoroughly tested and inspected the controller 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 Model 200 Controller package to Intermec.

Model 200 Controller User's Manual

Contents of the Model 200 Controller Package

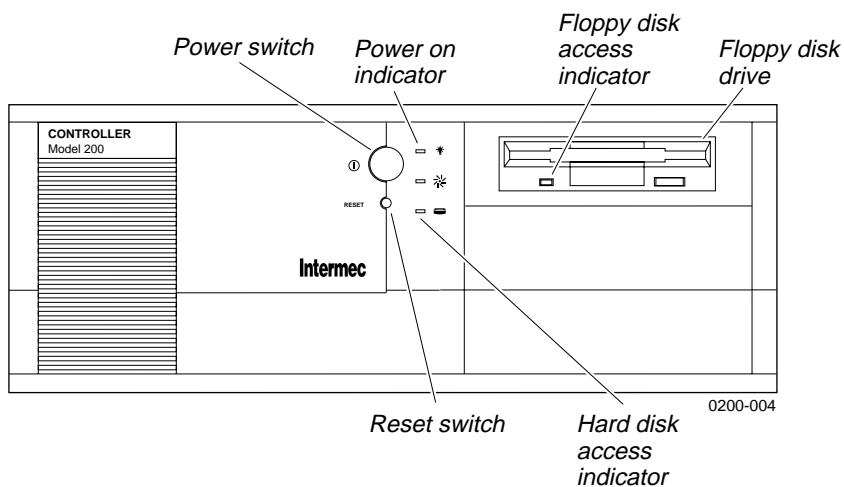


0200-002

Description

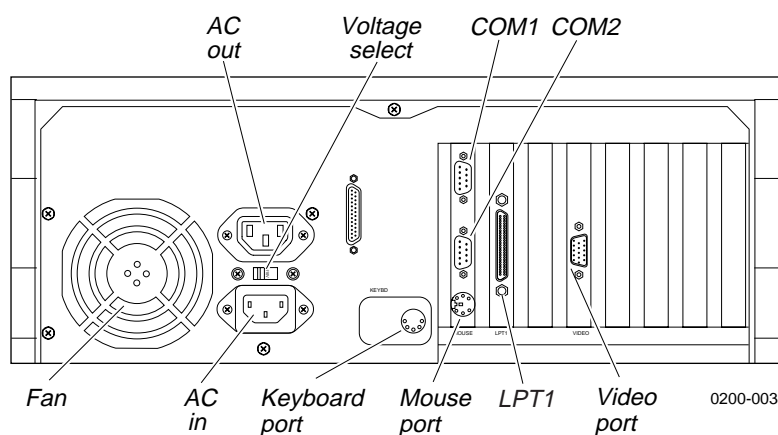
The Model 200 Controller contains several components on the front panel and on the rear panel that you should be able to identify.

Understanding the Front Panel



Component	Description
Power switch	Turns the controller on and off.
Power on indicator	Lights when the controller power is on.
Floppy disk access indicator	Lights when data is being read from or written to the floppy disk.
Floppy disk drive	This drive is a standard 3.5-inch high-density disk drive.
Reset switch	Performs a warm boot on the controller. Same as pressing Ctrl-Alt-Del on the keyboard.
Hard disk access indicator	Lights when data is being read from or written to the hard disk.

Understanding the Rear Panel



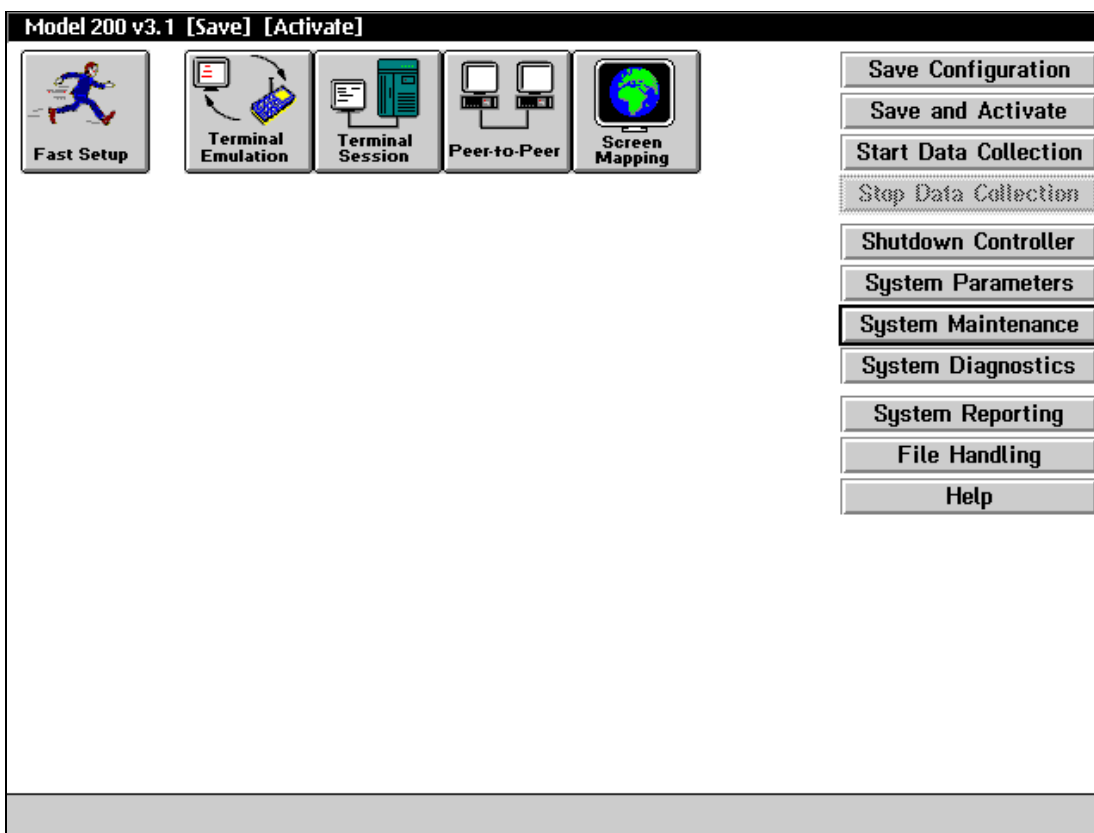
Component	Description
AC out	Provides AC power for accessories.
Voltage select	Sets the voltage of your controller to 110V or 220V.
COM1, COM2	Provides connections for external Intermec controllers, a modem, or other devices that require serial ports to connect to your controller.
Fan	Prevents your controller from overheating. When situating your controller, do not place it where the fan is obstructed.
AC in	Connects to one end of the AC power cord that provides power to the controller.
Keyboard port	Connects the keyboard to your controller.
Mouse port	Connects the mouse to your controller.
LPT1	Provides connection for the CD-ROM disk drive that you use to upgrade the software.
Video port	Connects the monitor to your controller.

About the Graphical User Interface

When you are ready to turn on the Model 200 Controller, push the yellow power switch. When you power on the controller for the first time, a dialog box appears that lists the network adapter cards in your controller. Choose one of the following:

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

The main menu appears.



Model 200 Controller User's Manual

The main menu has three parts:

Title bar The bar at the top of the main menu contains the name and version. If you are configuring the controller, [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 controller such as backing up the configuration files, viewing Hot Standby files, and defining system parameters.

Using Help

The Model 200 Controller includes online help that provides descriptions of the controller 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 Model 200 Controller, there are various ways that you can move through dialog boxes:

To Do This Action

Move between fields in a dialog box

Access the buttons in a dialog box

Go to the end of a file

Go to the top of a file.

Access a window that shows you which applications are running.

Do This Action

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.

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**.

Press **Ctrl-End**.

Press **Ctrl-Home**.

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 Model 200 Controller.

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 Controller Works

The Model 200 Controller 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 controller. 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 controller communicates with, and various transaction-related information. If you are using screen mapping, you can build script files and define terminal templates. 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 data collection devices, applications, and the controller 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 data collection devices and the message handler. DevComms implement all protocols that are required to communicate with the devices. The controller starts one DevComm for each communication channel that has been configured.

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

Model 200 Controller User's Manual

Network communication processes (NetComms) NetComms are the communication links between remote applications and the controller. 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 controller 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 controller, the transaction is actually received by the receive NetComm and then forwarded to the input channel. When the controller is started, it recognizes each remote application and then it creates the NetComms.

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

Note: The terminal sessions are established and run on the controller, not on the data collection devices.

For example, a transaction is built by a JR2020 and then transmitted through the BRU to the controller. The controller 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 controller 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 Model 200 Controller to data collection 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 controller. When a data collection 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 controller 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 controller, 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 controller has shut down.

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

How the Controller Routes Transactions

Transactions have a well-defined structure consisting of a header and data. The header contains a transaction ID, which the Model 200 Controller uses to determine the destination for a transaction. The transaction ID is the primary routing mechanism used by the controller.

When the controller 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 controller routes the transaction by examining the transaction header:

- If the destination field in the transaction header contains a name, the controller 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 controller 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 controller 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 controller ACK channel and it tells the controller that the application has responsibility for the transaction. Only then does the controller discard its copy and send another transaction to the application. Hot Standby logic controls how long the controller waits for an ACK transaction and what it does with other transactions while waiting.

Routing Transactions From Applications

The Model 200 Controller can route transactions from applications to data collection 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 controller searches through internal tables that are created from the run-time configuration to find all the correct information about the destination.

Learning About the Controller

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.

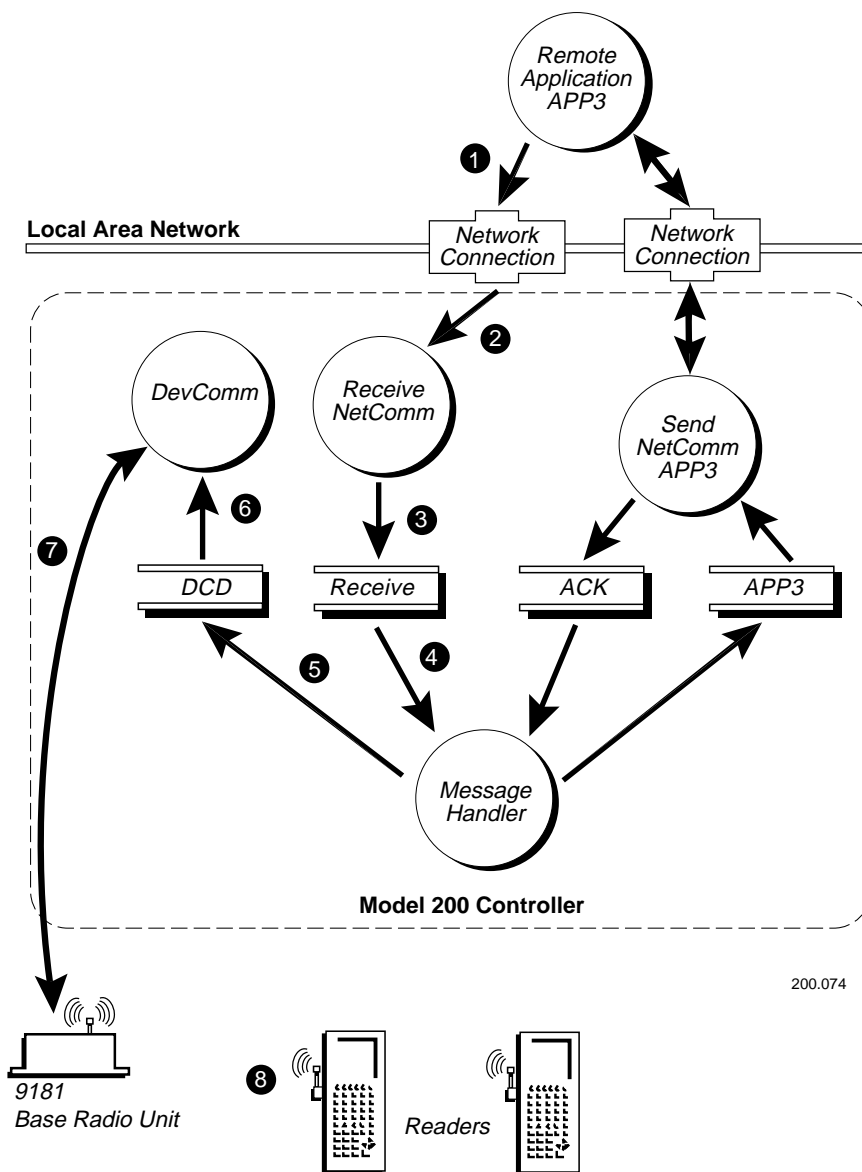
In this example, the application sends a transaction to a specific destination using the destination name in the transaction header. The numbers on the following paragraphs correspond to the numbers on the illustration on the next page.

- 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 controller delivers the transaction to the proper device 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 data collection 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



200.074

Routing Transactions From Devices

This example discusses the steps to move data from the data collection 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 controller.
- 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:

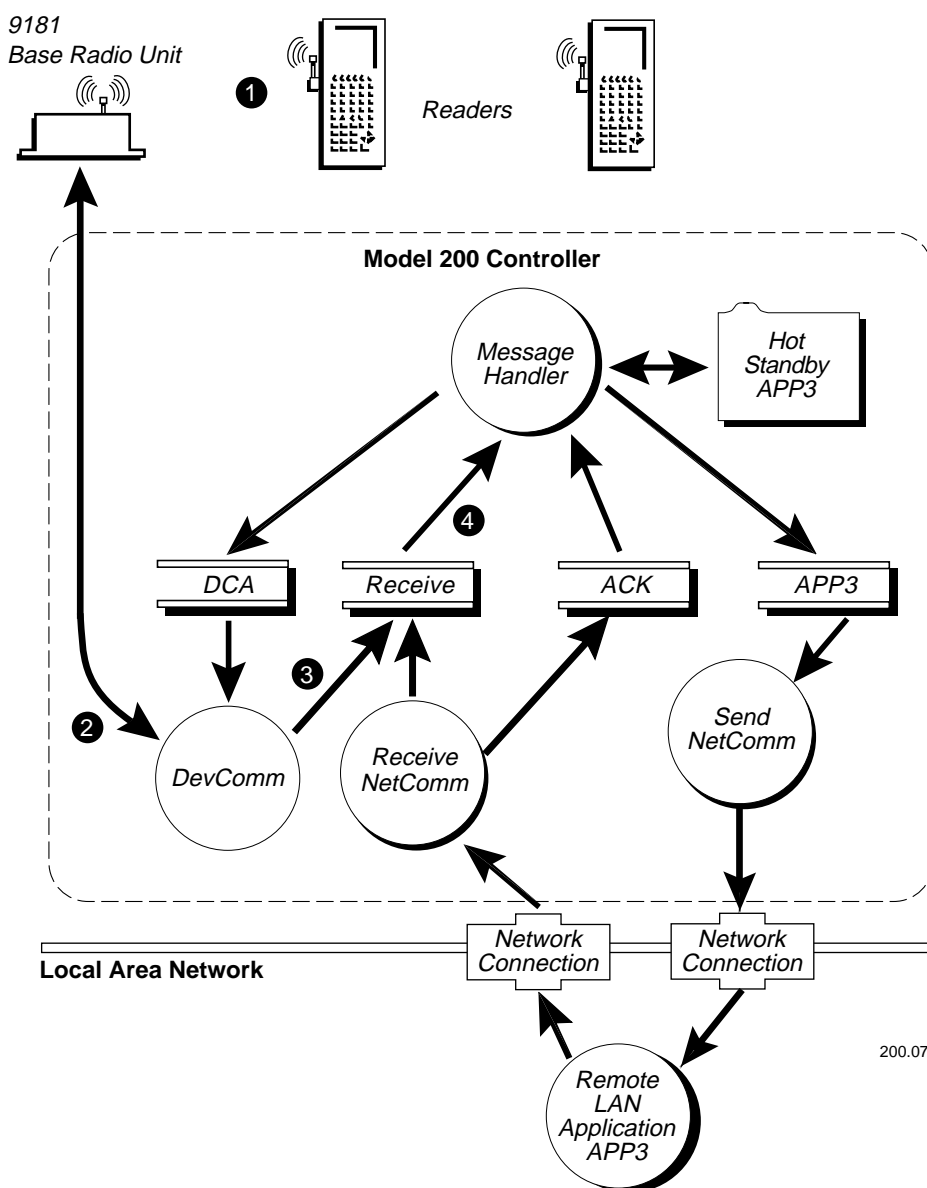
Timestamp The message handler gets the current time from the system and places it in the transaction header.

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



200.070

Learning About the Controller

Note: Steps 5 through 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

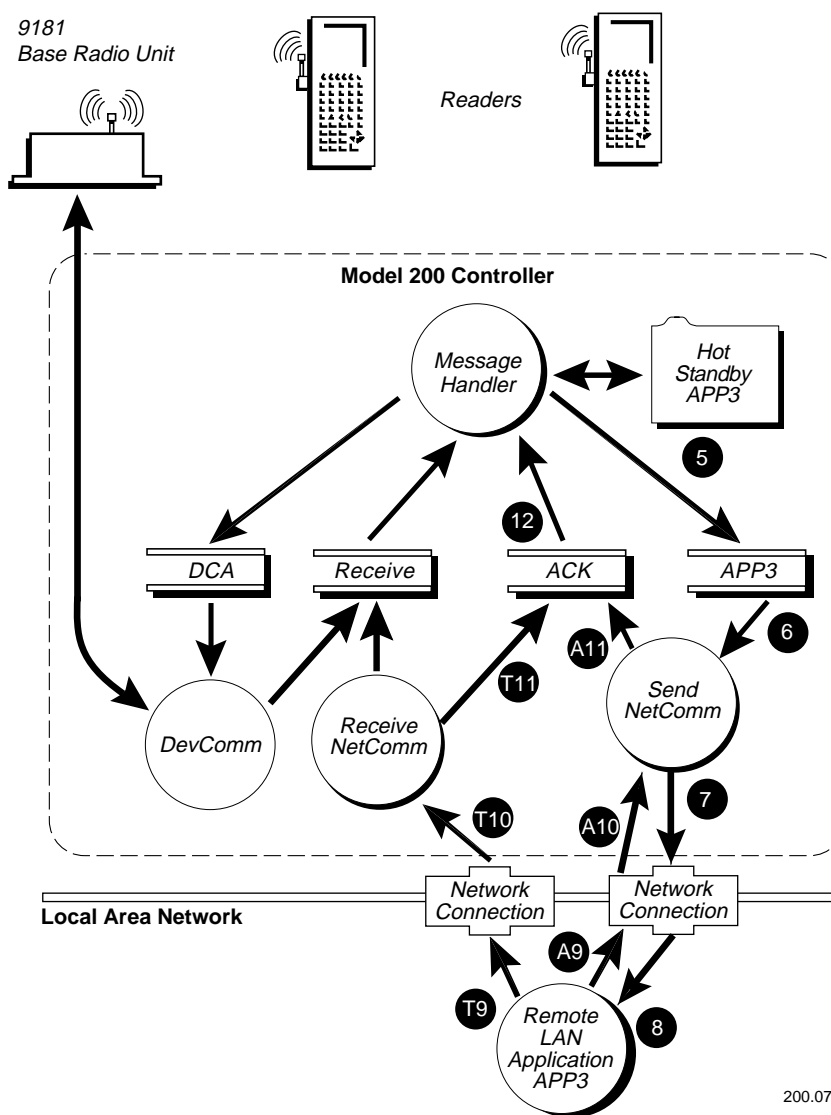
- T9 The remote application writes the ACK transaction to the receive NetComm.
- T10 The receive NetComm reads the ACK transaction sent from the remote application.
- T11 The receive NetComm places the ACK transaction in the ACK channel and sends a network ACK to the application.
- T12 The message handler reads the ACK transaction from the ACK channel.

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.

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 Data Collection Devices (continued)



200.072

How the Controller Acknowledges Transactions

After the controller 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 controller 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 controller. 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 controller fails to deliver a transaction to a device, the transaction is not discarded. The controller 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 Controller Ensures Data Integrity

The controller ensures data integrity from data collection devices to applications through the protocol handshakes that exist between the various components of the system. The controller 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 Data Collection Devices

Generally there is a tradeoff between response time and how interactive the data collection 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 controller, which then periodically uploads data to the application in a Batch mode.

Model 200 Controller User's Manual

There are three levels of interactivity which the controller 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 controller 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 data collection 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 controller can be configured to automatically assume responsibility for the application's transactions by becoming interactive with the device. When the controller becomes interactive with the device, it invokes the Hot Standby feature. The controller 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 controller saves the transactions bound for that application in a Hot Standby file. The controller maintains a Hot Standby file for each application it knows about. When the controller 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 data collection device is interactive with the controller instead of the application. To guarantee data integrity, the controller 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 controller.

When the application becomes active and is ready to accept more data from the controller, the controller checks the Hot Standby file and delivers transactions to the application in a first-in-first-out (FIFO) order. The controller 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 controller 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 data collection 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 controller. Once the controller has received a transaction, features such as Hot Standby mode are still active to ensure data integrity.

To configure the controller's Hot Standby feature for noninteractive systems, you set up the controller 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 controller is accepting the data and storing it in the Hot Standby file.

Data Integrity Modes

The Model 200 Controller 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 Model 200 Controller 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 Model 200 Controller.

Faster Mode

Faster mode is the default integrity mode. The advantage of Faster mode is speed: the external controller can forward data to the Model 200 Controller faster than in Safer mode. The disadvantage is a small risk that transactions will be lost if the Model 200 Controller 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 Model 200 Controller uses this queue as a temporary holding place for transactions that are waiting to be sent to a destination while the controller is waiting for an ACK from that destination.

AUX_Q is used only in this situation:

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

You can specify the number of transactions the controller 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 controller from using AUX_Q by setting the parameter to None, which forces the controller 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 controller 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 Controller Sets Application Status

When the Model 200 Controller 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 controller waits for an ACK transaction for the duration of the Hot Standby timeout. If an ACK is not received within the timeout period, the controller automatically places the application in a nonactive, Hot Standby state.

During a controller 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 controller. The next time the controller 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 Model 200 Controller 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 controller can deliver only one transaction at a time to each application. Before the controller delivers a second transaction to a destination, the remote application must take responsibility for the current transaction by sending an ACK transaction.

The controller 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 Model 200 Controller for a transaction. An application becomes nonactive in these two situations:

- If the Hot Standby timeout expires before the controller received an ACK from the application, the controller places the application in a nonactive state. Also, the controller 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 controller places the application in a nonactive state. Also, the controller writes the contents of AUX_Q and all new transactions for the application into the Hot Standby file.

Sending Hot Standby Messages

When the controller receives a transaction for a nonactive application, it can send a user-defined response to the device that was the source of the transaction. This optional, user-defined response is known as 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 controller does not recognize the transaction ID, the controller 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 in the GUI.

If the Hot Standby message field is empty, the controller sends nothing to the device when it saves a transaction on disk. It is the application's responsibility to return a response to a device when it receives the transaction. A response may not be required, for example, when receiving status transactions from printers. If the transaction is from a bar code reader that is operating in computer response required mode, the reader remains locked until a response is received or the reader times out. Therefore, when readers are configured this way, it is better to have the controller reply with the Hot Standby message when it cannot deliver a transaction to the application.

Because transactions can have multiple routes, the controller 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 named TRANID1 that gets routed to three destinations (selftest, writeit, and batchit) and has the following Hot Standby message, "Data saved on disk." When the message handler receives a TRANID1 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 originated 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 Model 200 Controller 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 Controller

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

Chapter Checklist

Done?	Task	Page
<input type="checkbox"/>	Plug in the power cord.	2-4
<input type="checkbox"/>	Plug in the keyboard.	2-5
<input type="checkbox"/>	Plug in the mouse.	2-6
<input type="checkbox"/>	Connect the monitor to the controller.	2-7
<input type="checkbox"/>	Connect the uninterruptable power supply to the controller.	2-8
<input type="checkbox"/>	Connect the modem to the controller.	2-11
<input type="checkbox"/>	Set the system parameters on the controller.	2-14
<input type="checkbox"/>	Understand the configuration files and how to restore your default configuration.	2-17
<input type="checkbox"/>	Understand how to back up and restore the system and user files on your controller.	2-18
<input type="checkbox"/>	Understand how to start data collection, stop data collection, and shut down the controller.	2-24

If you already understand and have performed these tasks, connect the controller 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 Model 200 Controller. However, you may want to plug the power cord into an uninterruptible 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 Uninterruptible Power Supply" later in this chapter.



Warning

Before connecting the power cord, make sure that the controller 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 to the controller

1. Locate the AC in receptacle on the rear panel of the controller.
2. Insert the power cord's 3-pin connector into the AC in receptacle.
3. Intermec recommends that you use a surge protector. Plug the surge protector into the AC power outlet.
4. Set the voltage select switch to 110V or 220V.
5. Plug the power cord into an AC power outlet or surge protector.

Plugging In the Keyboard

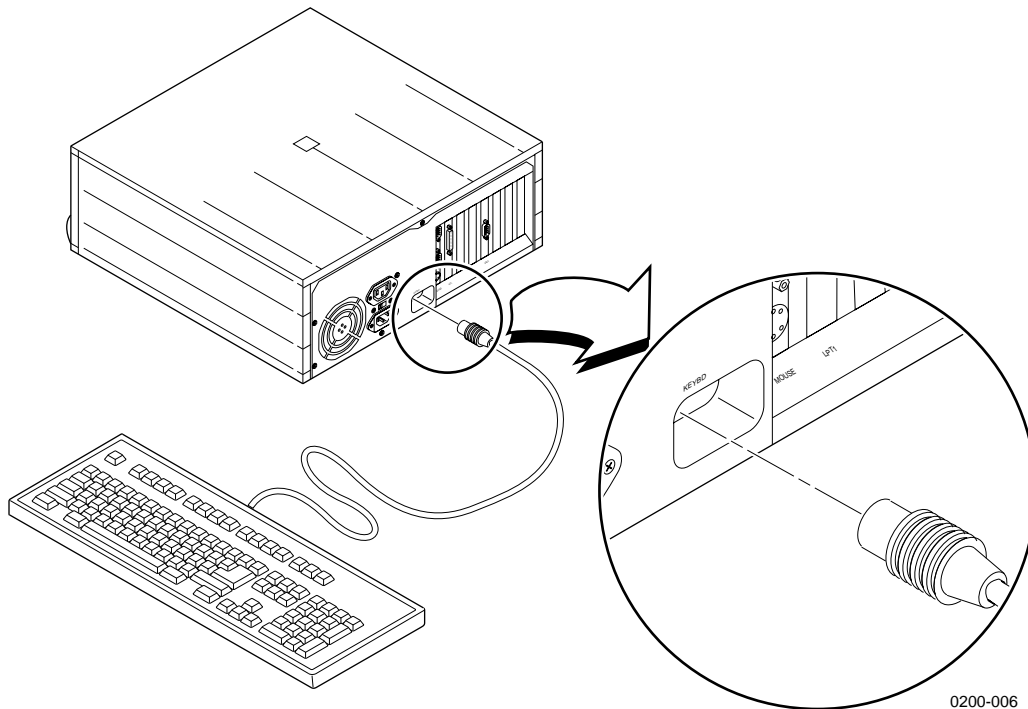
You may need to use the keyboard to enter information when using the GUI to configure the Model 200 Controller.

Equipment

- Keyboard (standard)

To plug in the keyboard

1. Locate the keyboard port on the rear panel of the controller.
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 Model 200 Controller.

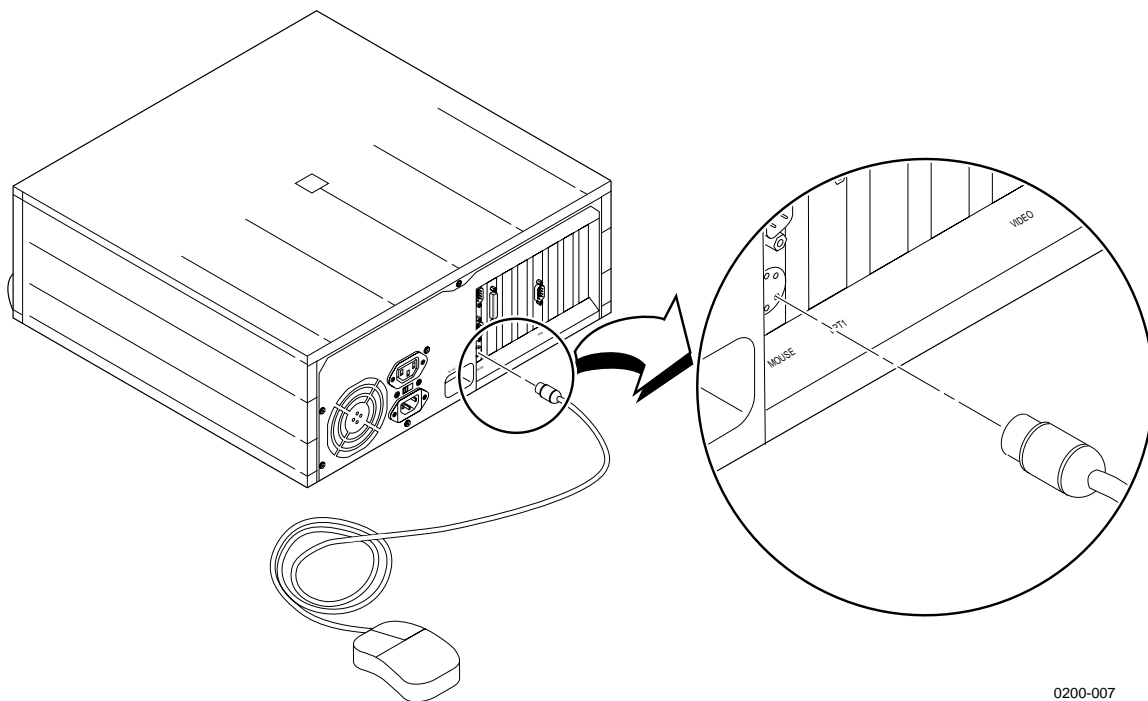
Note: You must have the mouse plugged into the controller whenever you boot the controller.

Equipment Required

- Mouse (standard)

To plug in the mouse

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



0200-007

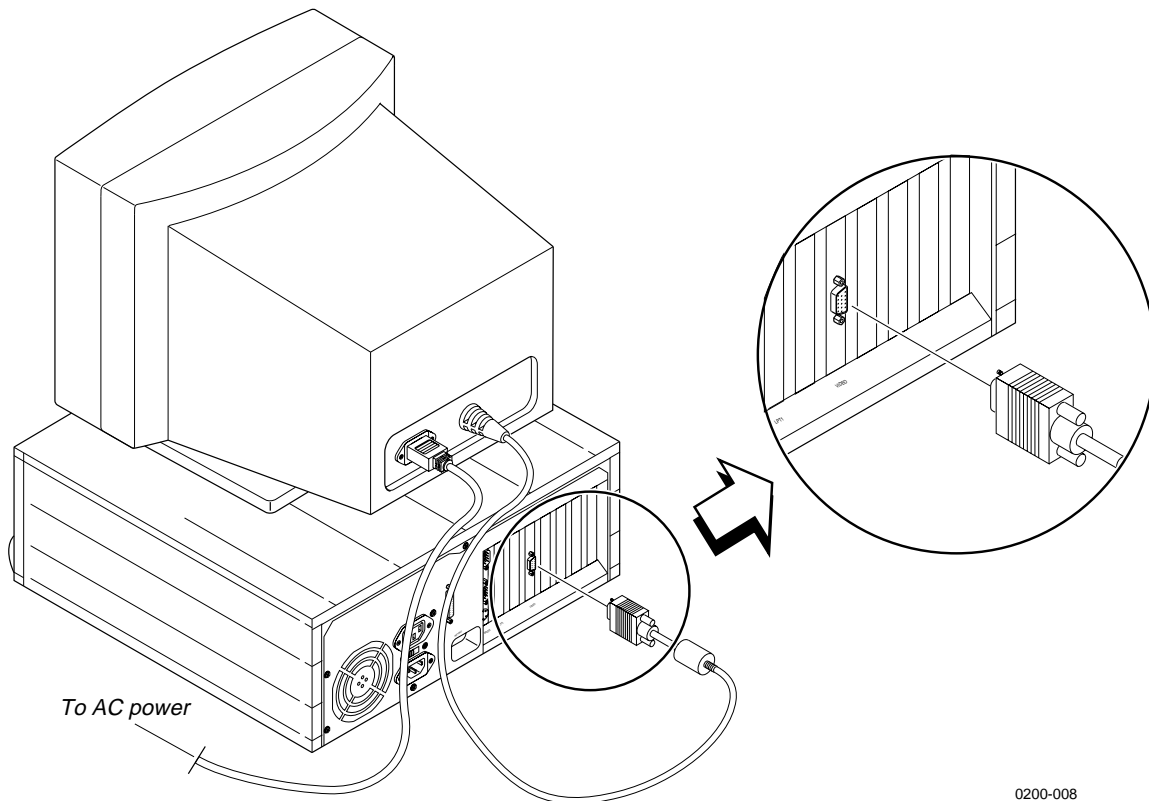
Connecting the Monitor

Equipment

- Monitor with cable and power cord (not provided)

To connect the monitor to the controller

1. Locate the video port on the rear panel of the controller.
2. Insert one end of the monitor's 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.



0200-008

Connecting an Uninterruptable Power Supply

Intermec strongly recommends that you connect an uninterruptable power supply (UPS) to your Model 200 Controller. In case of a power failure, the UPS provides enough backup power to allow the Model 200 Controller 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.  
Controller shutdown will occur in approx 5 minutes.
```

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

You can configure the controller 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)

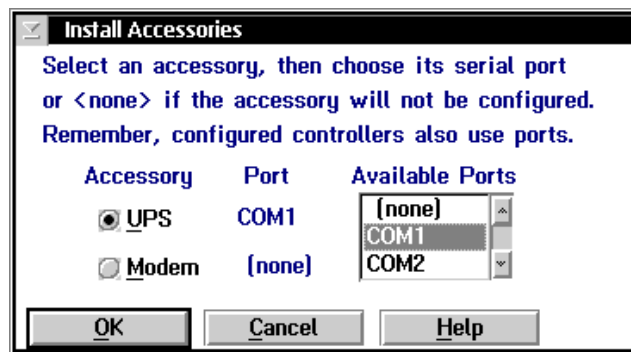
Or,

Uninterruptable power supply, International (Intermec Part No. 589079)

- Cable for auto-restoration (Intermec Part No. 589157)

To connect a UPS to the controller

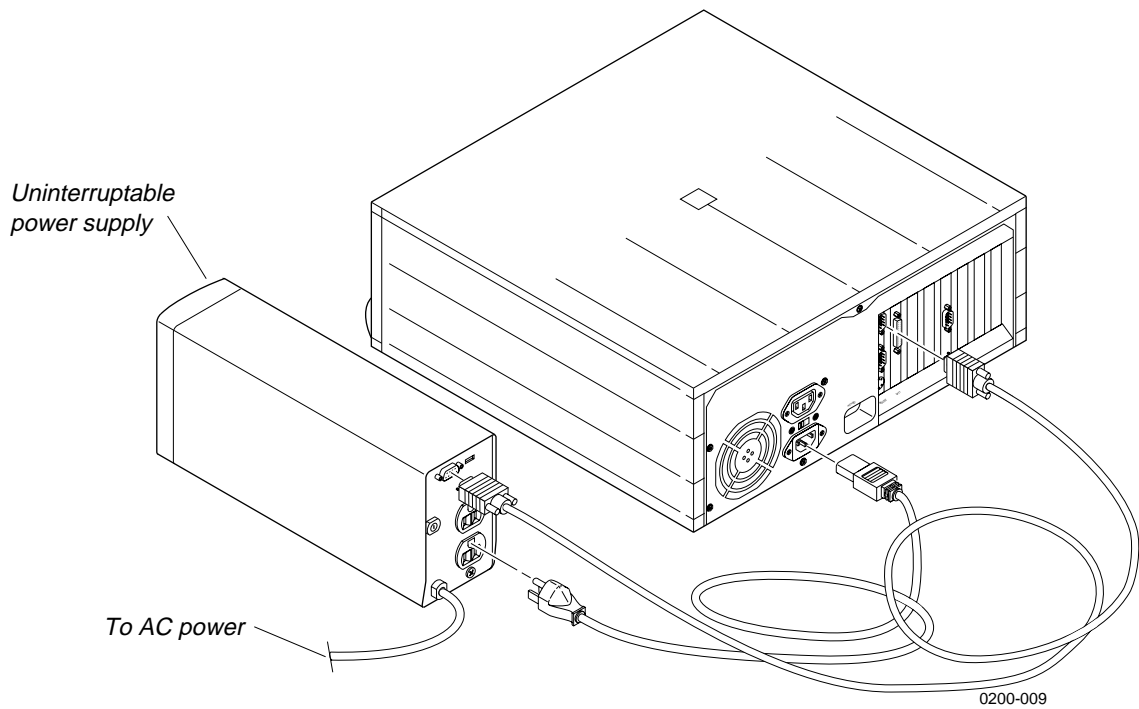
1. Make sure the power is off. The power indicator should be off.
2. Insert the controller power cord's 3-pin connector into the AC in receptacle.
3. Plug the other end of the power cord into the UPS.
4. (Optional) Intermec recommends that you use a surge protector. Plug the power cord of the UPS into 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 controller.
7. Set the voltage select switch to 110V or 220V.
8. Press the power button on the controller. The power indicator turns on. The main menu appears.
9. From the main menu sidebar buttons, choose System Maintenance. The System Maintenance dialog box appears.
10. In the System Maintenance list box, choose Install Accessories and then choose Start. The Install Accessories dialog box appears.



11. Choose UPS.
12. In the Available Ports list box, select the serial port on the Model 200 Controller that you used to connect to the UPS.

Model 200 Controller User's Manual

13. Choose OK to save your changes. You return to the System Maintenance dialog box.
14. Choose Close to return to the main menu.



Connecting a Modem

You may want to connect your Model 200 Controller 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 controller 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

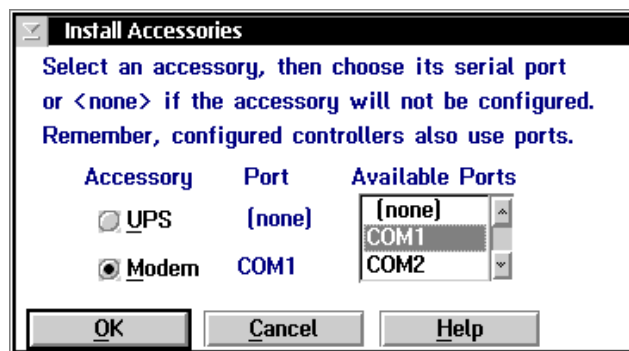
- Modem with telephone cable and power cord, U.S. and Canada (Intermec Part No. 590201)
- Serial cable to connect the modem to the Model 200 Controller (Intermec Part No. 589182)

To attach a modem to the controller

1. Make sure the power is off. The power indicator 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 controller.
6. Press the power button on the controller. The power indicator turns on. The main menu appears.
7. From the main menu sidebar buttons, choose System Maintenance. The System Maintenance dialog box appears.

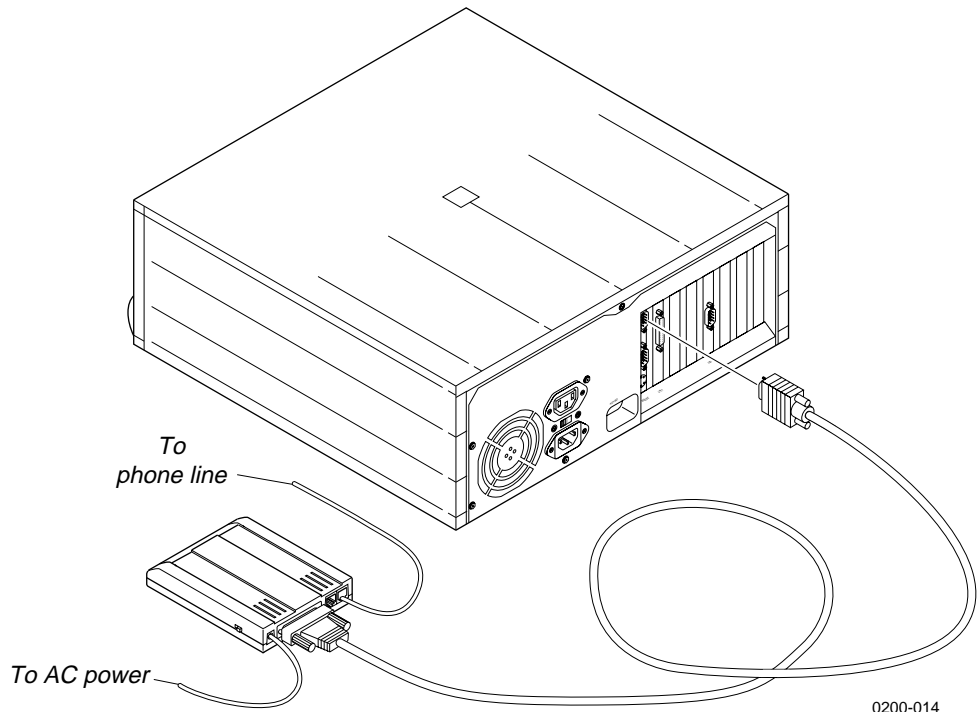
Model 200 Controller User's Manual

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



9. Choose Modem.
10. In the Available Ports list box, select the serial port on the Model 200 Controller 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.

Connecting the Model 200 Controller to a Modem



Setting the System Parameters

When you set system parameters, you are defining the operating parameters for the Model 200 Controller.

Time Synchronization This optional parameter causes the Model 200 Controller to send a time broadcast at certain intervals to all external Intermecc controllers.

Note: The time broadcast is not necessarily sent to the data collection devices that are connected to the external Intermecc controllers. However, when you configure a controller, you can configure it to broadcast the time to its devices.

Transaction Parameters These optional parameters make sure that the system knows the delimiter that separates the transaction ID from the transaction fields. Use the Bad ID response field if you want to make sure that there is always a response for a failed delivery of a transaction.

Peer-to-Peer Network Connection Parameters These required parameters tell the controller how to set up network connections in a peer-to-peer environment.

System Parameters
Modify the system operation parameters.

Time Synchronization
 Send to downline devices every minutes (0-9999)

File Transfer Time
 seconds (0-9999)

Transaction Parameters
ID delimiter: The delimiter separates the transaction ID from the rest of the transaction's fields.
Bad ID response:

Peer-to-Peer Network Connection Parameters
Maximum connections: (1-256) Strip pad:

Auto-Start
 Auto-start data collection when the Model 200 Controller is booted.

Terminal Emulation Setup Screens
 VT/ANSI 5250 3270

OK Cancel Help

Field	Description	Value	Default
Send to downline devices every...	This check box determines if the Model 200 Controller sends its time to all external Intermecc controllers.	Check, Clear	Check
...minutes	This field specifies how often in minutes the controller sends the time synchronization message.	0 to 9999	60
File Transfer Time	This box specifies how long in seconds the controller waits for a response from the data collection device when it is downloading files before it times out.	0 to 9999	180
ID delimiter	The character that the data collection devices use to separate the transaction ID from the transaction fields.	Predefined	, (comma)
Bad ID response (Optional)	The message that the controller sends to the source of the transaction if the controller does not recognize the transaction ID.	1 to 39 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 controller to remove before sending the transaction.	Predefined	None
Auto-Start	This check box determines if the controller starts data collection when it is booted.	Check, Clear	Clear
Terminal Emulation Setup Screens (Optional)	This box allows you to customize which terminal emulation buttons appear in the main menu.	VT/ANSI, 5250, 3270	All

To set the system parameters

1. From the main menu sidebar buttons, choose System Parameters. The System Parameters dialog box appears.
2. Enable or disable time synchronization. A check in the check box indicates that time synchronization is enabled. Enter how often (in minutes) you want the controller to send the time broadcast to all external Intermecc controllers.
3. In the File Transfer Time box, enter the number of seconds the controller waits for a response from a device when it is downloading files to that device, before it times out.
4. In the ID delimiter field, click the down arrow on the right side of the field. A list of available delimiters appears. Select the delimiter that you want to use to separate the transaction ID from the rest of the transaction fields in data coming from data collection devices.
5. (Optional) In the Bad ID response field, enter the message that you want sent back to the source of the transaction if the controller does not recognize the transaction ID.
6. (Peer-to-peer applications) In the Peer-to-Peer Network Connection Parameters box, enter the maximum number of connections for each NetComm process.
7. (Peer-to-peer applications, APPC only) In the Strip pad field, click the down arrow on the right side of the field. A list of characters that a host application may use to pad fixed-length transactions appears. Select the character that the controller removes before sending on the transaction.
8. In the Auto-Start box, enable or disable the controller from automatically starting data collection when it boots. A check in the check box enables this feature.
9. (Optional) In the Terminal Emulation Setup Screens box, choose which type of terminal emulation you want displayed in the main menu.
10. Choose OK to save your changes and return to the main menu.

About the Configuration Files

The Model 200 Controller 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 controller to a new system, select this option. For help, see “Restoring Default Configuration” in the next section.

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

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

Restoring Default Configuration

This procedure restores the factory default configuration of the Model 200 Controller. 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 Controller 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 Controller to shut down the controller.
6. Press **Ctrl-Alt-Del** to reboot the controller.

Backing Up the Controller 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 Model 200 Controller.

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 Model 200 Controller package, unpack the blank, formatted, 3.5-inch disk. Use this disk to back up your system files and run-time configuration. If your controller loses its configuration, you can use these files to restore the controller.

To back up the configuration

1. Insert the 3.5-inch disk into the controller 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 controller 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.
6. From the System Maintenance dialog box, choose Close to return to the main menu.

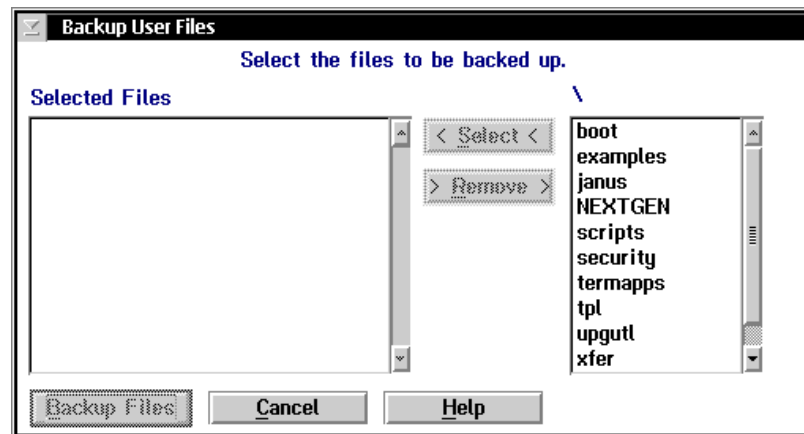
Backing Up Your User Files

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

Note: When backing up your user files, you need to 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 controller 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 controller backs up the user files you selected.
7. Remove your disk from the disk drive, label it, and put it in a safe place.
8. From the File Handling dialog box, choose Close to return to the main menu.

Restoring the Controller Configuration

If your Model 200 Controller loses its configuration, you can recover the system files and run-time configuration.

Restoring Your System Files and Run-Time Configuration

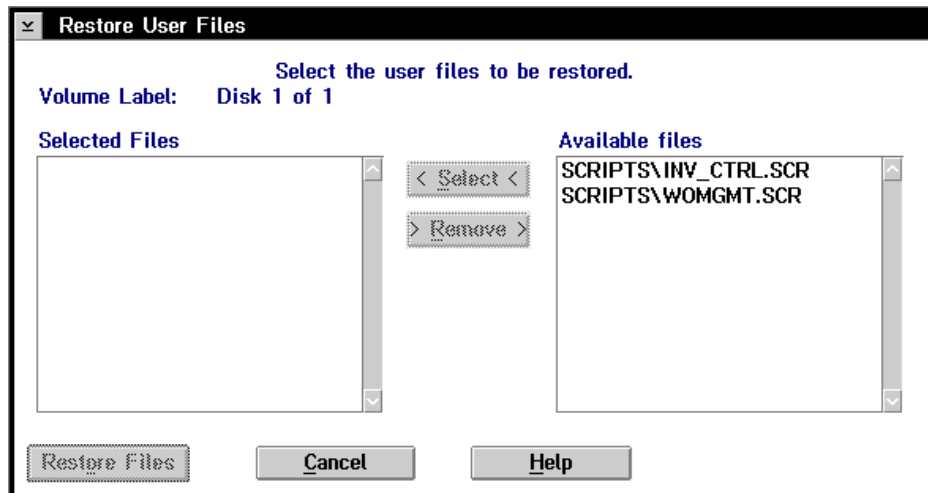
1. Insert the 3.5-inch disk that contains the system files and run-time configuration backup into the controller disk drive.
2. From the main menu sidebar buttons, choose System Maintenance. The System Maintenance dialog box appears.
3. In the System Maintenance list box, select Restore System Files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

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 controller.

To restore your user files

1. Insert the 3.5-inch disk that contains the backup of your user files into the controller 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 controller.
4. Choose OK. The Restore User Files dialog box appears. The files on the floppy disk appear in the Available Files list box.

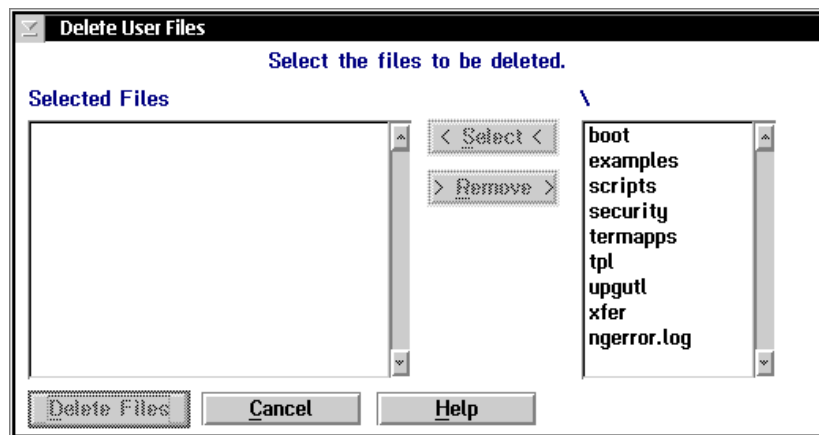


Model 200 Controller User's Manual

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 controller restores the files you selected.
8. Remove your disk from the disk drive and put it in a safe place.
9. From the File Handling dialog box, choose Close to return to the main menu.

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 controller deletes the user files you selected.
7. From the File Handling dialog box, choose Close to return to the main menu.

Using the Controller

To use the Model 200 Controller, you need to know how to start and stop data collection and shut down the controller.



Caution

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

Conseil

Choisissez toujours le bouton Shutdown Controller 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.

Stopping Data Collection

You may need to stop data collection on your Model 200 Controller to update its configuration file. When you stop data collection, all data collection activities are stopped, but any external Intermecc controllers continue polling and buffering data. Data collection devices using programs that require a response directly from a destination (interactive mode) also stop until the controller is started again.

To stop data collection on the controller

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.

Turning Off the Controller

You may need to power off the Model 200 Controller for maintenance or relocation. The controller 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 shut down the controller

1. From the main menu sidebar buttons, choose Shutdown Controller. The Shutdown Model 200 Controller message box appears.
2. Enable or disable the Save and activate changes check box depending on if you want to save any changes you have made to the configuration.
3. Choose Shutdown to shut down the controller. The controller 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 controller.

Accessing a Command Prompt

While maintaining or configuring your controller, 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 Controller Command Prompt and then choose Start. The Command Prompt Password dialog box appears.



3. In the Password field, type:
INTERMEC
4. Choose OK. The Controller 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.

Connecting to the Intermec RF Network

This chapter explains how to connect the Model 200 Controller to the 900 MHz RF network using RF controller cards and BRUs and to the UDP Plus network using access points, JANUS devices, and TRAKKER Antares terminals.

Chapter Checklist

Done?	Task	Page
<input type="checkbox"/>	Connect the controller to the 900 MHz RF network.	3-4
<input type="checkbox"/>	Connect the controller to the Ethernet network.	5-5
<input type="checkbox"/>	Configure the RF controller cards in the controller to communicate with the BRUs.	3-6
<input type="checkbox"/>	Set the time parameters for the 900 MHz network.	3-11
<input type="checkbox"/>	Identify the JANUS 900 MHz RF devices.	3-15
<input type="checkbox"/>	Edit the JANUS 900 MHz RF devices.	3-17
<input type="checkbox"/>	Configure the 2.4 GHz RF (UDP Plus) network.	3-19
<input type="checkbox"/>	Set the time parameters for the UDP Plus network.	3-27
<input type="checkbox"/>	Identify the UDP Plus devices.	3-31
<input type="checkbox"/>	Edit the UDP Plus devices.	3-33

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

- Chapter 4, "Connecting to the 9180 and the Intermecc CrossBar Network"
- Chapter 5, "Connecting to an Ethernet/Token Ring Network"
- Chapter 6, "Connecting to a Coaxial/Twinaxial Network"
- Chapter 7, "Connecting to an SDLC Network"

Connecting the Controller to the 900 MHz RF Network

The Model 200 Controller can communicate with Intermec's 900 MHz RF data collection network. To communicate with this network, the controller contains RF controller cards (up to two) that connect by an RS-422 cable to 9181 Base Radio Units (BRUs). The BRUs transmit information from the controller to Intermec RF devices and receive signals from them. The illustration on the next page shows an example of a Model 200 Controller connected to a 900 MHz RF network.

Each RF controller card supports either 2-port or 4-port options so you can connect up to seven BRUs in an Intermec 900 MHz data collection network.

Before you configure the RF controller card, you should do the following:

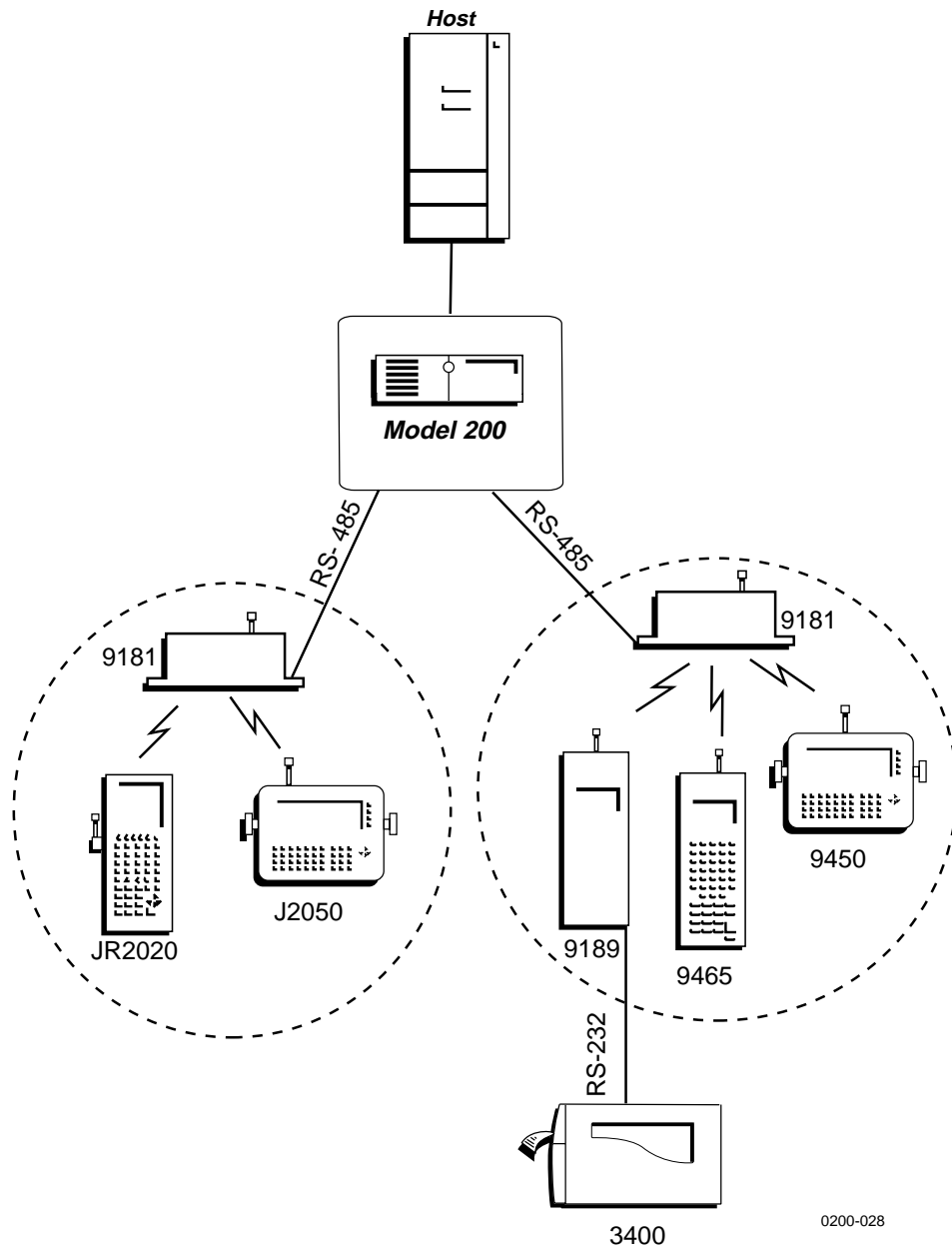
- Configure the host connection.
- Install the 9181 BRUs, JANUS RF devices, and any other Intermec RF devices.

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 Model 200 Controller and the BRU, you need to know if you have 2-port or 4-port RF controller cards in the controller. Cables must be ordered separately.

- If you have a 2-port card, you need an Intermec cable kit (Intermec P/N 055003) or equivalent. You also need a Belden 89688 cable (Intermec P/N 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 controller card. Use Intermec cable kit (Intermec P/N 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 P/N 583326) or equivalent.

Example: The Model 200 Controller Connected to the Intermec 900 MHz RF Network



0200-028

Configuring RF Controller Cards

You need to configure the communications parameters, enable the BRUs, set the Hot Standby timeout, and set any special time parameters for the RF controller cards. Use the worksheets in Appendix E.

Communication Parameters These required parameters set the attributes of the RF controller cards. You need to set these parameters so the devices can transmit messages to the controller and the controller can send messages to the devices. Each RF controller card must have a unique RFNC address and a unique network ID.

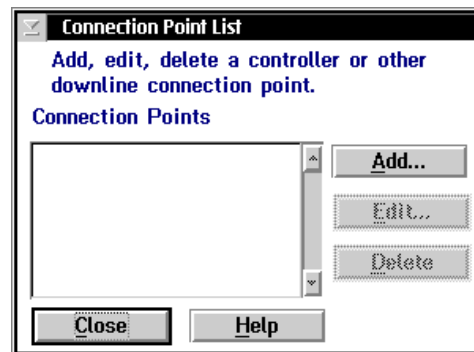
BRU Parameters These required parameters set the attributes of the BRUs that are connected to the RF controller cards. Identify which BRUs should be enabled, set each BRU to a unique channel/frequency, and choose the number of hops each message is allowed.

Hot Standby Timeout This required parameter sets the amount of time the controller waits to receive an acknowledgment after delivering a transaction to a data collection device. If it does not receive an acknowledgment, the controller writes the transactions for the device to a Hot Standby file. The device receives its transactions from this file when it comes back online.

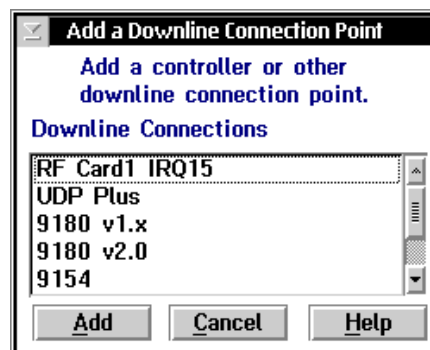
Transactions Routed to This Card box This required parameter lets you choose the number of transactions you want the server to keep in volatile RAM before it begins to write them to a Hot Standby file.

To configure the RF controller card

1. From the main menu, choose the type of communication you are using to connect the controller 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. Add, edit, or delete RF controller card connections. For help, see “Adding RF Controller Cards and BRUs” in the next section.
5. Choose Close to close the dialog box and return to the main menu.

**Adding RF Controller Card and BRUs**

1. In the Connection Point List dialog box, choose Add. The Add a Downline Connection Point dialog box appears.
2. In the Downline Connections list box, select the RF card you want to add.
3. Choose Add. The Setup for Controller: RF Card dialog box appears.



Model 200 Controller User's Manual

Setup for Controller: RF Card
 Edit the parameters for this RF controller card.

Communication Parameters

Card number: 1
 IRQ number: 15
 RFNC address: 0 (0-63)
 Network ID: 1 (1-254)
 Acknowledgment delay: 100 (0-255)
 Retry count: 64 (0-255)

BRU Parameters

BRU #	BRU Status	Channel Frequency	Repeat Count
1	<input checked="" type="checkbox"/> Enable 1	0 924 MHz	0 (0-7)
2	<input type="checkbox"/> Enable 2	1 921 MHz	0 (0-7)

Hot Standby Timeout
 40 seconds (1-9999)

Configure...
 Time Parameters...

Transactions Routed to This Card
 Transactions held in volatile memory:
 None Unlimited
 Maximum: 50 (1-9999)

OK Cancel Help

Field	Description	Value	Default
Card number	The RF controller card that you want to configure.	1, 2	1
RFNC address	The radio frequency network address of the RF controller 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 network ID of the RF controller card. Devices use this ID during a channel search to locate the RF controller card's RFNC address.	1 to 254	1. If 1 is being used, the next available value is used.

Field	Description	Value	Default
Acknowledgment delay	The maximum amount of time in milliseconds that the RF controller card waits before it determines that the device did not receive a message.	0 to 255	100
Retry count	The number of times the RF controller card tries to transmit to a device.	0 to 255	64
BRU Status	This check box determines which BRUs are connected to the RF controller 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.	0 to 7	0
Hot Standby Timeout	The number of seconds the controller waits for a response from a device before it writes transactions for the device to a Hot Standby file.	1 to 9999	40
Transactions held in volatile memory	The number of transactions the controller keeps in RAM before it writes the transactions to a Hot Standby file.	None, Unlimited, Maximum	Maximum 50

Model 200 Controller User's Manual

4. In the Card number field, click the arrow on the right side of the field. A list of the available RF controller cards appears. Select the RF controller card you want to configure.
5. Enter the RFNC address, network ID, acknowledgment delay, and retry count for the RF controller card. Each RF controller card must have a unique RFNC address and a unique network ID.
6. In the BRU Parameters box, enable or disable the BRUs that you want to communicate with this RF controller card.
7. In the Channel - Frequency field, click the down arrow on the right side of the field. A list of all the available channels and frequencies appears. For each BRU, select a unique channel - frequency.
8. In the Repeat count field, enter the number of repeaters each message is allowed to pass through.

Note: Intermec recommends that a message does not pass through more than three repeaters. Using more than three repeaters may cause excessive delays when communicating with the terminals.

9. In the Hot Standby Timeout box, enter the number of seconds the controller waits for a response from a device before it writes transactions for the device to a Hot Standby file.
10. In the Transactions Routed to this Card box, choose the number of transactions you want the controller to keep in RAM before it writes 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 controller has this number of transactions in RAM, it writes them to a file.
11. Choose Time Parameters to configure specific time parameters for this RF controller card. For help, see "Setting the Time Parameters" in the next section.
12. Choose OK to close this dialog box and return to the Connection Point List dialog box.

Setting the Time Parameters

Use this dialog box to configure the broadcast and append parameters between the BRUs and their devices.

Note: When the controller sends a time broadcast, it is not a guaranteed packet.

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

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.

Model 200 Controller User's Manual

Field	Description	Value	Default
Broadcast enabled	This check box determines if the BRUs broadcast a time to all devices communicating with them.	Check, Clear	Clear
Include Seconds	This check box adds seconds to the time.	Check, Clear	Clear
Include Date	This check box adds the date to the time.	Check, Clear	Clear

Field	Description	Value	Default
Time format	These option buttons choose the time broadcast format.	12 hour, 24 hour	12 hour
Interval	This field specifies how often in minutes the controller broadcasts the time.	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 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

To set the time parameters

1. From the Setup for Controller dialog box, in the Configure box, choose Time Parameters. The Configure Time Parameters dialog box appears.
2. In the Broadcast Parameters box, enable or disable the time broadcast. A check in the Broadcast enabled check box means that time broadcast is enabled.

If you do not enable time broadcast, skip to Step 8.

3. Enable or disable including seconds in the time. A check in the Include Seconds check box means that seconds are added.

Note: If you are using JANUS RF devices to communicate with the BRUs, you must enable this check box.

4. Enable or disable including the date in the time. A check in the Include Date check box means that the date is added.
5. Choose the 12 Hour or 24 Hour time format button.
6. In the Interval field, enter how often (in minutes) you want the controller to do a time broadcast. If you set this field to 0, no time broadcast is made.
7. In the Preamble and Postamble fields, enter a short string you want to add before or after the time to customize it.
8. In the Append Parameters box, enable or disable the time append. A check in the Append enabled check box means that there is a time appended to all messages.

If you do not enable time append, skip to Step 12.

9. Enable or disable Include Year, Include Month, Include Day, Include Seconds. A check in the check box means that the part of the date or time is included in the time.
10. In the Delimiter field, click the down arrow on the right side of the field. A list of available delimiters appears. Select the delimiter that you want to use to separate the appended time from the transaction data.
11. Enable or disable Julian format. A check in the check box means that the date is in Julian format. Other date and time options are not used.
12. Choose OK to save your changes and return to the Setup for Controller dialog box.

Identifying the RF Devices

You need to configure the Model 200 Controller for all the devices that use it to communicate with the host. The device list contains the logical names of all 128 devices. The first eight names are enabled and are configured as JANUS 2020s. You need to enable or disable the logical names of any other devices that you want to be available to communicate with the host.

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.

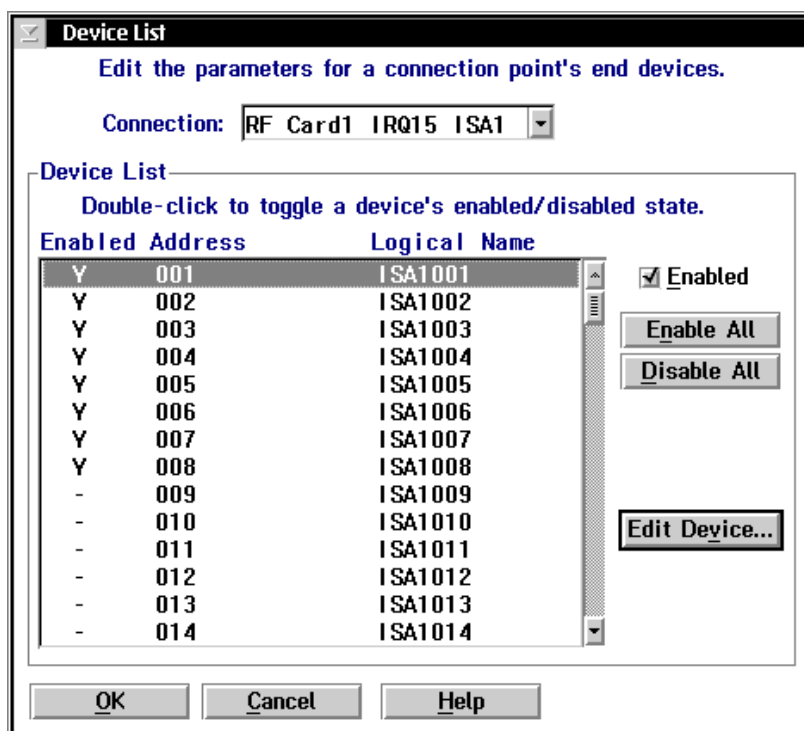
You can edit each device to change its logical name, device type, transaction IDs, and delivery responses.

Your controller is licensed to communicate with a fixed number of data collection devices (1-8, 1-24, 1-64, 1-128). The controller does not keep track of the number of devices you enable. You can enable all 128 devices. As each device sends messages to the controller, the controller logs its logical name. When the controller 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 controller, 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 RF devices

1. From the main menu, choose the type of communication you are using to connect the controller 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 connection points that you have configured appears. Select the RF controller 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 device whose individual parameters you want to edit and then choose Edit Device. For help, see, "Editing an RF Device" in the next section.
8. Choose OK to save your changes and return to the main menu.

Editing an RF Device

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

Model 200 Controller User's Manual

Field	Description	Value	Default
Auto-insert from device	This field provides a transaction ID for this device if it cannot put a transaction ID in its transactions.	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

To edit an RF device

1. In the Device List dialog box, select a device whose individual parameters you want to edit and choose Edit Device. The Device Parameters dialog box appears.
2. In the Logical name field, enter the logical name for the device that the network uses to identify it.
3. Enable or disable the check box that determines if the device can receive data from the network.
4. In the Device type field, click the down arrow on the right side of the field. A list of all the supported Intermec devices appears. Select the type of device you are configuring.
5. In the Auto-insert from device field, click the down arrow on the right side of the field. A list of all the transaction IDs appears. Select the transaction ID you want to use if this device cannot put a transaction ID in its transactions.

Note: All transactions from this terminal will be routed using this transaction ID.

6. In the To be routed to device field, click the down arrow on the right side of the field. A list of all the transaction IDs appears. Select the transaction ID you want to always route to this device.
7. In the Delivery Responses box, enter the messages you want to send to the transaction source.
 - In the Interactive response field, enter the message you want sent back to the source of the transaction if the delivery of the transaction for this device is successful in Interactive mode.
 - In the Hot standby field, enter the message you want sent back to the source of the transaction if the delivery of the transaction for this device is not immediately successful and is written to a Hot Standby file.
8. Choose OK to save your changes and return to the Controller Device List dialog box.

Connecting the Controller to the 2.4 GHz RF Network

The Model 200 Controller supports communications with Intermec's 2.4 GHz RF (UDP Plus) 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 controller. The illustration on the next page shows an example of a Model 200 Controller connected to a UDP Plus network.

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

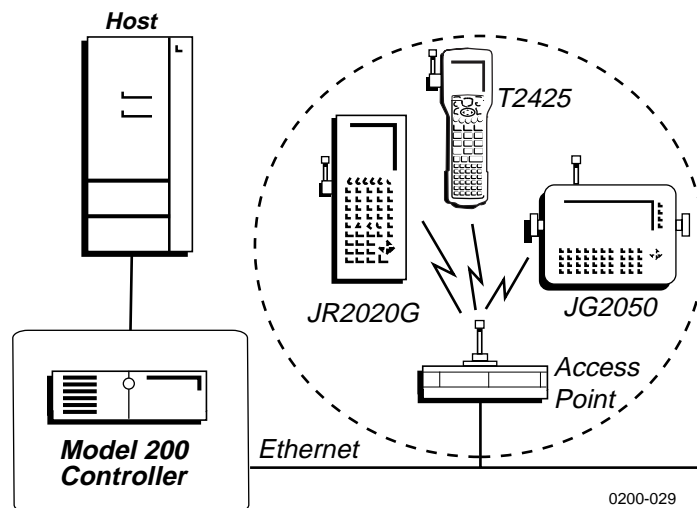
The UDP Plus network can consist of access points communicating with various JANUS devices and TRAKKER Antares terminals.

- 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.

Model 200 Controller User's Manual

- TRAKKER Antares terminals, such as the T2425, are terminals with network support. The controller supports these devices 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 controller communicates with these devices 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 Model 200 Controller Connected to the Intermec 2.4 GHz RF Network

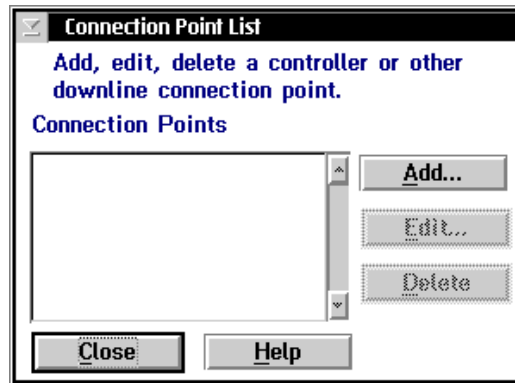


Configuring a UDP Plus Network

You need to configure the UDP Plus network if you want the Model 200 Controller to communicate with TRAKKER Antares terminals and JANUS devices that are using UDP Plus. Use the worksheets in Appendix E.

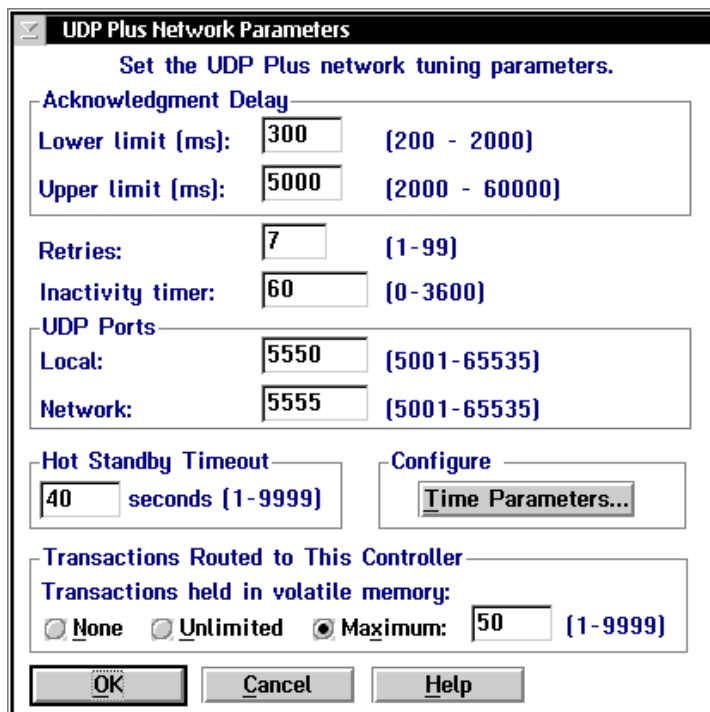
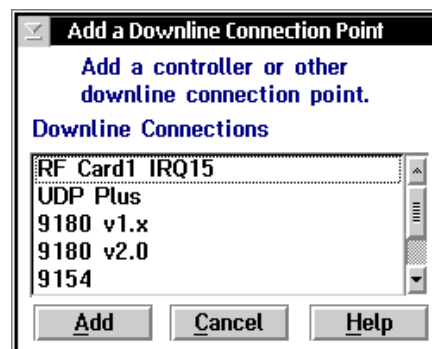
To configure a UDP Plus network

1. From the main menu, choose the type of communication you are using to connect the controller 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. Add, edit, or delete the UDP Plus network connection. For help, see “Adding a UDP Plus Network” in the next section.
5. Choose Close to close the dialog box and return to the main menu.



Adding a UDP Plus Network

1. In the Connection Point List dialog box, choose Add. The Add a Downline Connection Point dialog box appears.
2. In the Downline Connections list box, select UDP Plus.
3. Choose Add. The UDP Plus Network Parameters dialog box appears.



Field	Description	Value	Default
Lower limit	The minimum time in milliseconds the controller waits for an acknowledgment from the device before resending a transaction.	200 to 2000	300
Upper limit	The maximum time in milliseconds the controller waits for an acknowledgment from the device before resending a transaction.	2000 to 60000	5000
Retries	The number of times the controller 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 device can be "not responding" before it is set to "disconnected."	0 to 3600	60
Local	The UDP port through which the controller communicates with itself.	5001 to 65535	5550
Network	The UDP port that UDP Plus uses for communication.	5001 to 65535	5555
Hot Standby Timeout	The number of seconds the controller waits for a response from a device before it writes 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 controller keeps in RAM before it writes the transactions to a Hot Standby file.	None, Unlimited, Maximum	Maximum 50

4. In the Acknowledgment Delay box, set the minimum and maximum limits for how long the controller waits for an acknowledgment from the device before resending a transaction.
5. In the Retries field, enter the number of times the controller tries to transmit to a device before it sets the device to "not responding."
6. In the Inactivity timer field, enter the amount of time in minutes the device can be "not responding" before it is set to "disconnected."

Model 200 Controller User's Manual

7. In the Local field, enter the number of the port the controller uses to communicate with itself. This port must be different from the network port.
8. In the Network field, enter the number of the port that the UDP Plus network uses for communication. This number must match the network port set on the devices.
9. In the Hot Standby Timeout box, enter the number of seconds the controller waits for a response from a device before it writes transactions for the terminal to a Hot Standby file.
10. In the Transactions Routed to this Controller box, choose the number of transactions you want the controller to keep in RAM before it writes 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 controller has this number of transactions in RAM, it writes them to a file.
11. Set any time parameters for the UDP Plus network. For help, see "Setting the Time Parameters" later in this chapter.
12. Choose OK. The Setup for UDP Plus Terminals dialog box appears. Configure the IP addresses for the UDP Plus terminals. For help, see "Setting Up the UDP Plus Devices" in the next section.
13. Choose Close to return to the main menu.

Setting Up the UDP Plus Devices

The Model 200 Controller must know the IP address for every UDP Plus terminal that it may communicate with. You can either use the controller 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 controller. The controller 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 controller. However, the controller can help you generate an appropriate number of sequential IP addresses. Make sure that each IP address that the controller generates for a terminal matches an IP address on a terminal.

Setup For UDP Plus Terminals

Enable UDP Plus terminals by selecting a base logical name and starting IP address or domain.

Number of terminals to enable: 8 (0-128)

Terminal Addressing

Use DNS

Base logical name: UDPP

Starting IP address:

Subnet mask:

Domain:

OK Cancel Help

Model 200 Controller User's Manual

Field	Description	Value	Default
Number of terminals to enable	The number of IP addresses you want the controller to generate.	0 to 128	8
Use DNS	This check box determines if the controller uses a DNS server to translate the logical name to an IP address.	Check, Clear	Clear
Base logical name	The base name that the controller uses to create a unique logical name for each terminal.	1 to 13 alphanumeric characters	UDPP
Starting IP address	The starting IP address that the controller uses to assign IP addresses to each terminal.	xxx.xxx.xxx.xxx where xxx is a value between 0 and 255	None
Subnet mask	The subnet mask that the controller uses to validate the IP addresses.	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.	None	None

To set up the UDP Plus devices using a DNS server

1. In the Number of terminals to enable field, enter the number of logical names that you want the controller to generate.
2. Check the Use DNS check box.

Note: Before you enable this check box, you must first configure a DNS server in the DNS Configuration dialog box.

3. In the Base logical name field, enter the base name that the controller uses to create a unique logical name for each terminal. The controller appends a sequential 3-digit number to this name for each terminal.

4. In the Domain field, enter the name of the domain that all of the terminals are in.

Note: If you enable the Use DNS check box and you do not enter a domain, the controller searches the domains that are listed in the DNS Configuration dialog box.

5. Choose OK. The controller generates the logical names and you return to the Connection Point List dialog box.

To set up the UDP Plus devices using the controller to generate IP addresses

1. In the Number of terminals to enable field, enter the number of IP addresses that you want the controller to generate.
2. Clear the Use DNS check box.
3. In the Base logical name field, enter the base name that the controller uses to create a unique logical name for each terminal. The controller appends a sequential 3-digit number to this name for each terminal.
4. In the Starting IP address field, enter the starting IP address. The IP address must be a valid IP v4 address.
5. In the Subnet mask field, enter the subnet mask that the controller uses to validate the IP addresses. The controller verifies that they do not cross a subnet boundary.
6. Choose OK. The controller assigns valid sequential logical names and IP addresses to the terminals starting with the starting IP address and then you return to the Connection Point List dialog box.

Setting the Time Parameters

Use this dialog box to configure the broadcast and append parameters between the controller and the UDP Plus terminals.

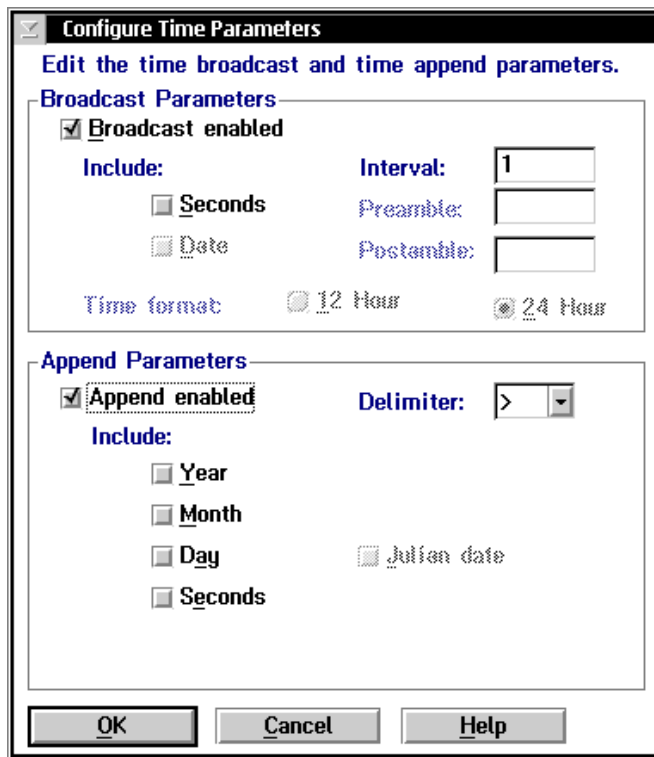
Broadcast Parameters These optional parameters allow the controller to broadcast a time at certain intervals to all UDP Plus terminals. These parameters synchronize the terminals with the controller.

Append Parameters These optional parameters configure the controller 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.



Field	Description	Value	Default
Broadcast enabled	This check box determines if the controller broadcasts a time to all terminals in the UDP Plus network.	Check, Clear	Clear
Interval	This field specifies how often in minutes the controller broadcasts the time.	0 to 99	1
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

Model 200 Controller User's Manual

Field	Description	Value	Default
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 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

To set the time parameters

1. From the UDP Plus Network Parameters dialog box, in the Configure box, choose Time Parameters. The Configure Time Parameters dialog box appears.
2. In the Broadcast Parameters box, enable or disable the time broadcast. A check in the Broadcast enabled check box means that time broadcast is enabled.
3. In the Interval field, enter how often (in minutes) you want the controller to do a time broadcast. If you set this field to 0, no time broadcast is made.
4. In the Append Parameters box, enable or disable the time append. A check in the Append enabled check box means that there is a time appended to all messages.
If you do not enable time append, skip to Step 8.
5. Enable or disable Include Year, Include Month, Include Day, Include Seconds. A check in the check box means that the part of the date or time is included in the time.
6. In the Delimiter field, click the down arrow on the right side of the field. A list of available delimiters appears. Select the delimiter that you want to use to separate the appended time from the transaction data.

7. Enable or disable Julian format. A check in the check box means that the date is in Julian format. Other date and time options are not used.
8. Choose OK to save your changes and return to the UDP Plus Network Parameters dialog box.

Identifying the UDP Plus Devices

You need to configure the Model 200 Controller for the logical names and IP addresses of the UDP Plus terminals that use it to communicate with the host. The device list contains the logical names of all 128 terminals. The first eight names are enabled and are configured as TRAKKER 2400s. You need to enable or disable the logical names of any other terminals that you want to be available to communicate with the host.

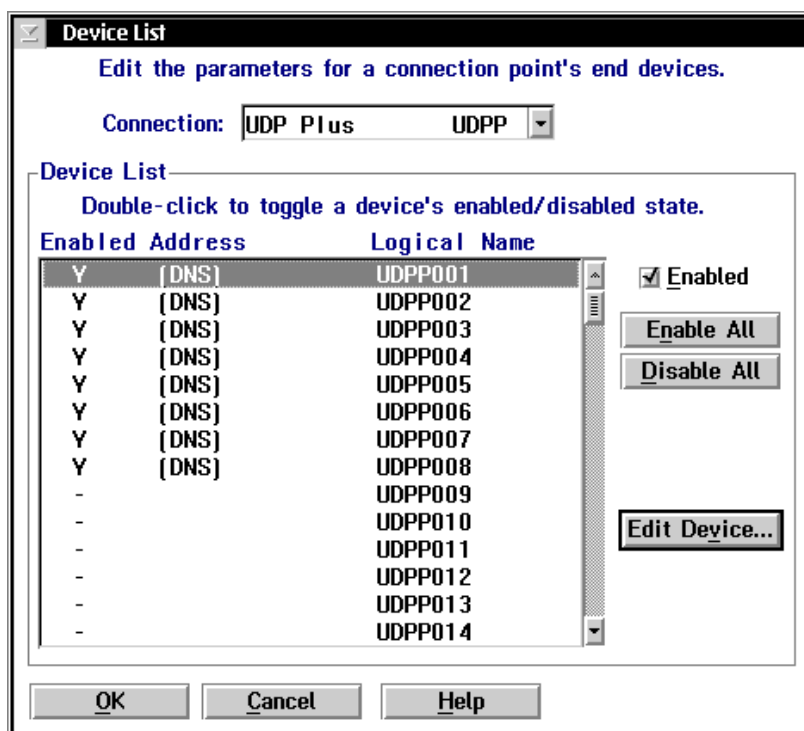
You can edit each terminal to change its logical name, IP address, device type, transaction IDs, and delivery responses. You can also use DNS to determine the device's IP address or to edit an IP address.

Your controller is licensed to communicate with a fixed number of terminals (1-8, 1-24, 1-64, 1-128). The controller does not keep track of the number of terminals you enable. You can enable all 128 terminals. As each terminal sends messages to the controller, the controller logs its logical name. When the controller 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 controller, the terminal license count number is reset.

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

To identify the UDP Plus terminals

1. From the main menu, choose the type of communication you are using to connect the controller 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 connection points that you have configured appears. Select UDP Plus.

5. To enable all 128 terminals, 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 128 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. For help, see “Editing a UDP Plus Device” in the next section.
8. Choose OK to save your changes and return to the main menu.

Editing a UDP Plus Device

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

Device Parameters

Edit the parameters for the selected device.

Logical name: UDPP001 Able to receive data

Device type: TRAKKER 2400 Addressing...

Physical address: n/a

Transaction ID...

Auto-insert from device: (none)

To be routed to device: (none)

Delivery Responses (if any)

Interactive response:

Hot standby:

OK Cancel Help

Model 200 Controller User's Manual

Field	Description	Value	Default
Logical name	The logical name of the terminal.	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 devices supported.	Predefined list	TRAKKER 2400
Auto-insert from this device	This field provides a transaction ID for this terminal if it cannot put a transaction ID in its transactions.	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

To edit a UDP Plus device

1. From the Device List dialog box, select the logical name of the terminal whose individual parameters you want to edit and choose Edit Device. The Device Parameters dialog box appears.
2. In the Logical name field, enter the logical name for the terminal that the network uses to identify it.
3. Enable or disable the check box that determines if the terminal can receive data from the network.

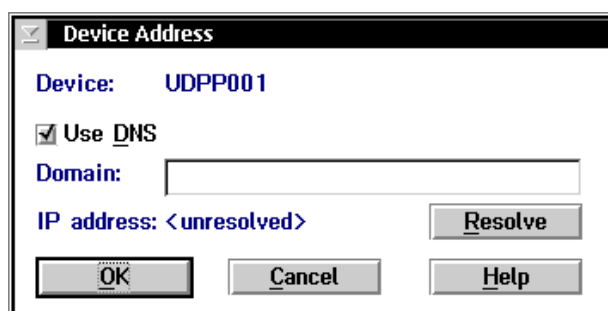
4. In the Device type field, click the down arrow on the right side of the field. A list of all the devices that can run in a UDP Plus network appears. Select a device.
5. In the Auto-insert from device field, click the down arrow on the right side of the field. A list of all the transaction IDs appears. Select the transaction ID you want to use if this terminal cannot put a transaction ID in its transactions.

Note: All transactions from this terminal are routed using this transaction ID.

6. In the To be routed to device field, click the down arrow on the right side of the field. A list of all the transaction IDs appears. Select the transaction ID you want to always route to this terminal.
7. In the Delivery Responses box, enter the messages you want to send to the transaction source.
 - In the Interactive response field, enter the message you want sent back to the source of the transaction if the delivery of the transaction for this terminal is successful.
 - In the Hot standby field, enter the message you want sent back to the source of the transaction if the delivery of the transaction for this terminal is not immediately successful and is written to a Hot Standby file.
8. Resolve or edit the terminal IP address. For help, see “Determining a UDP Plus Device’s IP Address” or “Editing a UDP Plus Device’s IP Address” later in this chapter.
9. Choose OK to save your changes and return to the Device List dialog box.

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, from the Device Parameters dialog box, choose Addressing. The Device Address dialog box appears.

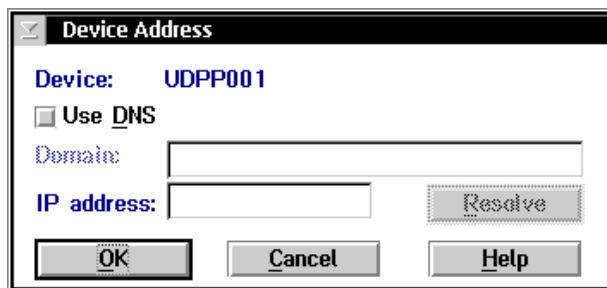


To determine a terminal's IP address

- (Optional) In the Domain field, enter the specific domain that contains the terminal.
- 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.

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.

***Connecting to the 9180 and the
Intermec CrossBar Network***

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

Chapter Checklist

Done?	Task	Page
<input type="checkbox"/>	Install all your external Intermec controllers.	None
<input type="checkbox"/>	Identify all the external controllers on the Model 200 Controller.	4-4
<input type="checkbox"/>	Configure each external controller connected to the Model 200 Controller.	4-7
<input type="checkbox"/>	Set the time parameters for each external controller.	4-15
<input type="checkbox"/>	Identify all the CrossBar devices connected to external controllers.	4-19
<input type="checkbox"/>	Edit the CrossBar devices.	4-21

***Note:** In order for the 9181 Base Radio Units (BRUs) to communicate with a 9180 Network Controller that is connected to the Model 200 Controller, you need to configure these BRUs using the 9180 configuration menu. Refer to your 9180 user's manual.*

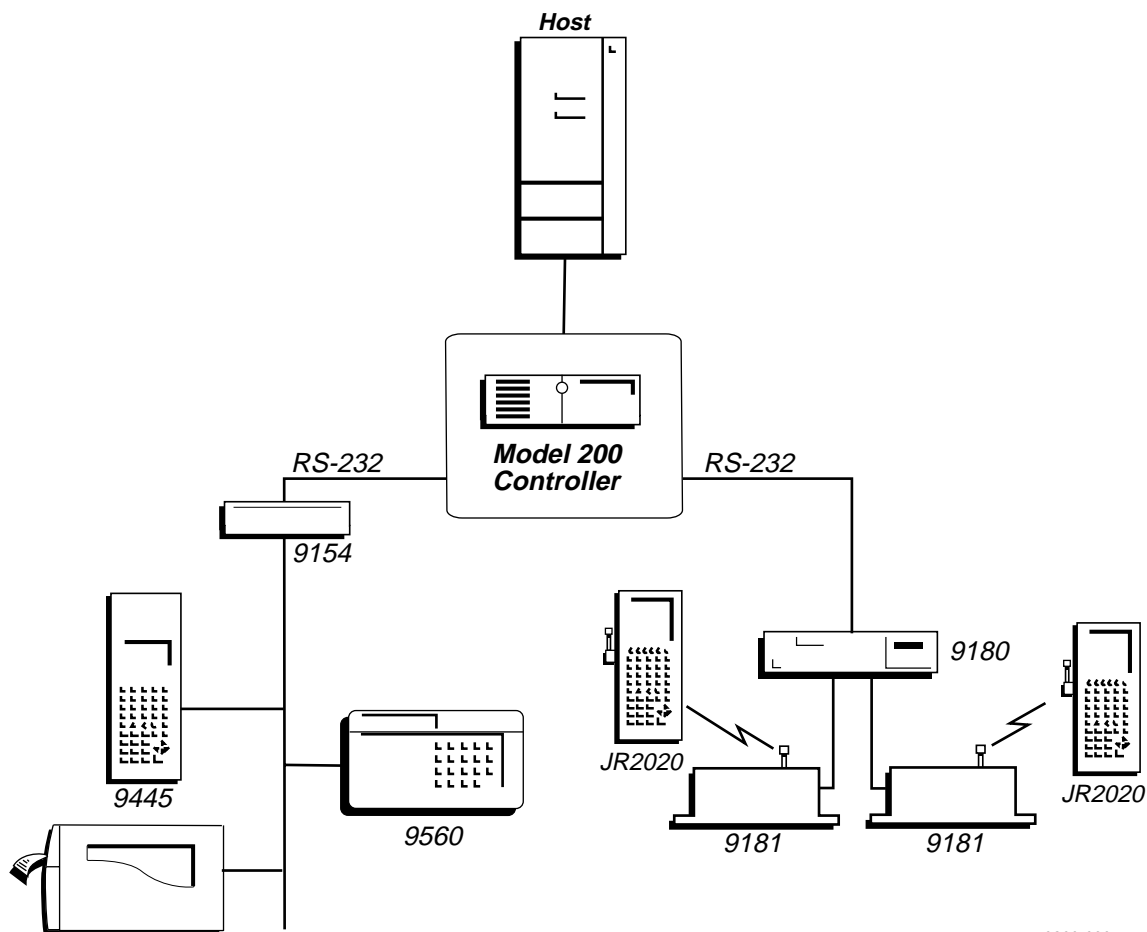
If you already understand and have performed these tasks, connect the controller to your Intermec RF network or host environment as described in these chapters:

- Chapter 3, "Connecting to the Intermec RF Network"
- Chapter 5, "Connecting to an Ethernet/Token Ring Network"
- Chapter 6, "Connecting to a Coaxial/Twinaxial Network"
- Chapter 7, "Connecting to an SDLC Network"

Configuring an External Intermec Controller

An external Intermec controller is a 9180 Network Controller, 9161 Port Concentrator, or a 9154 Multi-Drop Line Controller that is connected to the Model 200 Controller through a serial port. The following illustration is an example of a controller connected to a 9180 and a CrossBar network.

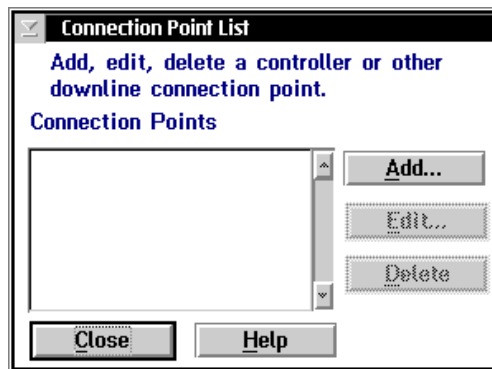
Example: The Model 200 Controller Connected to a 9180 and CrossBar Network



0200-030

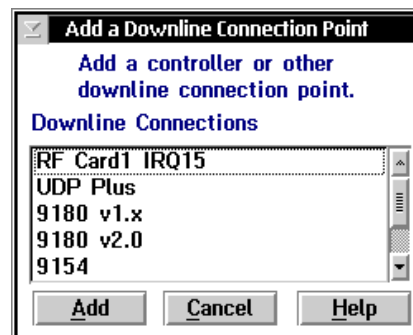
To configure the controller to work with an external Intermec controller

1. From the main menu, choose the type of communication you are using to connect the controller 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. Add, edit, or delete external Intermec controllers. For help, see “Adding a Controller” in the next section.
5. Choose Close to close the dialog box and return to the main menu.



Adding a Controller

1. In the Connection Point List dialog box, choose Add. The Add a Downline Connection Point dialog box appears.
2. In the Downline Connections list box, select the controller that you want to add.
3. Choose Add. The setup dialog box for the controller appears.
4. Configure the controller. For help, see “About the Controller Parameters” in the next section and then see the appropriate section for your controller.



5. Set any time parameters for the controller. For help, see "Setting the Time Parameters" later in this chapter.
6. 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 external 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. Use the worksheets in Appendix E.

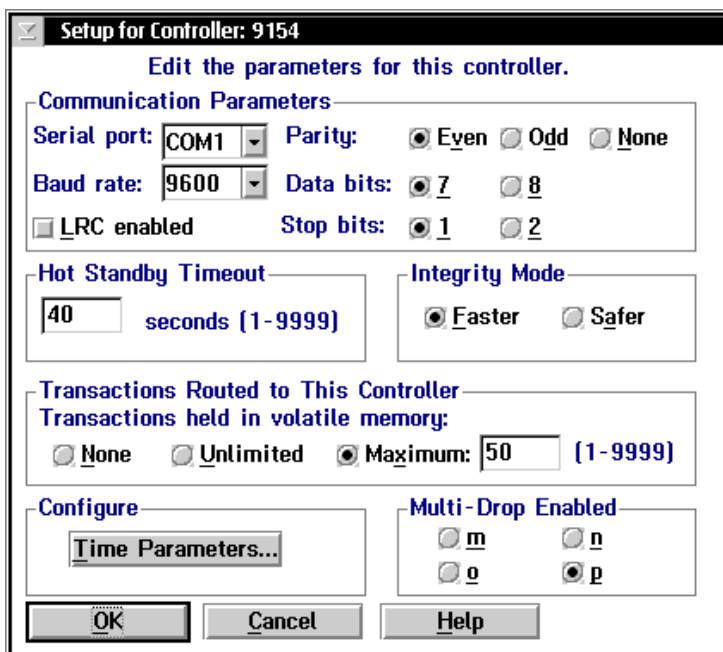
Communication Parameters These required parameters define how the serial port on the Model 200 Controller communicates with the controllers that are connected to it. Make sure that any communication parameters that you define on the Model 200 Controller are the same as the parameters set on the external Intermec controller.

Hot Standby Timeout This required parameter sets the amount of time in seconds the Model 200 Controller waits after delivering a transaction to a device to receive an acknowledgment for the transaction. If it does not receive an acknowledgment, the controller writes all transactions for the device to a Hot Standby file. The device receives its transactions from the Hot Standby file either when it sends an acknowledgment to the most recently delivered transaction or when it sends a system transaction. Before the device becomes interactive again, it receives all the transactions, from oldest to newest, that are in its Hot Standby file.

Integrity Mode This mode determines the amount of transaction verification that the Model 200 Controller performs. In Faster mode, the Model 200 Controller acknowledges the transaction as soon as it receives the transaction from the external Intermec controller. In Safer mode, the Model 200 Controller acknowledges the transaction only after it is stored in a Hot Standby file. In Safer mode, transaction throughput is slower because the controller cannot accept another transaction from the device until it verifies the previous one.

Multi-Drop Enabled This required parameter defines which Multi-Drop line the external Intermec controller uses.

Adding a 9154 Controller



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

Model 200 Controller User's Manual

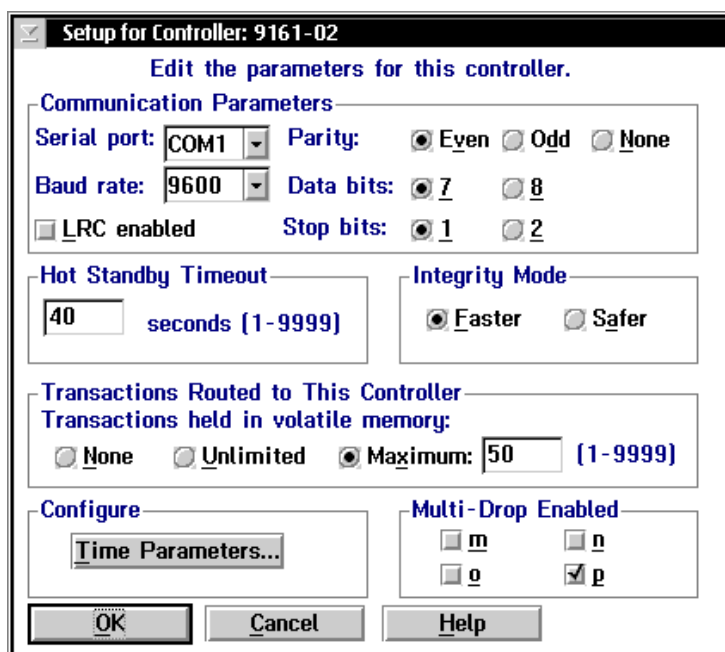
Field	Description	Value	Default
Stop bits	The number of bits to use for setting communications protocol.	1, 2	1
Hot Standby Timeout	The number of seconds the Model 200 Controller waits for a response from the 9154 controller before it places the 9154 controller in Hot Standby mode.	1 to 9999	40
Integrity Mode	This mode determines the amount of transaction verification that the Model 200 Controller performs.	Faster, Safer	Faster
Transactions held in volatile memory	The number of transactions the controller keeps in volatile RAM before it begins to write them to a Hot Standby file.	None, Unlimited, Maximum	Maximum 50
Multi-Drop Enabled	The Multi-Drop line that the 9154 controller uses.	m, n, o, p	p

To edit the parameters for a 9154 controller

1. In the Connection Point List dialog box, select the 9154 controller and then choose Add. The Setup for Controller dialog box appears.
2. In the Serial port field, click the down arrow on the right side of the field. A list of available COM ports appears. Select the COM port on the controller that connects to the 9154 controller.
3. In the Baud rate field, click the down arrow on the right side of the field. A list of baud rates appears. Select the baud rate you want to use to communicate with the 9154 controller.
4. Enable or disable the LRC check box. The LRC provides additional data integrity.
5. Choose the parity, data bits, and stop bits. These parameters must match the parameters configured in the 9154 controller.

6. In the Hot Standby Timeout box, enter the number of seconds you want the Model 200 Controller to wait for a response from the 9154 controller before it places the 9154 controller in Hot Standby mode.
7. In the Integrity Mode box, choose the mode that determines the amount of transaction verification the Model 200 Controller performs.
8. In the Transactions Routed to This Controller box, choose the number of transactions you want the controller to keep in RAM before it writes them to a Hot Standby file.
 - Choose None if you want the transaction always written to the file.
 - Choose Unlimited if you don't 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 controller has this number of transactions in RAM, it writes them to a file.
9. Choose Time Parameters to set the time parameters for the 9154 controller. For help, see "Setting the Time Parameters" later in this section.
10. In the Multi-Drop Enabled box, choose the Multi-Drop line that the 9154 controller supports.
11. Choose OK to save your changes and return to the Connection Point List dialog box.

Adding a 9161 Controller



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

Field	Description	Value	Default
Stop bits	The number of bits to use for setting communications protocol.	1, 2	1
Hot Standby Timeout	The number of seconds the Model 200 Controller waits for a response from the 9161 controller before it places the 9161 controller in Hot Standby mode.	1 to 9999	40
Integrity Mode	This mode determines the amount of transaction verification the Model 200 Controller performs.	Faster, Safer	Faster
Transactions held in volatile memory	The number of transactions the controller keeps in volatile RAM before it begins to write them to a Hot Standby 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

To edit the parameters for a 9161 controller

1. In the Connection Point List dialog box, select the 9161 controller and then choose Add. The Setup for Controller dialog box appears.
2. In the Serial port field, click the down arrow on the right side of the field. A list of available COM ports appears. Select the COM port on the controller that connects to the 9161 controller.
3. In the Baud rate field, click the down arrow on the right side of the field. A list of baud rates appears. Select the baud rate you want to use to communicate with the 9161 controller.
4. Enable or disable the LRC check box. The LRC provides additional data integrity.
5. Choose the parity, data bits, and stop bits. These parameters must match the parameters configured on the 9161 controller.

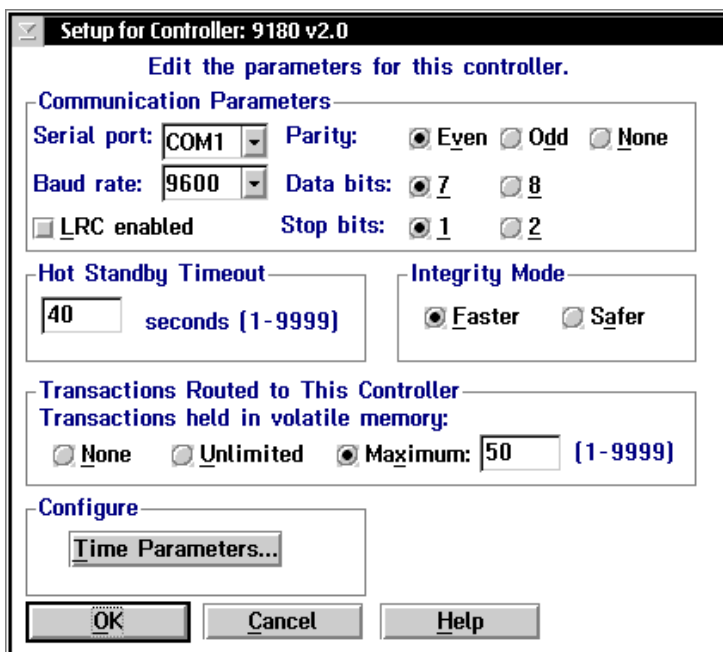
Model 200 Controller User's Manual

6. In the Hot Standby Timeout box, enter the number of seconds you want the Model 200 Controller to wait for a response from the 9161 controller before it places the 9161 controller in Hot Standby mode.
7. In the Integrity Mode box, choose the mode that determines the amount of transaction verification the Model 200 Controller performs.
8. In the Transactions Routed to This Controller box, choose the number of transactions you want the controller to keep in RAM before it writes them to a Hot Standby file.
 - Choose None if you want the transaction always written to the file.
 - Choose Unlimited if you don't 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 controller has this number of transactions in RAM, it writes them to a file.
9. Choose Time Parameters to set the time parameters for the 9161 controller. For help, see "Setting the Time Parameters" later in this section.

Note: Intermec recommends that you enable the time append feature when you set the time parameters. If you do not enable this feature, you may see a "protocol error occurred" message in the error log.

10. (9161-02 only) In the Multi-Drop enabled box, choose the Multi-Drop lines that the 9161-02 controller supports (up to four).
11. Choose OK to save your changes and return to the Connection Point List dialog box.

Adding a 9180 Controller



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

Model 200 Controller User's Manual

Field	Description	Value	Default
Stop bits	The number of bits to use for setting communications protocol.	1, 2	1
Hot Standby Timeout	The number of seconds the Model 200 Controller waits for a response from the 9180 controller before it places the 9180 controller in Hot Standby mode.	1 to 9999	40
Integrity Mode	This mode determines the amount of transaction verification the Model 200 Controller performs.	Faster, Safer	Faster
Transactions held in volatile memory	The number of transactions the controller keeps in volatile RAM before it begins to write them to a Hot Standby file.	None, Unlimited, Maximum	Maximum 50

To edit the parameters for a 9180 controller

1. In the Connection Point List dialog box, select the 9180 controller and then choose Add. The Setup for Controller dialog box appears.
2. In the Serial port field, click the down arrow on the right side of the field. A list of available COM ports appears. Select the COM port on the controller that connects to the 9180 controller.
3. In the Baud rate field, click the down arrow on the right side of the field. A list of baud rates appears. Select the baud rate you want to use to communicate with the 9180 controller.
4. Enable or disable the LRC check box. The LRC provides additional data integrity.
5. Choose the parity, data bits, and stop bits. These parameters must match the parameters configured for the 9180 controller.
6. In the Hot Standby Timeout box, enter the number of seconds you want the Model 200 Controller to wait for a response from the 9180 controller before it places the 9180 controller in Hot Standby mode.
7. In the Integrity Mode box, choose the mode that determines the amount of transaction verification the Model 200 Controller performs.

8. In the Transactions Routed to This Controller box, choose the number of transactions you want the controller to keep in RAM before it writes them to a Hot Standby file.
 - Choose None if you want the transaction always written to the file.
 - Choose Unlimited if you don't 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 controller has this number of transactions in RAM, it writes them to a file.
9. Choose Time Parameters to set the time parameters for the 9180 controller. For help, see "Setting the Time Parameters" later in this section.
10. Choose OK to save your changes and return to the Connection Point List dialog box.

Setting the Time Parameters

Use this dialog box to configure the time broadcast and time append parameters. These time parameters synchronize the external Intermec controllers with their devices. In the System Parameters dialog box, you can set a time synchronization parameter that synchronizes the time on the Model 200 Controller with its external Intermec controllers. If the external 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 external Intermec controller to all data collection devices connected to it. These parameters synchronize the data collection devices with the controller.

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

HH:MM:SS

Model 200 Controller User's Manual

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 external Intermec controller and the data collection device itself. If it is enabled on both, two timestamps are appended to incoming data.

Configure Time Parameters

Edit the time broadcast and time append parameters.

Broadcast Parameters

Broadcast enabled

Include: Interval:

Seconds Preamble:

Date Postamble:

Time format: 12 Hour 24 Hour

Append Parameters

Append enabled Interval:

Include:

Year

Month

Day

Seconds

Record day rollover

OK Cancel Help

Field	Description	Value	Default
Broadcast enabled	This check box determines if the external Intermec controller broadcasts its 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 sends the time broadcasts.	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.	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.	0 to 99	1

To configure the time parameters

1. From the Setup for Controller dialog box, in the Time Parameters box, choose Configure. The Configure Time Parameters dialog box appears.
2. In the Broadcast Parameters box, enable or disable the time broadcast. A check in the Broadcast enabled check box means that time broadcast is enabled.

If you do not enable time broadcast, skip to Step 8.

3. Enable or disable including seconds in the time. A check in the Include Seconds check box means that seconds are added.
4. Enable or disable including the date in the time. A check in the Include Date check box means that the date is added.
5. Choose 12 Hour or 24 Hour time format.
6. In the Interval field, enter how often you want the controller to do a time broadcast. If you set this field to 0, no time broadcast is made.

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

7. In the Preamble and Postamble fields, enter a short message you want to add before or after the time.
8. In the Append Parameters box, enable or disable the time append. A check in the Append enabled check box means a timestamp is added to messages at a certain interval.

If you do not enable time append, skip to Step 12.

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.

9. Enable or disable Include Seconds. A check in the check box means that seconds are included in the time stamp.
10. Enable or disable placing a timestamp in the buffer for the host at midnight. A check in the Record day rollover check box adds the time stamp.

11. In the Interval field, enter how often you want the controller to append a timestamp on messages from devices. If you set this field to 0, every message from a device will have a timestamp.
12. Choose OK to save your changes and return to the Setup for Controller dialog box.

Identifying the CrossBar Devices

The Model 200 Controller needs to know the addresses of all the devices that use it to communicate with the host. This section explains how to configure the controller for the CrossBar devices.

The device list is automatically populated with device addresses as you configure the external 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 controller 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 controller does not keep track of the number of devices you enable. You can enable all 128 devices. As each device sends messages to the controller, the controller logs its address. When the controller logs the maximum number of addresses that your terminal license allows, it will not accept messages from any new addresses.

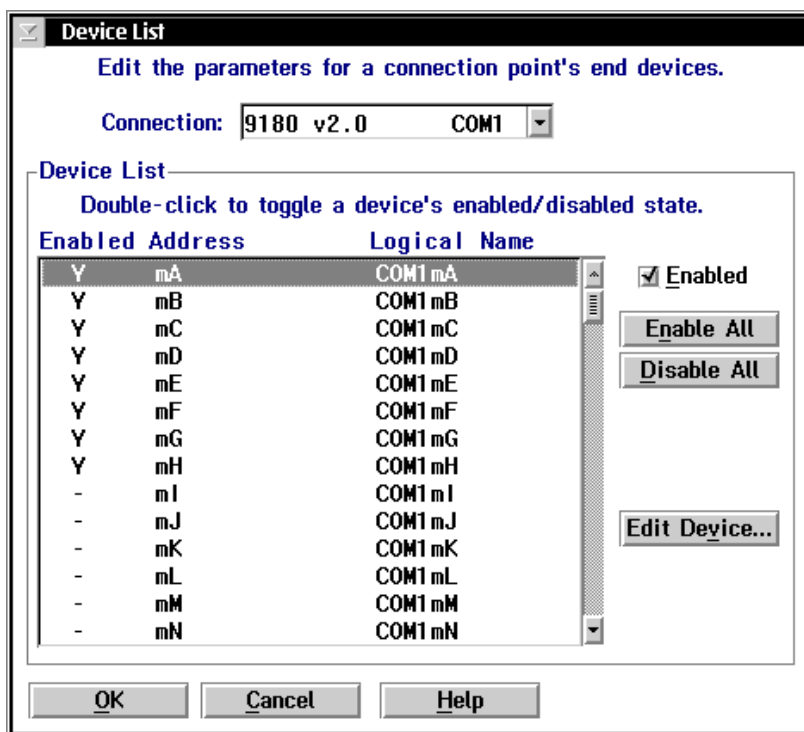
If you need to upgrade your terminal license, contact your local Intermec representative.

To identify CrossBar devices

1. From the main menu, choose the type of communication you are using to connect the controller to the host.
2. Choose Downline Network. Two buttons, Connection Points and Downline Devices, appear.

Model 200 Controller User's Manual

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.



5. Select the controller whose devices you want to configure. The Device List displays the status, physical 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 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

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 display, it is checked, else it is cleared.

Model 200 Controller User's Manual

Field	Description	Value	Default
Device type	This list box contains all the current Intermec devices supported by the Model 200 Controller.	Predefined	J2020
Physical address	This read-only field displays the physical address of the device.	Predefined	Predefined
Auto-insert from device	This field adds a transaction ID to end devices that cannot put a transaction ID in the transactions they send.	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

To edit a CrossBar device

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

1. From the Device List dialog box, select a device whose individual parameters you want to edit and choose Edit Device. The Device Parameters dialog box appears.
2. In the Logical name field, enter the logical name for the device that the network uses to identify it.
3. Enable or disable the check box that determines if the device can receive data from the system.

4. In the Device type field, click the down arrow on the right side of the field. A list of all the supported Intermec devices appears. Select the type of device you are configuring.
5. In the Auto-insert from device field, click the down arrow on the right side of the field. A list of all the transaction IDs appears. Select the transaction ID you want to use if the device cannot put a transaction ID in the transactions it sends.

Note: All transactions from this terminal will be routed using this transaction ID.

6. In the To be routed to device field, click the down arrow on the right side of the field. A list of all transaction IDs appears. Select the transaction ID you want to always route to this device.
7. (Optional) In the Delivery Responses box, enter the messages you want to send to the transaction source.
 - In the Interactive response field, enter the message you want sent back to the source of the transaction if the delivery of the transaction for this device is successful in Interactive mode.
 - In the Hot standby field, enter the message you want sent back to the source of the transaction if the delivery of the transaction for this device is not immediately successful and is written to a Hot Standby file.
8. Choose OK to save your changes and return to the Device List dialog box.

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.

5

***Connecting to an Ethernet/
Token Ring Network***

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

Chapter Checklist

Done?	Task	Page
<input type="checkbox"/>	Install the controller in the Ethernet network.	5-4
<input type="checkbox"/>	Install the controller in the token ring network.	5-5
<input type="checkbox"/>	Use the GUI to configure each Ethernet and token ring card for TCP/IP.	5-6
	Or,	
<input type="checkbox"/>	Use the GUI to configure each Ethernet and token ring card for IEEE 802.2.	5-16
<input type="checkbox"/>	Save your run-time configuration.	5-19

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

- Chapter 6, "Connecting to a Coaxial/Twinaxial Network"
- Chapter 7, "Connecting to an SDLC Network"
- Chapter 8, "Using Terminal Emulation"
- Chapter 9, "Using Peer-to-Peer Applications"
- Chapter 10, "Using Terminal Sessions"

Installing the Controller in an Ethernet Network

Your Model 200 Controller contains a 10/100 Mbps Ethernet card. The card automatically switches between 10 Mbps and 100 Mbps. The default configuration for the Ethernet card is 10BaseT or 100BaseTX.

Before you can configure the Model 200 Controller, you need to install it in your network.

Equipment

- An Ethernet connection where you can connect the controller.
- A cable to connect the controller to the connection. For a 10BaseT or 100BaseTX connection, you use RJ-45.

To install the controller



0200-099

1. Locate the slot that contains the Ethernet card(s) on the rear panel of your controller. The figure on the left shows the connector for the Ethernet card.
2. Insert one end of the cable into the appropriate Ethernet port on the card and the other end into the Ethernet connection.

Installing the Controller in a Token Ring Network

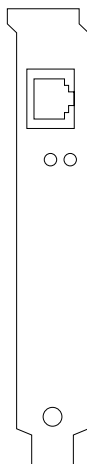
Before you can configure the Model 200 Controller, you need to install it in your network.

Equipment

- A token ring connection where you can connect the controller.
- A cable to connect the controller 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 controller



1. Locate the slot that contains the token ring card on the rear panel of your controller. The token ring card is the card that is furthest right when you are looking at the rear panel. 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.

0200-019

Configuring the Network Adapter Card for TCP/IP

After you install the Model 200 Controller, you need to turn it on and configure its network adapter cards. Ethernet and token ring cards support both TCP/IP and IEEE 802.2 protocols. Use the worksheets in Appendix E.

To configure the card for TCP/IP, either use a Dynamic Host Configuration Protocol (DHCP) server to provide the controller 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 TCP/IP information You can configure the controller to be a DHCP client in a network that uses a DHCP server. The server can provide the controller 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 controller supports only one network adapter card that is using DHCP.

For each TRAKKER Antares terminal, you must scan the Enable DHCP bar code if you want it to be able to look for the controller that is a DHCP client.

Enable DHCP



\$+NI0

Disable DHCP



\$+NI1

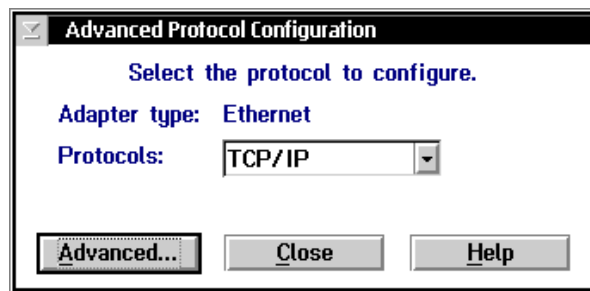
Note: To use DHCP across routers in your network, the routers must have the DHCP relay agent configured and enabled. For help, see your router user's manual.

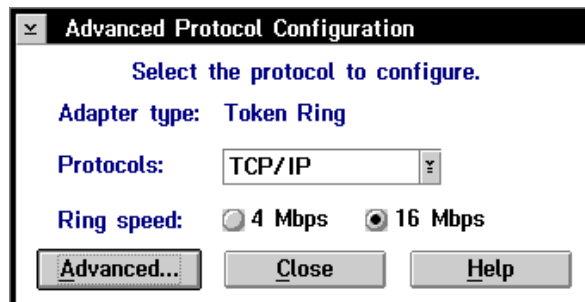
Enter the TCP/IP information manually From your network administrator, obtain a valid IP v4 address for each Ethernet and token ring card. You may also need to know the controller's local host name and the subnet mask. If you have two or more cards communicating using TCP/IP, each card must be on a different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

If you are going 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 controller to the host.
2. Choose Local Network Adapter. Five buttons for different network adapter card types appear.
3. Choose Ethernet or token ring. The Advanced Protocol Configuration dialog box appears. Make sure the Adapter type is correct.

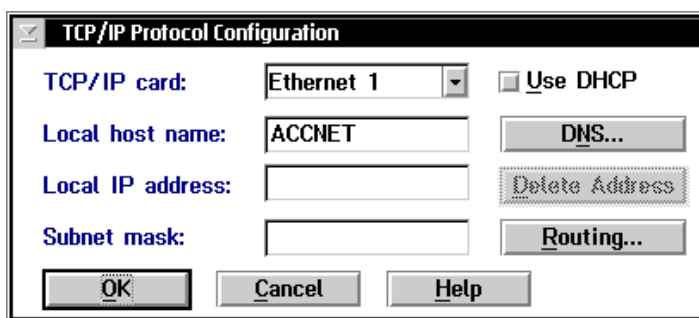
Advanced Protocol Configuration Dialog Box for the Ethernet Card

Advanced Protocol Configuration Dialog Box for the Token Ring Card

4. In the Protocols field, click the down arrow on the right side of the field. Select TCP/IP.

Model 200 Controller User's Manual

5. (Token ring only) Choose the ring speed of your token ring network. The default ring speed is 16 Mbps.
6. Choose Advanced. The TCP/IP Protocol Configuration dialog box appears.



Field	Description	Value	Default
TCP/IP card	The card that you are configuring.	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 controller (host) to the network.	1 to 12 alphanumeric characters	ACCNET
Local IP address	The unique IP address that identifies the Ethernet card in the controller (host) to the network.	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

To configure the TCP/IP protocol

1. In the TCP/IP Protocol Configuration dialog box, click the down arrow on the right side of the TCP/IP card field. A list of Ethernet cards that are installed in your controller appears. Select the card you want to configure.

Note: If you have two or more 10 Mbps Ethernet cards, Ethernet 1 is the Ethernet card that is in the slot the furthest left if you are facing the controller front panel. If you have a 100 Mbps Ethernet card, it is Ethernet 1.

2. To enable DHCP, check the Use DHCP check box. Go to Step 6.
Or, to disable DHCP, clear the Use DHCP check box. Go to Step 3.
3. (Optional) In the Local host name field, enter a meaningful TCP/IP host name for the controller.
4. In the Local IP address field, enter the address that identifies this Ethernet card in the controller (host) to the network. This IP address must be a valid IP v4 address.
5. In the Subnet mask field, enter the mask used in the IP protocol layer to separate the subnet address from the local IP address.
6. Choose DNS to configure DNS servers that resolve name/IP address conversions. The DNS Configuration dialog box appears. For help, see "Using DNS" in the next section.
7. Choose Routing to enable or disable the routing daemon and to set up routing tables for the network. The Routing Table Entries Configuration dialog box appears. For help, see "Using the Routing Daemon" and "Configuring Routing Tables" later in this chapter.
8. Choose OK to save your changes and return to the Advanced Protocol Configuration dialog box.
9. Choose Close to close the dialog box and return to the main menu.

Using DNS

The controller 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 controller automatically obtains these 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 controller with the IP addresses for 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 controller locate and connect to TCP/IP hosts that are administered by a DHCP server. The controller 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.

The screenshot shows a dialog box titled "DNS Configuration". It contains two sections:

- Name Server Addresses:** "Enter the IP addresses of your DNS name servers [up to 3].". It features an input field, an "Add -->" button, a list box, and "Move Up", "Move Down", and "Delete" buttons.
- Domain Names:** "Enter the domains to be searched [up to 6].". It features an input field, an "Add -->" button, a list box, and "Move Up", "Move Down", and "Delete" buttons.

At the bottom of the dialog are three buttons: "OK", "Cancel", and "Help".

Field	Description	Value	Default
Name Server Addresses	List of IP addresses of DNS servers (in search order) that are used to resolve TCP/IP host names.	xxx.xxx.xxx.xxx where xxx is a value between 0 and 255	None
Domain Names	List of internet domains (in search order) that are searched when an abbreviated TCP/IP host name is entered.	256 alphanumeric characters, dash	None

To use DNS

1. From the TCP/IP Protocol Configuration dialog box, choose DNS. The DNS Configuration dialog box appears.
2. In the Name Server Addresses box, enter the IP address of a DNS server that you want to use to resolve TCP/IP host names.
3. Choose Add. The address is added to the list box to the right.
4. Repeat Steps 2 and 3 until you have added the IP addresses of the DNS servers you want to use. You can enter up to three IP addresses.
5. Verify that the DNS servers are listed in the order in which you want to use them. If the first one in the list fails to respond, the next one in the list is used. To move a DNS server up or down in the list, select it and choose Move Up or Move Down.

Note: If the first DNS server does not respond, then the controller uses the next IP address. However, if the DNS server responds, even if the response is a "not resolved" response, the search stops.

6. Remove any DNS server that you do not want to use by selecting it and choosing Delete.
7. In the Domain Names box, enter the domain that you want to search when a shortened name is entered. The controller appends the complete domain name before attempting to use the DNS server to resolve the IP address.
8. Choose Add. The name is added to the list box to the right.

9. Repeat Steps 7 and 8 until you have added the domain names of the DNS servers you want to use. You can enter up to six domain names.
10. Verify that the domain names are listed in the order that you want them searched through when attempting to resolve a host name. To move a domain name up or down in the list, select it and choose Move Up or Move Down.
11. Remove any domain name that you do not want searched by selecting it and choosing Delete.
12. Choose OK to save your changes and return to the TCP/IP Protocol Configuration dialog box.

Clearing the IP Address and Subnet Mask

When you configure a card for TCP/IP, you must enter the IP address and subnet mask or use DHCP. The Delete Address button lets you clear the Local IP address and Subnet mask fields. By clearing these two fields, you disable TCP/IP on this local network adapter card.

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 TCP/IP network adapter card defined, you must delete the UDP Plus network before you can clear the IP address and subnet mask.

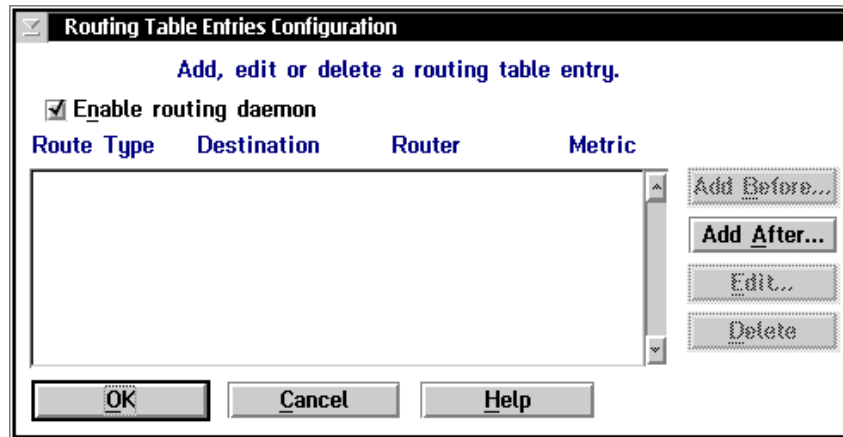
Using the Routing Daemon

The routing daemon tells the Model 200 Controller 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. For help, see "Configuring Routing Tables" later in this section.
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 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.

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

To add a routing table entry

1. From the TCP/IP Protocol Configuration dialog box, choose Routing. The Routing Table Entries Configuration dialog box appears.
2. Select a route in the list box and choose Add before or Add after. The Configure Route dialog box appears.

Note: If the route that you are configuring is the first route, choose Add after.

3. In the Route type field, click the down arrow on the right side of the field. A list box appears that contains the different types of routes you can use. Select a route type.
4. (N, S, H route types only) In the Route destination field, enter the IP address of the destination.
5. In the Router field, enter the IP address of the router for the destination address.
6. In the Metric count field, enter the number of hops it takes to get to the destination.
7. Choose OK to save your changes and return to the Routing Table Entries Configuration dialog box.

Configuring the Network Adapter Card for IEEE 802.2

After you install the Model 200 Controller, 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. Use the worksheets in Appendix E.

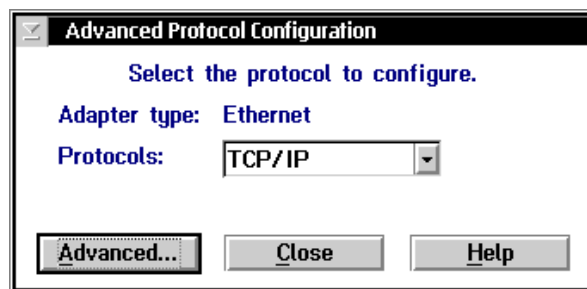
To configure the card for IEEE 802.2, you need to know the network adapter address, Ethernet driver support, and the maximum number of link stations. This protocol is used for IBM connectivity. It coexists with TCP/IP in the network adapter card.

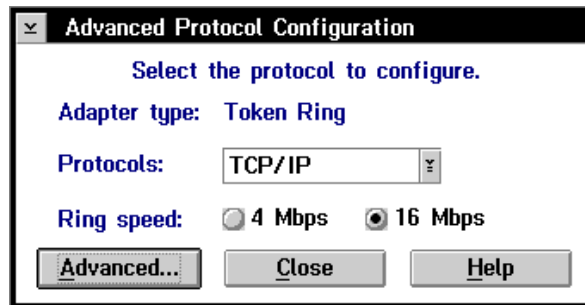
Auto Calc button You can choose the Auto Calc button instead of entering a number for the maximum link stations if you want the server to determine the optimal values for this field based on how it is configured.

To configure the network adapter card

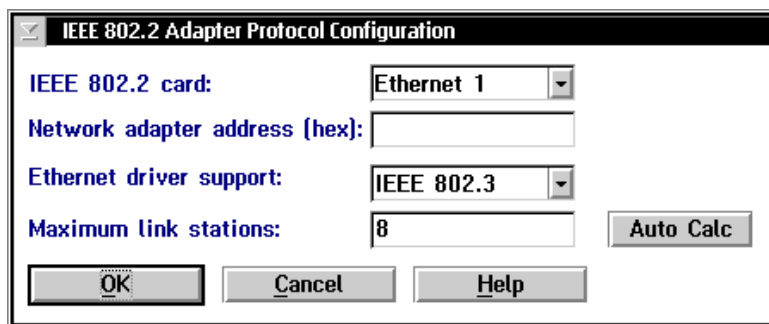
1. From the main menu, choose the type of communication you are using to connect the controller to the host.
2. Choose Local Network Adapter. Five buttons for different network adapter card types appear.
3. Choose Ethernet or token ring. The Advanced Protocol Configuration dialog box appears. Make sure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

Advanced Protocol Configuration Dialog Box for the Ethernet Card



Advanced Protocol Configuration Dialog Box for the Token Ring Card

4. In the Protocols field, click the down arrow on the right side of the field. Select IEEE 802.2.
5. (Token ring only) Choose the ring speed of your token ring network. The default ring speed is 16 Mbps.
6. Choose Advanced. The IEEE 802.2 Adapter Protocol Configuration dialog box appears.



Model 200 Controller User's Manual

Field	Description	Value	Default
IEEE 802.2 card	The 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 FFFFFFFF	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.	Based on how the controller is configured.	8

To configure the IEEE 802.2 protocol

1. In the IEEE 802.2 Adapter Protocol Configuration dialog box, click the down arrow on the right side of the IEEE 802.2 card field. Select the card you want to configure.

Note: If you have two or more 10 Mbps Ethernet cards, Ethernet 1 is the Ethernet card that is in the slot the furthest left if you are facing the controller front panel. If you have a 100 Mbps Ethernet card, it is Ethernet 1.

2. (Optional) In the Network adapter address field, enter a locally administered MAC address. This address overrides the one on the card. To see the default address, view the run-time configuration.
3. In the Ethernet driver support field, click the down arrow on the right side of the field. Select IEEE 802.3 or Ethernet DIX.
4. In the Maximum link stations field, enter the maximum number of link stations that can exist for all SAPs concurrently.

Or, choose Auto Calc if you want the controller to determine the optimal values for this field based on how the controller is configured.

5. Choose OK to save your changes and return to the Advanced Protocol Configuration dialog box.

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.

Connecting to a Coaxial/Twinaxial Network

This chapter describes how to connect the controller 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
<input type="checkbox"/>	Install the controller.	6-4
<input type="checkbox"/>	Use the GUI to configure the coaxial card for the coaxial network.	6-5
	Or,	
	Use the GUI to configure the twinaxial card for the twinaxial network.	6-6

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

- Chapter 5, "Connecting to an Ethernet/Token Ring Network"
- Chapter 7, "Connecting to a SDLC Network"
- Chapter 8, "Using Terminal Emulation"
- Chapter 9, "Using Peer-to-Peer Applications"
- Chapter 10, "Using Terminal Sessions"

Installing the Controller

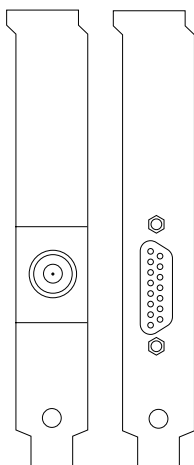
Before you can configure the Model 200 Controller, you need to install it in your network.

Equipment

- A coaxial or twinaxial connection where you can connect the controller.
- A cable to connect the controller 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 controller

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

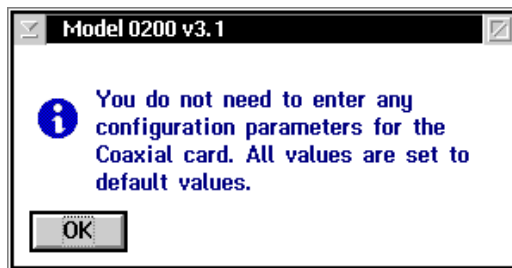


0200-021

0200-022

Configuring the Coaxial Adapter Card

If you have a coaxial network adapter card in the controller, 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:

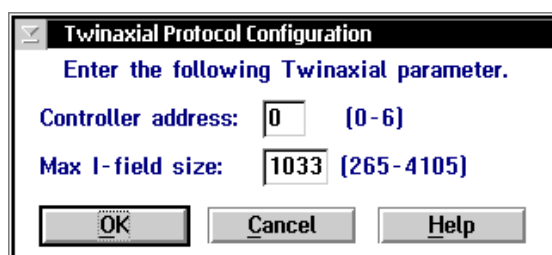


Choose OK to close the dialog box.

Configuring the Twinaxial Adapter Card

After you install the Model 200 Controller, you need to turn it on and configure its network adapter cards. Use the worksheets in Appendix E.

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



Field	Description	Value	Default
Controller address	The address of the host twinaxial connection.	0 to 6	0
Max I-field size	The maximum frame size that is used in this connection mode.	265 to 4105	1033

To configure a twinaxial network adapter card

1. From the main menu, choose the type of communication you are using to connect the controller 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.
4. In the Controller address field, enter the twinaxial connection address. This value must be unique for each twinaxial device connected to the host on this line.
5. In the Max I-field size field, enter the maximum frame size used in this connection mode.
6. Choose OK to save your changes and return to the main menu.

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.

7

Connecting to an SDLC Network

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

Chapter Checklist

Done?	Task	Page
<input type="checkbox"/>	Install the controller.	7-4
<input type="checkbox"/>	Use the GUI to configure the SDLC card for the SDLC network.	7-5

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

- Chapter 5, “Connecting to an Ethernet/Token Ring Network”
- Chapter 6, “Connecting to a Coaxial/Twinaxial Network”
- Chapter 8, “Using Terminal Emulation”
- Chapter 9, “Using Peer-to-Peer Applications”
- Chapter 10, “Using Terminal Sessions”

Installing the Controller

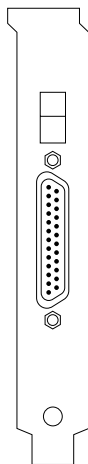
Before you can configure the Model 200 Controller, you need to install it in your network.

Equipment

- An SDLC connection where you connect the controller.
- An SDLC cable to connect the controller 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.

To install the controller



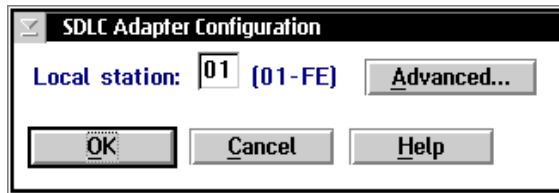
0200-020

1. Locate the slot that contains the SDLC card on the rear panel of your controller. The SDLC card is the card that is furthest right when you are looking at the rear 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 Model 200 Controller, you need to turn it on and configure its network adapter cards. Use the worksheets in Appendix E.

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, modem speed, NRZI, and maximum I-field size.



Field	Description	Value	Default
Local station	The address (in hex) that identifies the controller station.	01 to FE	01

To configure an SDLC network adapter card

1. From the main menu, choose the type of communication you are using to connect the controller 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 that identifies the controller's station.
5. Configure any advanced parameters for SDLC. For help, see, "Configuring Advanced SDLC Parameters" in the next section.
6. Choose OK to save your changes and return to the main menu.

Configuring Advanced SDLC Parameters

Field	Description	Value	Default
Line type	The type of telecommunications link that the controller 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 controller to your host.	Full duplex, Half duplex	Half duplex
NRZI	Non-return-to-zero inverted. The data encoding for modems that are sensitive to certain bit patterns.	On, Off	On
Link station role	This field sets the role of the controller to be the primary workstation or the secondary workstation to the host.	Primary, Negotiable, Secondary	Secondary

Field	Description	Value	Default
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 controller sends the XID response without waiting for the host to send the XID request.	Check, Clear	Clear

To configure the advanced SDLC parameters

1. From the SDLC Protocol Configuration dialog box, choose Advanced. The Advanced SDLC Adapter Protocol Configuration dialog box appears.
2. Choose the Line type to be Switched or Non-switched.
3. Choose the Line mode to be Full duplex or Half duplex.
4. Choose the NRZI to be On or Off.
5. In the Link station role field, click the down arrow on the right side of the field. A list of roles appears. Select the controller to be the primary or secondary workstation.

Note: If you are configuring 3270 terminal emulation, the default for this field is Secondary. When you are communicating with a mainframe, this field is typically Secondary.

Or, choose Negotiable if you want the controller and host to negotiate their roles when they connect.

6. In the Max I-field size, enter the maximum frame size that is used in this connection mode.
7. Decide if you want the controller to send its XID response before the host requests it. Enabling this check box sends the XID response immediately. This XID is also the Node ID.
8. Choose OK to save your changes and return to the SDLC Protocol Configuration dialog box.

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.

8

Using Terminal Emulation

Now that you have configured the Model 200 Controller 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 an application, such as terminal emulation.

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

Chapter Checklist

Done?	Task	Page
<input type="checkbox"/>	Understand how terminal emulation (TE) runs on the host, controller, and data collection devices.	8-5
<input type="checkbox"/>	For VT, ANSI, TN5250, or TN3270 TE, identify all the TCP/IP hosts on the network. If necessary, link and unlink terminal addresses to TCP/IP hosts.	8-7
	Or,	
	For 5250 TE, identify all the IBM SNA hosts on the network. If necessary, link and unlink terminal addresses to IBM SNA hosts.	8-12
	For 3270 TE, identify all the IBM SNA hosts on the network. If necessary, define the NAU pool and link and unlink terminal addresses to IBM SNA hosts.	8-22
<input type="checkbox"/>	Save and activate the configuration.	8-29
<input type="checkbox"/>	Configure your JANUS devices for TE.	8-30
<input type="checkbox"/>	To run VT and ANSI TE on your JANUS devices, download the TE files.	8-31
<input type="checkbox"/>	Configure your TRAKKER Antares terminals for TE.	8-40

Model 200 Controller User's Manual

Done?	Task	Page
<input type="checkbox"/>	Set security for accessing the TE Configuration menu.	8-46

Note: If your JANUS 2.4 GHz RF devices are running TCP/IP, you do not need a Model 200 Controller to run VT or ANSI TE, TN5250, or TN3270.

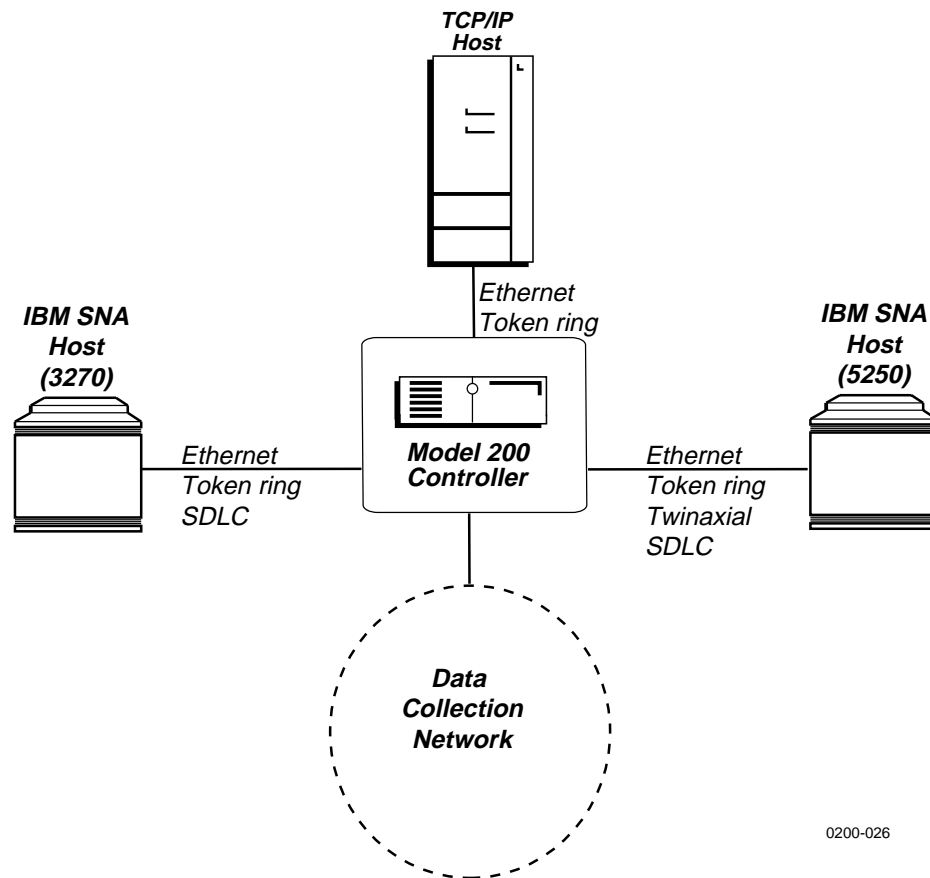
If your JANUS 2.4 GHz RF devices are running UDP Plus, you need to use a Model 200 Controller.

Note: You can also use the controller 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 controller.

About Terminal Emulation

Terminal emulation (TE) lets data collection devices communicate through the Model 200 Controller as if they were directly connected to the host. The controller sends data to the device in a screen format that emulates the host session. Vehicle-mount terminals automatically see the entire screen. Other terminals have viewporting abilities; that is, you can use commands to move the smaller device screen around to see a much larger terminal screen.



0200-026

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 Model 200 Controller, you can run VT/ANSI TE on JANUS UDP Plus devices and TRAKKER Antares terminals. The UNIX or other TCP/IP host must support Telnet. You can also run TN5250 or TN3270 on TRAKKER Antares terminals. Your IBM host must support Telnet. When you send data from the device, the controller routes it to the Telnet session on the host.

Using the controller, you can also run IBM SNA 5250 TE or IBM SNA 3270 TE on JANUS UDP Plus devices and TRAKKER Antares terminals to an IBM AS/400 or other IBM SNA host.

Your controller is licensed to communicate with a fixed number of devices (1-8, 1-24, 1-64, 1-128). When a device first sends a message through the controller, the controller logs its logical name. When the controller 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 Application

For JANUS devices that run VT or ANSI TE, the Model 200 Controller provides the JANUS TE application.

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

For help, see "Downloading the JANUS TE Application" later in this chapter.

Note: If you are replacing a 9185 controller with a Model 200 Controller, you must download the new JANUS TE application to all your JANUS devices.

TRAKKER Antares TE Application

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 controller, if you need to download it to your device.

For help, see “Downloading the TRAKKER Antares TE Application” later in this chapter.

Setting Up Telnet Terminal Emulation

When you set up your data collection network to run Telnet TE, you need to configure the Model 200 Controller and the data collection devices. Telnet TE includes VT100, VT220, VT320, ANSI, TN5250, and TN3270.

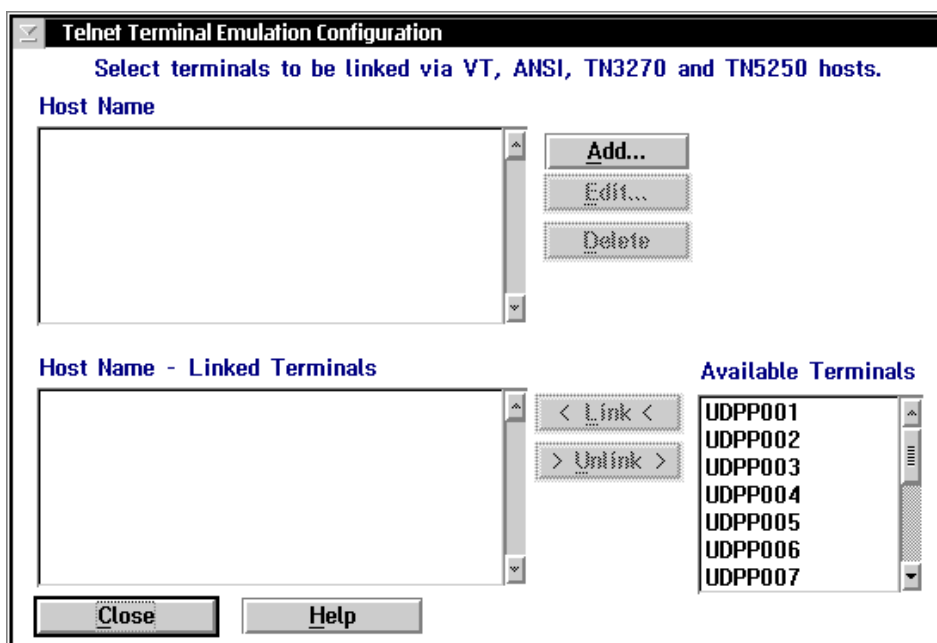
Note: For VT, ANSI, TN5250, and TN3270 TE, your network administrator does not need to configure anything on the host.

Configuring the Controller

To run Telnet TE between JANUS devices and TRAKKER Antares terminals and the host, you need to identify all the TCP/IP hosts and use DNS or manually enter their IP addresses. Then, you can explicitly link or unlink terminal names to hosts. If an explicit link is set up between a terminal and a host, it means that the terminal can only start TE sessions with that host. If no explicit link is set up, the terminal can start a TE session with any host in the Host Name list. The terminal will start a TE session with the host that is configured on it.

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

- Installed the Model 200 Controller.
- Installed and configured the connection points and downline devices.
- Configured the network adapter cards.



Field	Description	Value	Default
Host Name	This list box contains the logical names of the TCP/IP hosts that you have defined.	Predefined	None
Host Name - Linked Terminals	The terminal names that are linked to a specific host.	None	None
Available Terminals	The list of all the terminal names that are available to add to the Host Name - Linked Terminals list box.	Predefined	All configured terminals

To set up Telnet terminal emulation

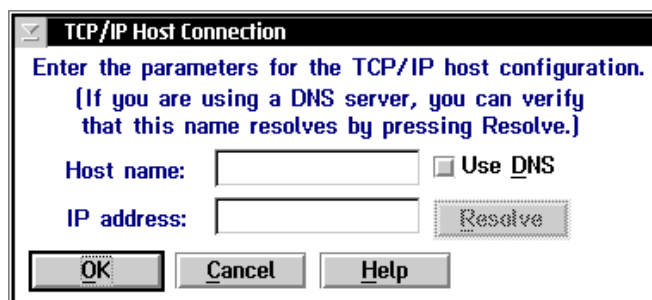
1. From the main menu, choose Terminal Emulation.
2. Choose Telnet Terminal Emulation. The Telnet Terminal Emulation Configuration dialog box appears.
3. Make sure that you have added all your TCP/IP hosts. The Host Name list box contains all the existing host names. For help, see “Adding a TCP/IP Host” in the next section.

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

4. (Optional) Create any explicit links between terminals and hosts.
 - a. In the Host Name list box, select the host that you want to link to a terminal.
 - b. In the Available Terminals list box, select the logical name of the terminal that you want to link to the host.
 - c. Choose Link. The host name and the terminal appear in the Host Name - Linked Terminals list box.
5. (Optional) Unlink any explicit links between terminals and hosts.
 - a. In the Host Name - Linked Terminals list box, select the host and the logical name of the terminal you want to unlink.
 - b. Choose Unlink. The host name and the terminal are removed from the Host Name - Linked Terminals list box.
6. Choose Close to close the dialog box and return to the main menu.

Adding a TCP/IP Host

To communicate with TCP/IP hosts, the Model 200 Controller must know their IP addresses. You can either use DNS to resolve these IP addresses or you can enter them in manually.



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.	Check, Clear	Clear
IP address	The address that identifies the TCP/IP host to the network.	xxx.xxx.xxx.xxx where xxx is a value between 0 and 255.	None

To determine the host IP address using DNS

1. From the Telnet Terminal Emulation Configuration dialog box, choose Add. The TCP/IP Host Connection dialog box appears.
2. In the Host name field, enter the abbreviated or long host name. If you enter the abbreviated name, the controller searches the domain names in the DNS Configuration dialog box to determine the long host name.
3. Enable the Use DNS check box.

Note: Before you enable this check box, you must first configure a DNS server in the DNS Configuration dialog box.

4. (Optional) Choose Resolve. The controller searches the domains that are listed in the DNS Configuration dialog box for the host name and resolves the IP address.
5. Choose OK to save your changes and return to the Telnet Terminal Emulation Configuration dialog box.

To configure the host IP address manually

1. From the Telnet Terminal Emulation Configuration dialog box, choose Add. The TCP/IP Host Connection dialog box appears.
2. In the Host name field, enter the host name.
3. Make sure the Use DNS check box is disabled.
4. In the IP address field, enter the host's IP address.
5. Choose OK to save your changes and return to the Telnet Terminal Emulation Configuration dialog box.

Setting Up 5250 SNA Terminal Emulation

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

Note: To set up TN5250 terminal emulation, see "Setting Up Telnet Terminal Emulation" earlier in this chapter.

Configuring the Host

For 5250 TE, your network administrator needs to define the Model 200 Controller on the host unless you have auto-create controller turned on.

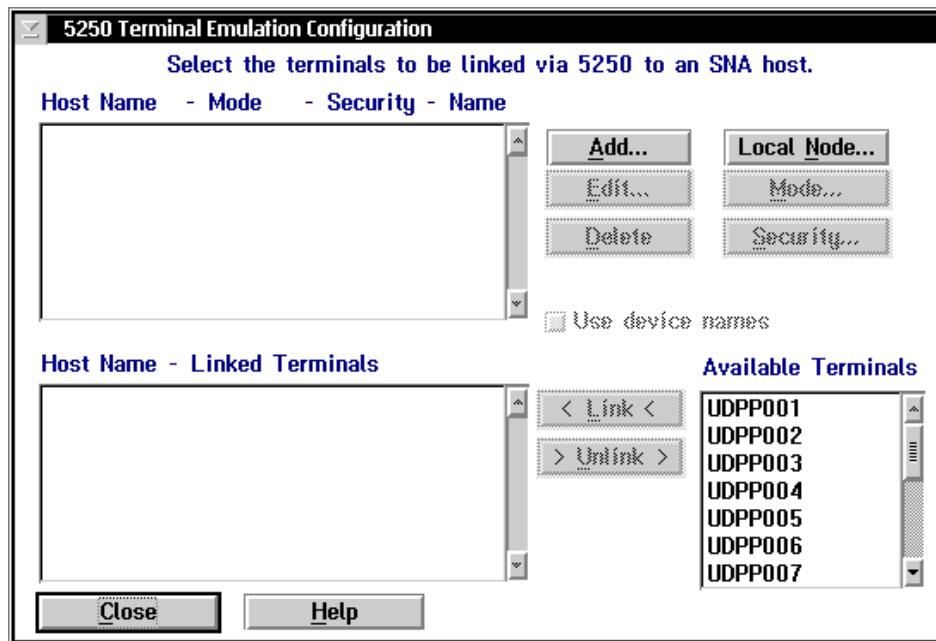
Configuring the Controller

To run 5250 TE between JANUS devices and TRAKKER Antares terminals and the host, you must identify all the IBM SNA hosts. Then, you can link or unlink terminals to specific hosts. If an explicit link is set up between a terminal and a host, it means that the terminal can only start TE sessions with that host. If no explicit link is set up, the terminal can start a TE session with any host in the Host Name list. The terminal will start a TE session with the host that is configured on it.

Use device names check box Check this check box if you want the host to use the logical name of the device when establishing terminal sessions. These logical names are the same ones that you assigned when you identified these devices. For help, see "Identifying the RF Data Collection Devices" and "Identifying the UDP Plus Terminals" in Chapter 3. If you use device names, you must configure all the devices that communicate to the AS/400 host as virtual devices of the type 3197.

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

- Installed the Model 200 Controller.
- Installed and configured the connection points and downline devices.
- Configured the network adapter cards.



Field	Description	Value	Default
Host Name - Mode - Security - Name	This list box contains the logical names of the 5250 SNA hosts that you have defined, what mode they are using, if security is set, and if they are using device names.	Predefined	None
Use device names (Optional)	This check box determines if the selected host in the Host Name list box uses the logical name of the device when establishing terminal sessions.	Check, Clear	Clear
Host Name - Linked Terminals	The terminals that are linked to a specific host.	None	None
Available Terminals	The list of all the terminals that are available to add to the Host Name - Linked Terminals list box.	Predefined	None

To set up 5250 terminal emulation

1. From the main menu, choose Terminal Emulation.
2. Choose 5250 SNA Terminal Emulation. The 5250 Terminal Emulation Configuration dialog box appears.
3. Make sure that you have added all your hosts. The Host Name list box contains all the existing host names. For help, see "Adding an IBM SNA Host" later in this chapter.

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

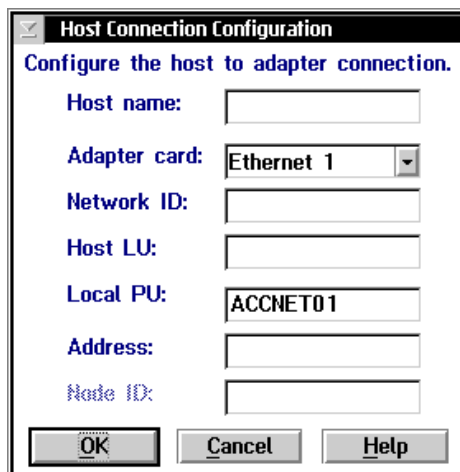
4. Make sure that you have configured the controller SNA node for the network. For help, see "Configuring the Controller SNA Node" later in this chapter.
5. (Optional) Create a user ID and password for the controller so it can access the host. If you set security, a Yes appears next to the host name in the Security column. For help, see "Setting and Removing the User ID and Password" later in this chapter.
6. (Optional) Select the IBM mode that defines the class of service and other session characteristics that you want for your network design. If you select a mode, the mode appears next to the host name in the Mode column. For help, see "Selecting an IBM Mode" later in this chapter.
7. (Optional) Check the Use device names check box if you want the selected host to use the logical names of the devices when establishing terminal sessions. A Yes appears next the host name under the Names column.
8. (Optional) Create any explicit links between terminals and hosts.
 - a. In the Host Name list box, select the host that you want to link to a terminal.
 - b. In the Available Terminals list box, select the logical name of the terminal that you want to link to the host.
 - c. Choose Link. The host and the terminal appear in the Host Name - Linked Terminals list box.

9. (Optional) Unlink any explicit links between terminals and hosts.
 - a. In the Host Name - Linked Terminals list box, select the host and logical name of the terminal that you want to unlink.
 - b. Choose Unlink. The host name and the terminal are removed from the Host Name - Linked Terminals list box.
10. Choose Close to close the dialog box and return to the main menu.

Adding an IBM SNA Host

You must identify any hosts you want the Model 200 Controller 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 controller 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.

Local PU field Use this field when you want your terminals to be able to communicate with different hosts through one 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.



The image shows a dialog box titled "Host Connection Configuration" with a close button in the top-left corner. Below the title bar, the text "Configure the host to adapter connection." is displayed. The dialog contains several fields for configuration:

- Host name:** An empty text input field.
- Adapter card:** A dropdown menu currently showing "Ethernet 1".
- Network ID:** An empty text input field.
- Host LU:** An empty text input field.
- Local PU:** A text input field containing the value "ACCNET01".
- Address:** An empty text input field.
- Node ID:** An empty text input field.

At the bottom of the dialog, there are three buttons: "OK", "Cancel", and "Help".

Model 200 Controller User's Manual

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	Controller 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.	8 uppercase alphanumeric or special characters 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.	Token ring MAC address format	None

To add an IBM 5250 SNA host

1. From the 5250 Terminal Emulation Configuration dialog box, choose Add. The Host Connection Configuration dialog box appears.
2. In the Host name field, enter a meaningful unique name for the host.
3. In the Adapter card field, click the down arrow on the right side of the field. A list that contains the available adapter cards appears. Select the adapter card you are using to connect to the host.
4. In the Network ID field, enter the network ID of the network on which the host resides.

5. In the Host LU field, enter the LU name that identifies the host.
6. (Ethernet or token ring only) In the Local PU field, enter a unique PU (physical unit) name for the host. The default name is the local SNA node name plus a 2-digit suffix.
7. (Ethernet or token ring only) In the Address field, enter the LAN adapter address of the remote host. For help, see “Converting Ethernet Addresses to Token Ring MAC Format” in Appendix B.
8. Choose OK to save your changes. You return to the 5250 Terminal Emulation Configuration dialog box.

Configuring the Controller SNA Node

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 controller. 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.	8 hexadecimal characters	05D00000

To configure the controller SNA node

1. From the 5250 Terminal Emulation Configuration dialog box, choose Local Node. The SNA Local Node Information dialog box appears.
2. In the Network ID field, enter the network name used to create a unique SNA network.
3. In the Node Name field, enter the name of the Model 200 Controller that other nodes will use to address it.
4. In the Node ID field, enter the last eight characters in the XID that establish a host connection. The Node ID is the same as the XID.

When establishing a connection, the host or controller with the higher Node ID number is the primary workstation.

5. Choose OK to save your changes and return to the 5250 Terminal Emulation Configuration dialog box.

Selecting an IBM Mode

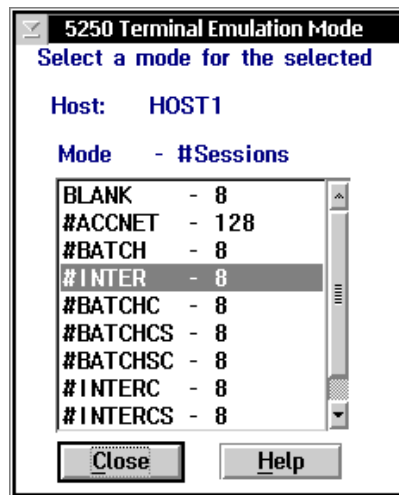
The IBM mode defines the terminal session characteristics between the controller and the SNA host. The default mode, #INTER, allows only eight sessions. If you need more than eight sessions, select a new IBM mode.

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. The mode appears next to the host name under the Mode column.

Setting and Removing the User ID and Password

Your host may implement security at the session level. This type of security requires the controller to log in before it can communicate with the host. Performing 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.



3. In the Host user ID field, enter a user ID that allows the controller to access the host.
4. In the Password field, enter a password that goes with the user ID.
5. Choose OK to save your changes and return to the 5250 Terminal Emulation Configuration dialog box. A Yes appears next to the host name in the Security column.

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. Instead of a Yes next to the host name in the Security column, there is a blank.

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

Note: To use this feature with 5250 terminal emulation, your AS/400 must be version 2.3 or higher.

When using 5250 terminal emulation, 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 controller.

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.

Setting Up 3270 SNA Terminal Emulation

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

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

Configuring the Host

For 3270 TE, your network administrator must set up the host to see the Model 200 Controller as an IBM model 3174 terminal controller. Your network administrator also needs to 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:

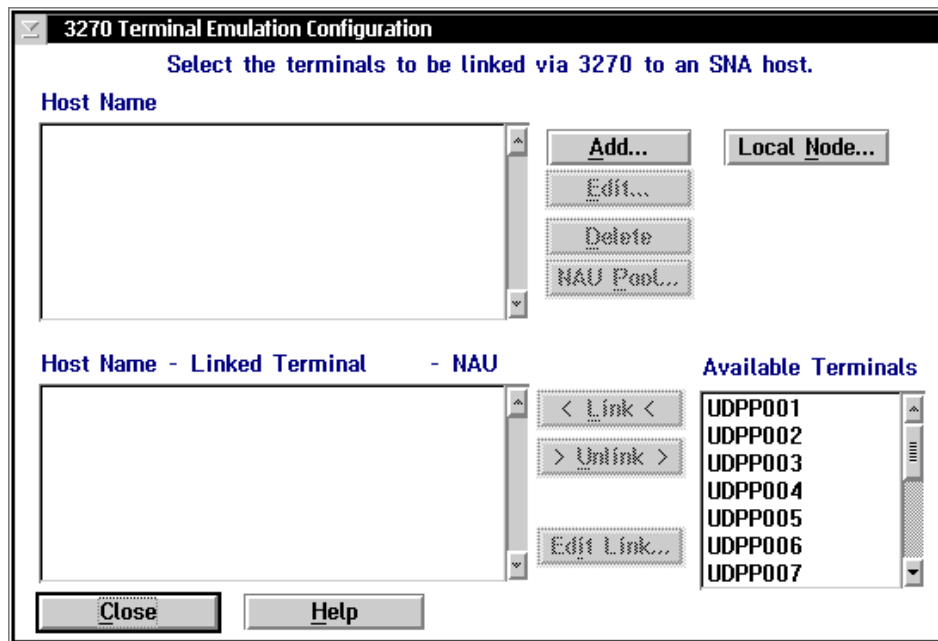
- the non-switched or switched SDLC station address (host field: ADDR)
- the node ID (host field: IDBLK+IDNUM)

Configuring the Controller

To run 3270 TE between JANUS devices and TRAKKER Antares terminals and the host, you must identify all the IBM SNA hosts. You also need to configure the controller SNA node. Then, you can link or unlink terminals to specific hosts. If an explicit link is set up between a terminal and a host, it means that the terminal can only start TE sessions with that host. If no explicit link is set up, the terminal can start a TE session with any host in the Host Name list. It will start a TE session with the host that is configured on the terminal.

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

- Installed the Model 200 Controller.
- Installed and configured the connection points and downline devices.
- Configured the network adapter cards.



Field	Description	Value	Default
Host Name	This list box contains the logical names of the 3270 SNA hosts.	Predefined	None
Host Name - Linked Terminal - NAU	The terminals that are linked to a specific host.	None	None
Available Terminals	The list of all the terminals that are available to add to the Host Name - Linked Terminal - NAU list box.	Predefined	None

To set up 3270 terminal emulation

1. From the main menu, choose Terminal Emulation.
2. Choose 3270 SNA Terminal Emulation. The 3270 Terminal Emulation Configuration dialog box appears.
3. Make sure that you have added all your hosts. The Host Name list box contains all the existing host names. For help, see "Adding an IBM SNA Host" later in this section.

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

4. Make sure that you configure the controller SNA node. For help, see "Configuring the Controller SNA Node" earlier in this chapter.
5. Decide how to set up NAUs for the terminals:
 - 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.
 - Do not fill the NAU pool for any of the hosts. When you explicitly link terminals to hosts, the controller automatically generates NAUs starting at 002.
 - 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" later in this chapter.

6. (Optional) Create any explicit links between hosts, terminals, and NAUs.
 - a. In the Host Name list box, select the host that you want to link to a terminal.
 - b. In the Available Terminals list box, select the terminal that you want to link to the host.
 - c. Choose Link. The host name, logical name of the terminal, and NAU appear in the Host Name - Linked Terminal - NAU list box.

To change the NAU that the controller assigns to the terminal, see "Editing a Link" later in this chapter.

7. (Optional) Unlink any explicit links between hosts, terminals, and NAUs.
 - a. In the Host Name - Linked Terminal - NAU list box, select the host, the logical name of the terminal, and NAU that you want to unlink.
 - b. Choose Unlink. The host name, terminal, and NAU are removed from the Host Name - Linked Terminal - NAU list box.
8. Choose Close to close the dialog box and return to the main menu.

Adding an IBM SNA Host

You need to identify any hosts you want the Model 200 Controller 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 controller 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.

Local PU field Use this field when you want your terminals to be able to communicate with different hosts through one 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.

Model 200 Controller User's Manual

Host Connection Configuration
 Configure the host to adapter connection.

Host name:

Adapter card:

Network ID:

Host LU:

Local PU:

Address:

Node ID:

OK Cancel Help

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.	8 uppercase alphanumeric or special characters 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.	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 controller.	8 hexadecimal characters	05D00000

To add an IBM 3270 SNA host

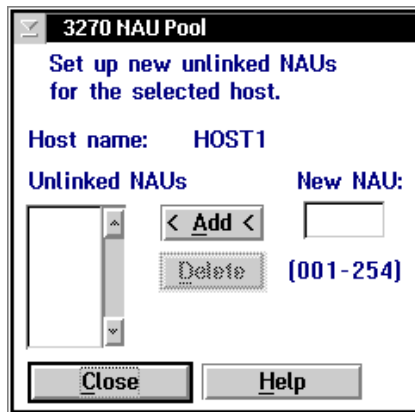
1. From the 3270 Terminal Emulation Configuration dialog box, choose Add. The Host Connection Configuration dialog box appears.
2. In the Host name field, enter a meaningful and unique name for the host.
3. In the Adapter card field, click the down arrow on the right side of the field. A list that contains the available adapter cards appears. Select the adapter card you are using to connect to the host.
4. (Ethernet or token ring only) In the Address field, enter the LAN adapter address of the remote host. For help, see “Converting Ethernet Addresses to Token Ring MAC Format” in Appendix B.
5. (Ethernet or token ring only) In the Local PU field, enter a unique PU (physical unit) name for the host. The default name is the local SNA node name plus a 2-digit suffix.
6. In the Node ID field, enter the last eight characters in the XID that establish a host connection. The Node ID is the same as the XID.

***Note:** When establishing a connection, the host or controller with the higher Node ID number is the primary workstation.*

7. Choose OK to save your changes. You return to the 3270 Terminal Emulation Configuration dialog box.

Filling the NAU Pool

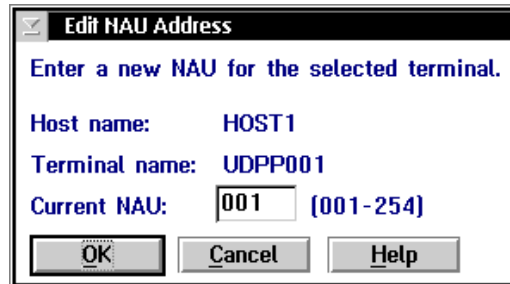
1. From the 3270 Terminal Emulation Configuration dialog box, choose NAU Pool. The 3270 NAU Pool dialog box appears.



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.

Editing a Link

1. From the 3270 Terminal Emulation Configuration dialog box in the Host Name - Linked Terminal -NAU list box, select the NAU that you want to change.
2. Choose Edit Link. The Edit NAU Address dialog box appears.



3. In the Current NAU field, enter a new NAU for the terminal.
4. 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 controller, save and activate your run-time configuration. When the activate is complete, a message box appears if you need to reboot the controller.

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 controller 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 Model 200 Controller and your JANUS 900 MHz RF devices or your JANUS 2.4 GHz RF devices using UDP Plus, 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.

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.

To configure your JANUS 900 MHz RF device

1. In the Com menu, choose RF and press .
2. Choose Activate.
3. In the RF Protocol field, select Enabled.
4. Choose Primary Cfg.
5. In the Device Address field, enter the address of the JANUS device. This address must match an address that is enabled on the Model 200 Controller.
6. Configure the Channel Select and the Network ID.
7. In the File menu, choose Exit.
8. Choose Yes to save your configuration.

Configuring for UDP Plus Communications

You need to configure each JANUS 2.4 GHz RF 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: If the access points are using a security ID, you must set the same security ID on the JANUS devices.

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 controller to each JANUS device. When you download the JANUS TE application, the files must be on the E drive.

On the controller, 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 terminal emulation. This file is read only.

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

Model 200 Controller User's Manual

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

TNVT900.EXE This executable file runs VT/ANSI TE. You can only use this file if your JANUS 900 MHz RF device uses firmware v3.1 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 v3.1 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 v3.1 or higher.

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

UDPPVT.EXE This executable file runs VT/ANSI TE. You can only use this file if your JANUS 2.4 GHz RF device uses UDP Plus and firmware v4.1 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 TE. You can only use this file if your JANUS 2.4 GHz RF device uses UDP Plus and firmware v4.1 or higher.

UDPP3270.EXE This executable file runs 3270 TE. You can only use this file if your JANUS 2.4 GHz RF device uses UDP Plus and firmware v4.1 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 device in a 900 MHz RF network has firmware v3.01 or later, use the download server feature.

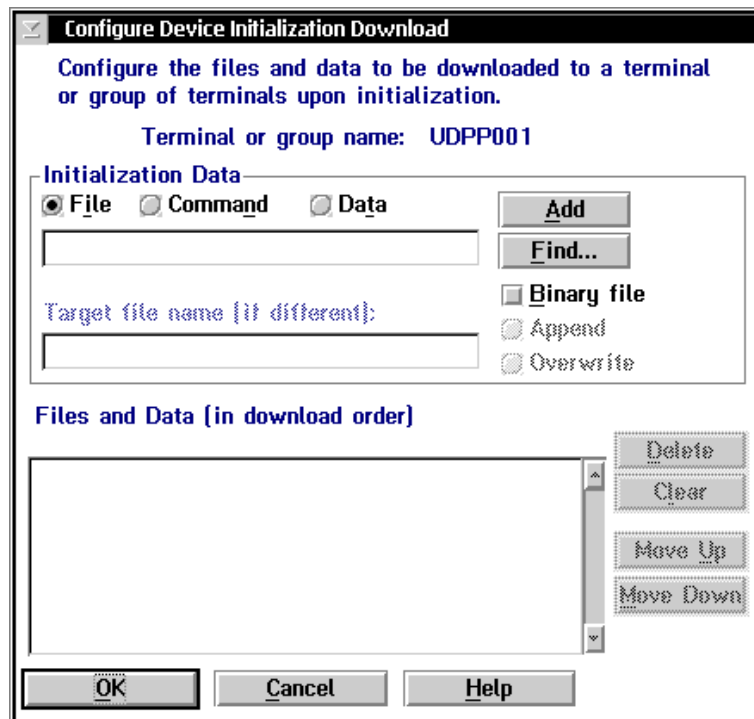
Note: Your JANUS devices must have FTA.EXE and FTA.INI loaded on drive C. Copy these files from Application companion disk 3. For help, see your JANUS user's manual.

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 feature or FTP. To use FTP, you must have an FTP client loaded on your JANUS device.

Using the Download Server to Download the JANUS TE Application

1. If you want to send the TE files to more than one JANUS device, define a group in the download server. For help, see “Adding a Group in the Download Server” in Appendix B.
2. From the main menu sidebar buttons, choose System Maintenance. The System Maintenance dialog box appears.
3. In the System Maintenance list box, select Configure Download Server and then choose Start. The Terminal Download Configuration dialog box appears.
4. In the Terminals and Groups list box, select the terminal or group that needs the TE files.
5. Choose Edit. The Configure Device Initialization Download dialog box appears.



Model 200 Controller User's Manual

6. In the Initialization Data box, choose File.
7. In the field, type the path and filename of the .CFG file that contains the configuration information that each JANUS device needs to run TE.
8. Check the Binary file check box.
9. Choose Overwrite if you want to overwrite any existing files with the same name on the JANUS devices. Do not choose Append.
10. Choose Add. The file appears in the Files and Data list box with a B in the leftmost column.
11. Repeat Steps 7 through 10 to add the path and filename of the .EXE file that runs the JANUS TE application.
12. (5250/3270 only) Repeat Steps 7 through 10 to add the path and filename of the .MAP file for the type of JANUS TE application you are using.
13. Choose OK to save your changes and return to the Terminal Download Configuration dialog box.
14. In the Terminals and Groups list box, choose the terminal or group you configured.
15. Choose Download. The TE files are downloaded to the terminal or group.
16. Choose Close to return to the System Maintenance dialog box.
17. Choose Close to return to the main menu.

Using 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 *IPaddress* and press where *IPaddress* is the IP address of the controller.
2. In the login name field, type and press .
3. Type *path* and press where *path* is the location of the JANUS TE application on the controller.

4. Type `B I N` and press `enter ↵`.
5. Type `G E T` `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` `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 ↵`.

Accessing the TE Configuration Menu

JANUS terminal emulation is controlled by a configuration file. You can edit the terminal emulation parameters using a menu-driven interface.

- When you are running VT or ANSI TE, you can access the TE Configuration menu at any time by pressing `Ctrl F9`.
- When you are running 5250 or 3270 TE, you can access the TE Configuration menu at any time by pressing `Alt X`. Or you can scan:

Exit



%EXIT

Use the `↑` and `↓` keys to move between fields. Use the `←` and `→` keys to change the preset values for the fields. For help using the TE Configuration menu, see your *JANUS 900 MHz Terminal Emulation Quick Reference Guide* or the *JANUS 2.4 GHz Terminal Emulation Quick Reference Guide*.

You can set a password for the TE Configuration menu to prevent unauthorized users from accessing this menu. For help, see “Setting Security for the TE Configuration Menu” later in this chapter. Using this menu, you can edit the parameters in the Terminal screen, Communications screen, and the Viewport screen. When you exit the TE menu, the TE session is restored.

Exiting the TE Configuration Menu

1. From the TE Configuration menu, choose Exit Config and press . The Save New Configuration screen appears.
2. Choose Yes and press if you want to save the TE configuration. Your terminal saves the configuration options to flash memory and the sign-on screen appears.
Choose No and press if you do not want to save the TE configuration. You exit the TE Configuration menu and the sign-on screen appears.
Choose Cancel and press to return to the TE Configuration menu. You can continue making changes to the TE configuration.

Starting TE

When you start a TE session on your JANUS device, the device establishes a connection with the controller and displays the host login screen.

To start a TE session on the JANUS device

1. Make sure the host and the application support the selected terminal type.
2. Make sure that you have started data collection on the controller.
3. Press to resume the JANUS device.
4. (5250/3270 only) At the DOS prompt on your JANUS device, type .
5. On the JANUS device type:
 to start a 5250 TE session.
 to start a 3270 TE session.
 to start a VT/ANSI TE session.
6. Wait a few seconds while the display clears and the TE program starts.
7. When the display on your JANUS device shows the login screen, log into the host. If the auto-login script file is in the current directory, the JANUS device keeps the login information in memory.

You are ready to use terminal emulation on your JANUS device.

Tip: To make it easier for users to start a TE session, you may want to create a batch file that performs this procedure.

Ending TE

To end a TE session on your JANUS device, perform one of these steps:

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   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  .

5250 or 3270 On the JANUS device, press  .

2. Select the Exit TE command and press . 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.

About Running TE

When you start the TE program on the JANUS device, it attempts to establish communications with a host session by sending a request to the Model 200 Controller terminal session manager.

- If a terminal session is started, then the terminal session becomes active and the JANUS device can communicate with the host.

- If a terminal session is started and then the connection is broken, the TE program on the JANUS device exits and you must restart it.
- If the request for a terminal session is rejected, a message is sent back to the JANUS device.

For help, see your *JANUS 900 MHz Terminal Emulation Quick Reference Guide* or the *JANUS 2.4 GHz Terminal Emulation Quick Reference Guide*.

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 need to reboot the device, you need to login again.

For more help on creating the auto-login script file, see the *JANUS 900 MHz Terminal Emulation Quick Reference Guide* or the *JANUS 2.4 GHz Terminal Emulation Quick Reference Guide*. After you create your auto-login script file (AUTOLOG.SCR), you need to download it to your JANUS device. This file must reside in the same directory as the TE application.

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

To use the auto-login feature

- For VT/ANSI, press \triangle \langle Ctrl \rangle \langle F4 \rangle .
- For 5250 or 3270, press \langle Alt \rangle \langle F5 \rangle .
- Or, you can scan:

Auto-Login Restart



%ALRS

Displaying International Characters

You can configure your JANUS devices to display single-byte international characters. This feature lets the device display 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 Model 200 Controller, you can find the .MAP files in the \USERDATA\TERMAPPS\TE\INTERNAT directory.

To use international character sets

1. On the Model 200 Controller, 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 Controller 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 the *JANUS 900 MHz Terminal Emulation Quick Reference Guide* or the *JANUS 2.4 GHz 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 Model 200 Controller, you can run VT or ANSI terminal emulation (TE) between your TRAKKER Antares terminals and a TCP/IP host. You can run 5250 or 3270 terminal emulation between your terminals and an IBM SNA host. You can also run TN5250 or TN3270 terminal emulation between your terminals and an IBM host that supports Telnet.

Configuring for Communications

Before you can run terminal emulation, you need to configure each terminal to communicate in the 2.4 GHz RF network or the Ethernet network. Press **[F] [T] [2] [M]** to access the TRAKKER Antares 2400 Menu System. On the T248X, press **[F] [←] [2] [4] [8]** to access the TRAKKER Antares 2400 Menu System. For help, see your TRAKKER Antares terminal user's manual. You need to set these parameters on each terminal:

- Time and date
- Network activate
- Network port (must match the Model 200 Controller)
- Controller IP address (must match the Model 200 Controller)
- Terminal IP address
- RF domain (for the access point)
- RF security identification (for the access point)

The terminal also needs to know where to send transactions. Choose one of these options:

- Explicitly link the terminals to a host. For help, see "Configuring the Controller" earlier in this chapter.
- Identify a host name on each terminal. For help, see your TRAKKER Antares terminal user's manual.

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 Model 200 Controller 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 Controller to Upgrade TRAKKER Antares Terminals” in Appendix D.
- Use the download server feature as described next.

To run VT or ANSI TE, download the .CFG file from the controller to each terminal. On the controller, the .CFG file is 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 controller, these files are in the \USERDATA\TERMAPPS\TE\POLUDPP directory:

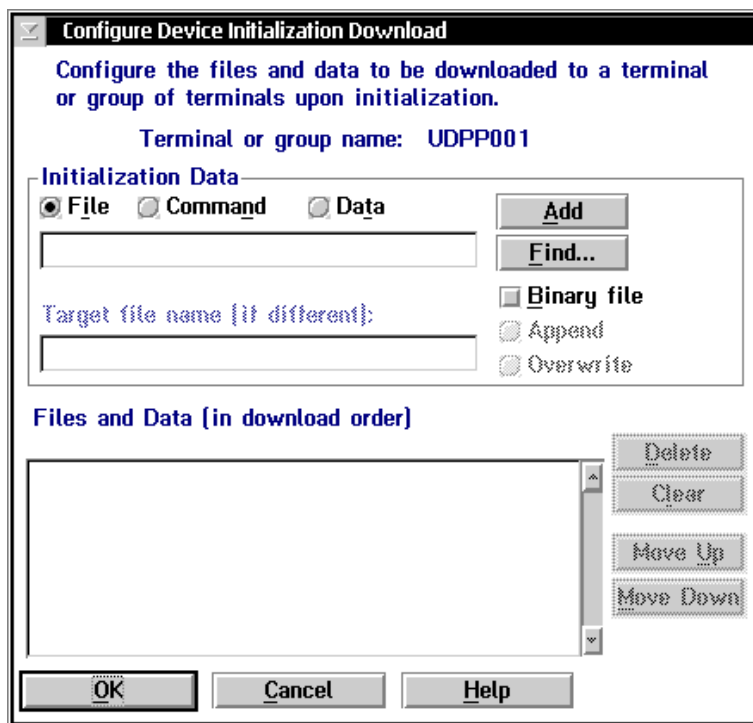
VTXXX_D.BIN This executable file runs VT/ANSI TE on the terminal.

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

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

To use the download server feature

1. If you want to send the TE files to more than one TRAKKER Antares terminal, define a group in the download server. For help, see "Adding a Group in the Download Server" in Appendix B.
2. From the main menu sidebar buttons, choose System Maintenance. The System Maintenance dialog box appears.
3. In the System Maintenance list box, select Configure Download Server and then choose Start. The Terminal Download Configuration dialog box appears.
4. In the Terminals and Groups list box, select the terminal or group that needs the TE files.
5. Choose Edit. The Configure Device Initialization Download dialog box appears.



6. In the Initialization Data box, choose File.
7. In the field, type the path and filename of the .CFG file that contains the configuration information that each terminal needs to run TE.
8. Check the Binary file check box.
9. Choose Overwrite if you want to overwrite any existing files with the same name on the terminals. Do not choose Append.
10. Choose Add. The file appears in the Files and Data list box with a B in the leftmost column.
11. Repeat Steps 7 through 10 to add the path and filename of the .BIN file that runs the TRAKKER Antares TE application. You may also need to download the .MAP file.
12. Choose OK to save your changes and return to the Terminal Download Configuration dialog box.
13. In the Terminals and Groups list box, choose the terminal or group you configured.
14. Choose Download. The TE files are downloaded to the terminal or group.
15. Choose Close to close the dialog box and return to the System Maintenance dialog box.
16. Choose Close to return to the main menu.

Accessing the TE Configuration Menu









If you are running TE on your terminal, you can access the TE Configuration menu when the TE welcome screen is displayed on the terminal or after a TE session is established. You cannot enter the TE Configuration menu when the terminal is trying to connect to the Model 200 Controller.

You can set a password for the TE Configuration menu to prevent unauthorized users from accessing this menu. For help, see "Setting Security for the TE Configuration Menu" later in this chapter.

When you leave the TE Configuration menu, the TE session is restored.

To access the TE Configuration menu

Note: The icons that are shown in this procedure represent the keys on a T2425. The keys on the T248X terminal may look slightly different.

1. Press   on the terminal to access the Terminal Emulation menu.
2. Press  or  to choose Configure TE and press . The TE Configuration menu appears.
3. Press  or  to choose the function you want to configure and press .



You may need to set the terminal, communications, and viewport parameters. For help, see your TRAKKER Antares terminal user's manual.


Note: If you choose Exit TE from the Terminal Emulation menu, the terminal session ends and the TRAKKER Antares terminal will reboot.


Exiting the TE Configuration Menu

After entering all configuration parameters, you are prompted to save the new configuration and exit the TE Configuration menu.

To exit the TE Configuration menu

1. From the TE Configuration menu, choose Exit Config and press . The Save new configuration screen appears.
2. Choose Yes and press  if you want to save the TE configuration. Your terminal saves the configuration options to flash memory and the TE screen appears.

Choose No and press  if you do not want to save the TE configuration. You exit the TE Configuration menu and the TE screen appears.

Choose Cancel and press  to return to the TE Configuration menu. You can continue making changes to the TE configuration.

About Running TE on Your Terminals

After you configure the parameters for communications on each terminal, the terminal attempts to establish communications with a host session by sending a request to the Model 200 Controller terminal session manager.

- If the terminal session is started, then the terminal session becomes active and the terminal can communicate with the host.
- If the terminal session is started and then the connection is broken, the TE program on the terminal exits and you must restart it.
- If the request for a terminal session is rejected, a message is sent back to the terminal.

For help, see the *TRAKKER Antares Terminal Emulation User's Guide*.

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 Model 200 Controller, 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 Controller to Transfer Files" in Appendix B.

Displaying International Characters

You may want to use an international character set with your TRAKKER Antares terminals. This feature allows these terminals to display screen data using this character set while running terminal emulation. You can also configure your terminals to display single-byte international characters. This feature maps SBCS code pages for various Latin-based languages to SBCS code page 850, a multilingual code page for Latin-based languages.

Model 200 Controller User's Manual

On the Model 200 Controller, you can find the .MAP files in the \USERDATA\TERMAPPS\TE\INTERNAT directory.

To use international character sets

1. On the Model 200 Controller, 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 Controller to Transfer Files" in Appendix B.

Code Page Table

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.

Setting Security for the TE Configuration Menu

You can set a password to control access to the terminal emulation configuration menu. When you first configure your devices, there are no passwords 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 need to 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 controller. Therefore, if you want to permanently change the password, you must change it from the controller.

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 the password on TRAKKER Antares terminals, see the *TRAKKER Antares Terminal Emulation User's Guide*.

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 choose Start. The Terminal Password Configuration dialog box appears.



Model 200 Controller User's Manual

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 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 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.

Verifying 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, you must enter the correct password before you can access the TE Configuration menu.
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.

Using Peer-to-Peer Applications

Now that you have configured the Model 200 Controller to communicate with your LAN and you have configured your controller to communicate with your Intermecc network, you are ready to tie the entire data collection network together using an application.

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

Chapter Checklist

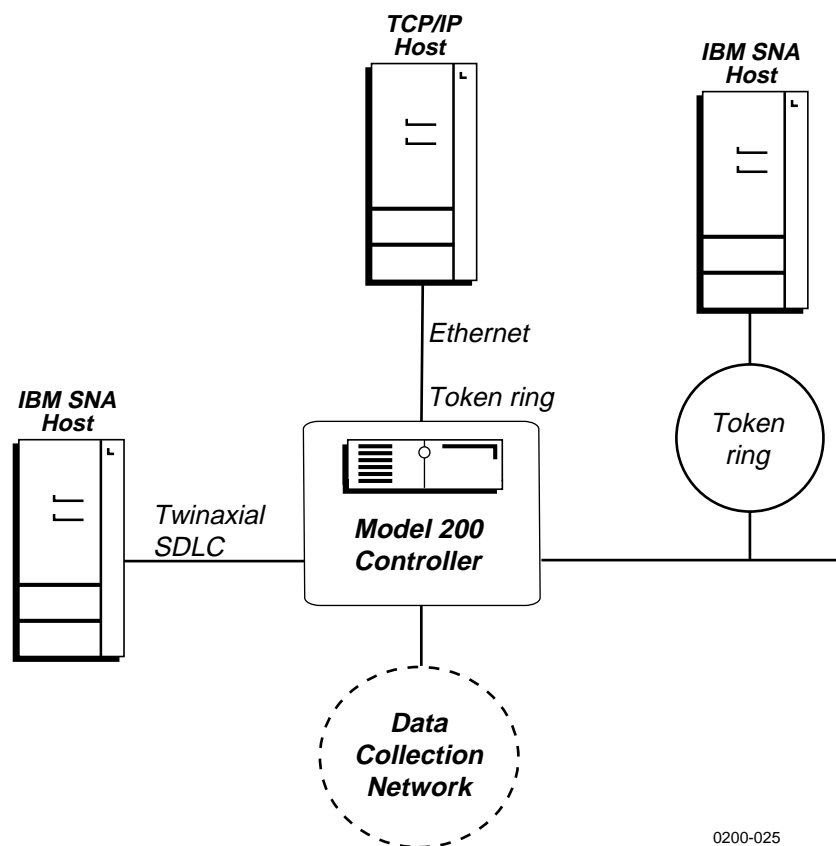
Done?	Task	Page
<input type="checkbox"/>	Configure the host for peer-to-peer applications.	9-5
<input type="checkbox"/>	Identify the peer-to-peer links.	9-6
<input type="checkbox"/>	Identify any transaction IDs that are routed to the peer-to-peer links.	9-11
<input type="checkbox"/>	Save and activate the configuration.	9-15
<input type="checkbox"/>	Understand how TCP/IP applications communicate with the controller.	9-16
	Or,	
	Understand how to use the direct TCP/IP socket interface.	9-23
	Understand how APPC applications communicate with the controller.	9-28

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

About Peer-to-Peer Applications

The Model 200 Controller runs an applications programming interface (API) that makes communicating with remote applications easier. Applications communicate with the controller through network communications processes called NetComms. NetComms are responsible for safely routing data from remote applications across a network to the controller and back.

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



0200-025

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 Model 200 Controller. 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 Model 200 Controller.

TCP/IP NetComm receive port (4401) This number identifies the port number through which the host makes receive connections to the Model 200 Controller.

APPC Applications

LU name The Model 200 Controller'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 Model 200 Controller. The default is APPN.

MAC address The Ethernet address or Token Ring address. You can verify the default value using the View Runtime Configuration feature. For help, see "Viewing the Configuration" in Appendix A.

Send transaction program This program is the Model 200 Controller'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 Model 200 Controller. 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 on the Controller

To run TCP/IP or APPC applications in your data collection network, you must identify all the application names in the Model 200 Controller. The controller puts these names in a peer-to-peer destination list. Every time an application connects to the controller, it informs the controller of its name. The controller dynamically associates the application as one of the destinations in its peer-to-peer destination list and forwards the appropriate transactions to it. The controller routes transactions to applications or other peer-to-peer destinations by one of two ways:

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

Use the worksheets in Appendix E to help you obtain the information you need.

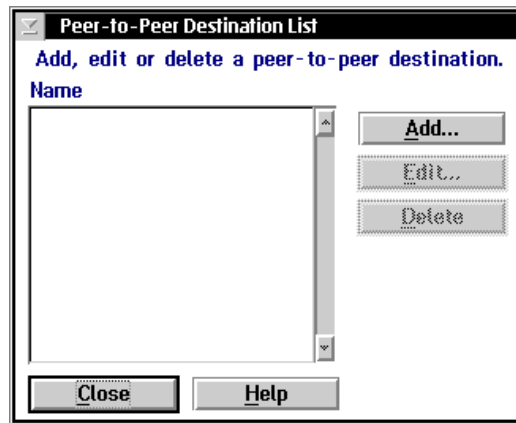
This section describes how to set up the peer-to-peer destination list for your host applications and your data collection devices.

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

- Installed the Model 200 Controller.
- 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. Add, edit, or delete destinations. For help, see "Adding a Destination" in the next section.
3. Choose Close to close the dialog box and return to the main menu.



Adding a Destination

The screenshot shows a dialog box titled "Peer-to-Peer Destination Parameters" with the instruction "Configure this peer-to-peer destination and its transactions." The dialog contains several input fields and controls:

- Destination name:** An empty text input field.
- Hot Standby timeout:** A numeric input field containing "20" followed by the text "seconds (1-9999)".
- Transactions held in volatile memory:** Three radio buttons labeled "None", "Unlimited", and "Maximum". The "Maximum" option is selected. To its right is a numeric input field containing "50" followed by "(1-9999)".
- International text pass-through:** A checkbox that is currently unchecked.
- Transactions:** A section with two list boxes. The "Selected" list is empty. The "Available" list contains the entry "VTDEMO_TRX". Between the lists are buttons for "< Select <" and "> Remove >". Below the "Selected" list are buttons for "Add...", "Edit...", and "Delete".
- Delivery Responses (if any):** A section with two text input fields labeled "Interactive response:" and "Hot Standby:".
- Buttons:** "OK", "Cancel", and "Help" buttons at the bottom of the dialog.

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 controller 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 controller keeps in RAM before it writes the transactions to a Hot Standby file.	None, Unlimited, Maximum	50
International text pass-through	This check box determines how much of the transaction is converted. Check this box to enable this feature. The server converts only the transaction header. Clear this box to use limited EBCDIC mapping. The server converts the entire transaction.	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

To define your peer-to-peer link

1. From the Peer-to-Peer Destination List dialog box, choose Add. The Peer-to-Peer Destination Parameters dialog box appears.
2. In the Destination name field, enter the name of the destination (application) that will accept the transactions in the Transaction box.
3. In the Hot Standby timeout field, enter the number of seconds the controller waits for an acknowledgment from this destination before it places the transactions going to this destination in a Hot Standby file.
4. Choose the number of transactions you want the controller to keep in RAM before it writes them to a Hot Standby file. This setting refers to the transactions the controller is processing. It does not affect the Hot Standby timeout.

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 controller stores in RAM before it writes them to a file.

5. Enable or disable international text pass-through. A check in the check box means that international text pass-through is enabled. For help, see "Using International Text Pass-Through" in the next section.
6. Add all transactions that you want routed to this destination (application) to the Selected list box.
 - a. From the Available list box, select a transaction to be added to the Selected list box.
 - b. Choose Select.
7. Remove any transactions that you do not want routed to this destination from the Selected list box.
 - a. From the Selected list box, select a transaction to be removed.
 - b. Choose Remove.
8. Add, edit, or delete any transactions that are listed in the Selected list box. For help, see "Adding a Transaction" later in this chapter.

9. (Optional) In the Delivery Responses box, enter the messages you want to send to the source of the transaction.
 - In the Interactive response field, enter the message that you want to send to the source of the transaction when the delivery of the transaction to this destination is successful in Interactive mode.
 - In the Hot standby field, enter the message that you want to send to the source of the transaction when the delivery of the transaction for this destination is not immediately successful and is written to a Hot Standby file.
10. Choose OK to save your changes and return to the main menu.

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 Model 200 Controller. 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 controller 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

Model 200 Controller User's Manual

Before you use this feature, note the following:

- The controller 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 for the transaction header and the transaction ID are limited to what you can enter on the controller. 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 controller and devices must use the ASCII character set.
- The controller still supports limited mapping from EBCDIC code page 037 to PC code page 437. If the controller cannot look up the source of the transaction in the peer-to-peer destination list, the controller assumes that EBCDIC mapping is enabled and international text pass-through is disabled. However, if you enable 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 controller does not support sort order, date, item, and currency.

Adding a Transaction

You need to define all transaction IDs that you want the Model 200 Controller to route to the destinations.

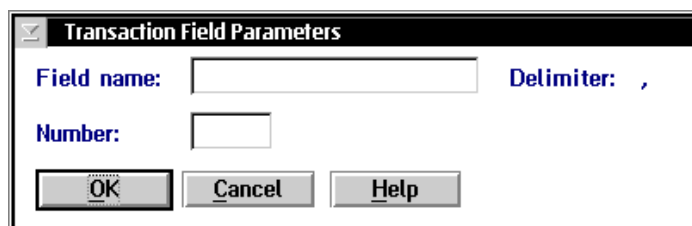
Field	Description	Value	Default
Transaction ID	The unique ID of the transaction.	1 to 20 alphanumeric characters	None
Hot Standby message (Optional)	The message that is sent to the source of the transaction when the controller places the transaction in a Hot Standby file.	1 to 40 characters	None
Delimiter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

To add a transaction

1. From the Peer-to-Peer Destination Parameters dialog box, choose Add. The Transaction Parameters dialog box appears.
2. In the Transaction ID field, enter the unique ID for the transaction.
3. (Optional) In the Hot Standby message field, enter the message that the controller sends to the source of the transaction when it places the transaction in a Hot Standby file.
4. Choose the delimiter for the transaction by clicking the down arrow on the right side of the field. The list of delimiter characters appears. Choose one.
5. Add, edit, or delete transaction fields from the list box. For help, see "Adding a Transaction Field" later in this section.
6. Choose OK to save your changes and return to the Peer-to-Peer Destination Parameters dialog box.

Adding a Transaction Field

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



Field	Description	Value	Default
Field name	The unique name for the transaction field.	1 to 16 alphanumeric characters	None
Number	The position of the field in the transaction.	1 to 9999	None

To add a transaction field

1. From the Transaction Parameters dialog box, choose Add. The Transaction Field Parameters dialog box appears.
2. In the Field name field, enter a name for the transaction field.
3. In the Number field, enter the order or position (for example, 1, 2, or 3) of the field in the transaction. Fields start at 1.
4. Choose OK to save your changes and return to the Transaction Parameters dialog box.

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 your controller, save and activate your run-time configuration. When the save and activate are complete, a message box appears if you need to reboot the controller.

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 controller 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

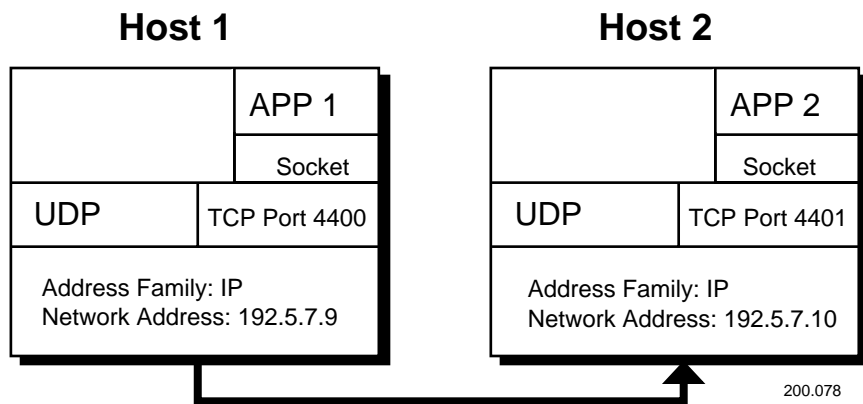
The Model 200 Controller communicates with remote applications using TCP/IP sockets. TCP provides a method for creating connection-oriented, error-free, full-duplex, byte-stream communications between two processes. IP provides a method for transmitting blocks of data, called IP datagrams, between hosts. Together, TCP and IP offer reliable, easy-to-use communications.

The controller 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 controller 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 controller, it must have a send and a receive connection.

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

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

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

How the Controller Communicates With Applications

To use the controller NetComms, you must first configure the controller for TCP/IP communications. For help, see "Configuring the TCP/IP Protocol" in Chapters 5 and 6.

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

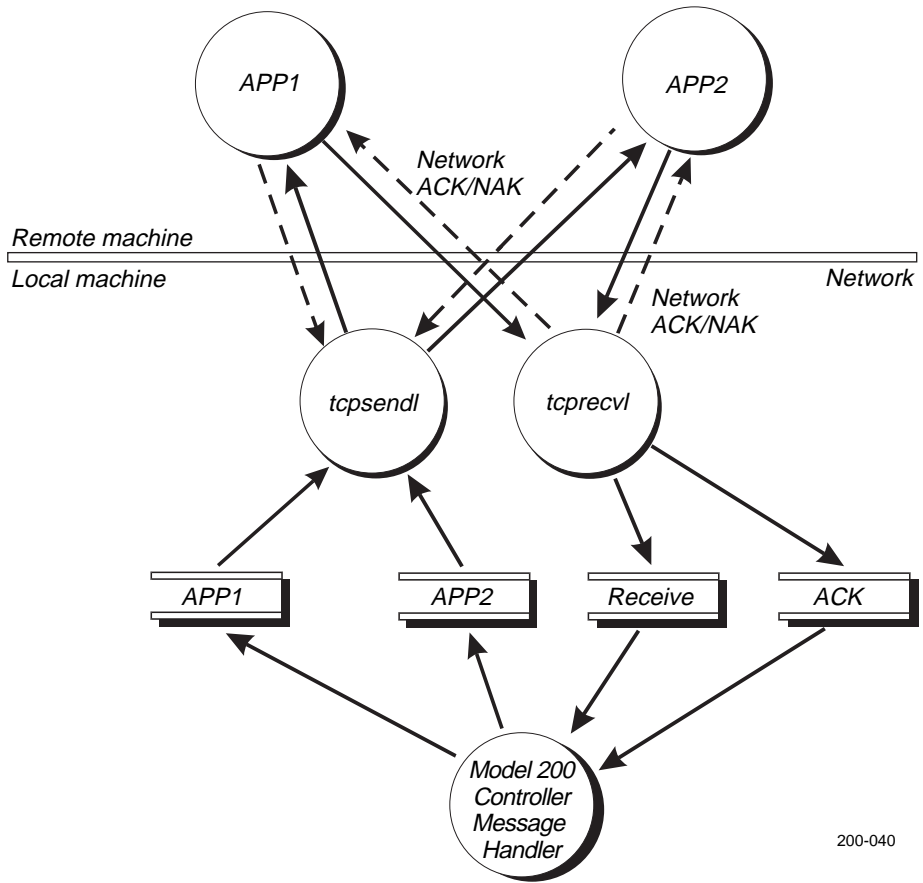
- The controller send NetComm is responsible for creating the application IPC channel and forwarding any data in that channel to the application.
- The controller receive NetComm is responsible for opening the Receive (input) channels of the message handler and for sending data that is received from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

When the controller 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 controller's NetComms communicating directly with applications. NetComms use IPC channels to exchange data with other controller components and they use sockets to exchange data with a TCP/IP application.

Controller NetComms Communicating With Applications



200-040

Understanding Transaction Routing in a TCP/IP Network

The applications you create to interact with the Model 200 Controller function as remote applications.

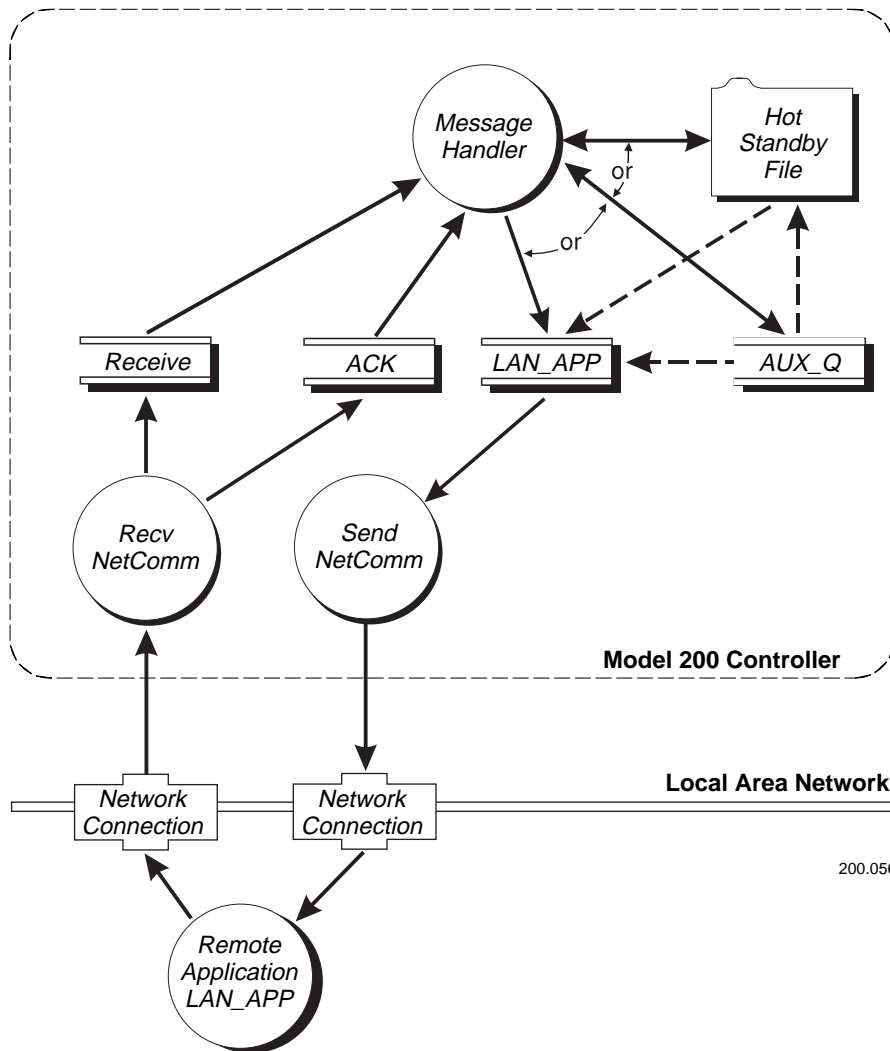
When your application receives a message from the controller, your application must perform these steps:

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 controller, 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 Controller



Model 200 Controller User's Manual

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

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

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

The controller 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 controller, you must pick a realistic value for the Hot Standby timeout so that the controller 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 controller. When an application is inactive, the last transaction sent to the controller 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

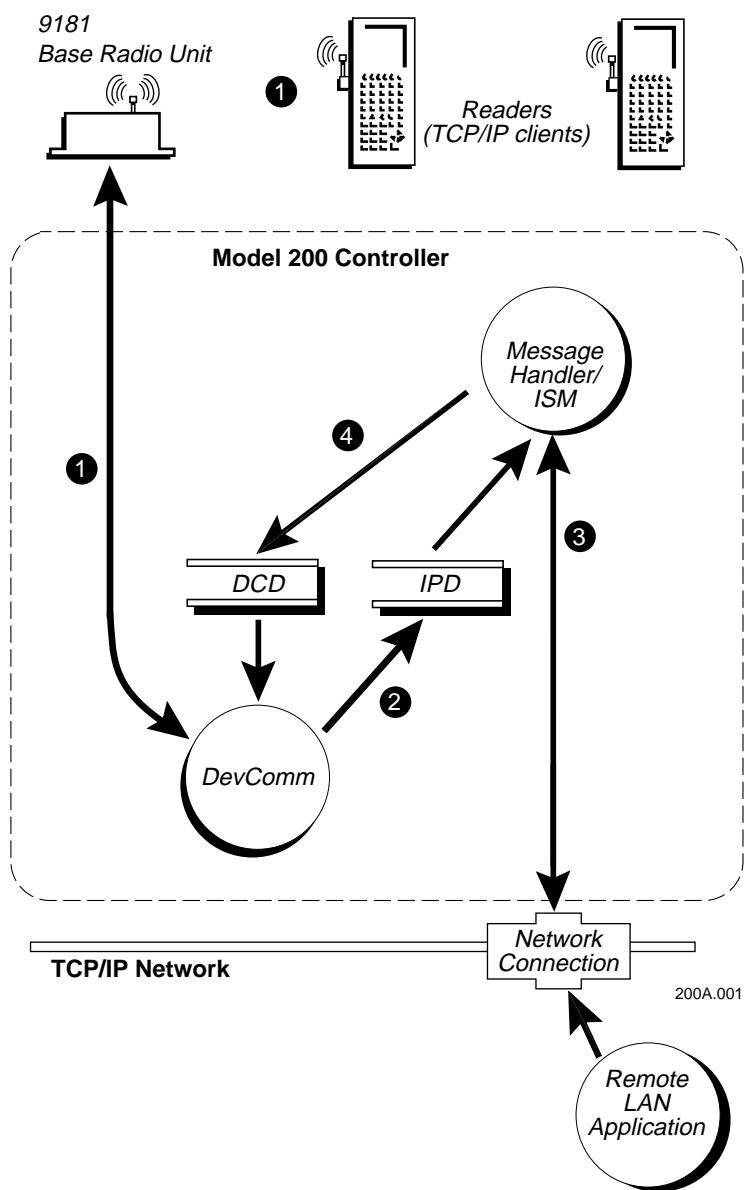
The direct TCP/IP socket interface allows non-TCP/IP capable devices, such as JANUS 900 MHz RF devices and TRAKKER Antares terminals, to establish a TCP/IP socket connection to the host through the Model 200 Controller. For more information on using the direct TCP/IP socket interface, see the *DCS 300 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 Model 200 Controller 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 controller 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 controller. You write your client application to communicate with an existing TCP/IP server application. The server application does not even know the controller 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 controller NetComm API.

The controller 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 controller 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 controller 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 devices and TRAKKER Antares terminals to communicate with the Model 200 Controller using the direct TCP/IP socket interface. Every transaction from a device needs \$IPT as the transaction ID, which allows the controller DevComm to route the data to the proper queue. When a device receives a transaction from the controller, 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 controller.
- Client receives a packet from the controller that acknowledges the request.
 - Client receives an OPEN_NAK (negative acknowledgment) packet from the controller, which indicates the request to open a socket has failed.
 - Client receives an OPEN_ACK (acknowledgment) packet from the controller, which indicates the request to open a socket has succeeded.
- Client sends and receives data to and from the host through the controller. 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 controller indicating that the connection is closed.

About the Host Application Requirements

The controller 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 Model 200 Controller 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 controller 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 controller 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 for the transaction header and the transaction ID are limited by what you can type on the controller. 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 controller and devices must use the ASCII character set.

- The controller supports limited mapping from EBCDIC code page 037 to PC code page 437. If the controller cannot look up the source of the transaction in the peer-to-peer destination list, the controller acts as if EBCDIC mapping is enabled and international text pass-through is disabled. However, if you enable 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 controller does not support sort order, date, item, and currency.

Communicating With APPC Applications

You can use APPC applications to communicate between the Model 200 Controller 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 controller.

APPC applications, acting as remote requester applications, initiate the connection to the controller. The controller acts as a server, which 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 controller a valid application name when it connects. The application name must be identical to the name configured for it in the controller.

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

Note: The controller'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 controller. 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 controller to communicate over an SNA network to other devices supporting APPC/LU 6.2. The controller uses APPC to route the data between remote applications and itself. In an SNA network there are two parts to communications: the controller and the host. The controller 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 controller. For a description of their functions, see the *DCS 300 Technical Reference Manual*.

MC_ALLOCATE
MC_CONFIRM
MC_CONFIRMED
MC_DEALLOCATE
MC_RECEIVE_AND_WAIT
MC_REQUEST_TO_SEND
MC_SEND_DATA
 CONFIRM
 FLUSH
 DEALLOCATE
 NONE

Model 200 Controller User's Manual

MC_SEND_ERROR
CONFIRM
FLUSH
ABEND
RECEIVE_ALLOCATE

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 controller's transaction header to "A."

NetComm Pairs

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

Controller 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 Model 200 Controller to communicate with your LAN and you have configured your controller 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 controller. You can use these terminal sessions for running screen mapping as explained in Chapter 11, "Using Screen Mapping."

Chapter Checklist

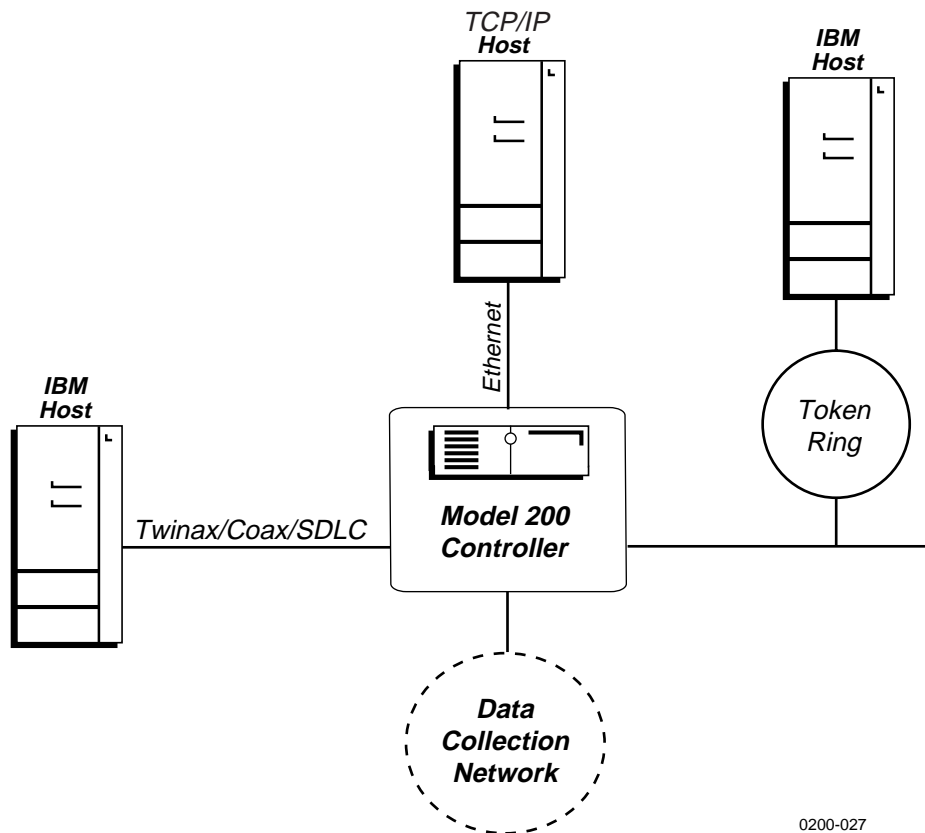
Done?	Task	Page
<input type="checkbox"/>	Configure the host for terminal sessions	10-5
<input type="checkbox"/>	Configure the VT terminal sessions on the Model 200 Controller.	10-6
	Or,	
<input type="checkbox"/>	Configure the 5250 terminal sessions on the Model 200 Controller.	10-15
	Or,	
<input type="checkbox"/>	Configure the 3270 terminal sessions on the Model 200 Controller.	10-21
<input type="checkbox"/>	Save and activate the configuration.	10-25
<input type="checkbox"/>	Start a host session.	10-26
<input type="checkbox"/>	(Optional) Map terminal keyboards to the DCS 300 keyboard.	10-27

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

About Terminal Sessions

You can establish VT, ANSI, 5250, or 3270 terminal sessions between the controller and your host. Use these sessions on the controller to access your host directly from the controller. 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."



0200-027

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 must 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 controller. You need to know this parameter when configuring the controller.

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 Model 200 Controller
- the maximum frame (I) size
- the local location address (NAU) for the controller, 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 Model 200 Controller and your host. You can use these sessions to access the host from the controller or you can use them for screen mapping sessions.

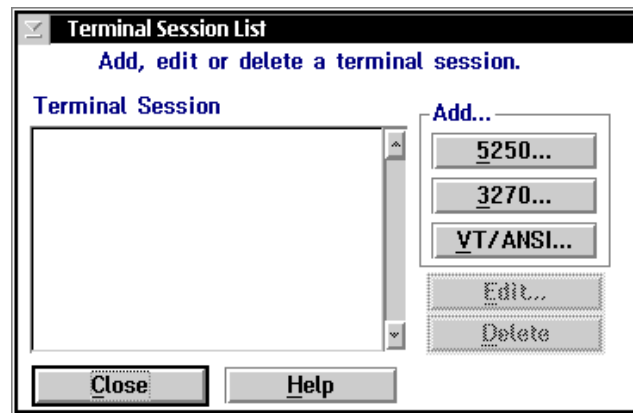
One terminal session on the Model 200 Controller can communicate with one terminal emulator session running on the host. However, the terminal session on the controller can receive transactions from multiple data collection devices.

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

- Installed the Model 200 Controller.
- Installed and configured the connection points and downline devices.
- Configured 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. The Terminal Session list box lists all the sessions that are already defined. From this dialog box you can add new sessions, or you can edit and delete existing 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

Use this dialog box to configure VT/ANSI terminal sessions between your Model 200 Controller and your host. You also need to define terminal sessions that you can use for screen mapping sessions.

Field	Description	Value	Default
Session name	A meaningful name for this terminal session.	1 to 8 alphanumeric characters	None
Terminal 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.	Predefined	None

Field	Description	Value	Default
Number of sessions	The number of terminal sessions that you want to run on the controller.	1 to 228	1
Port number	The port number that this session uses to communicate with the telnet daemon on the host.	0 to 65535	23

To set up a VT/ANSI terminal session.

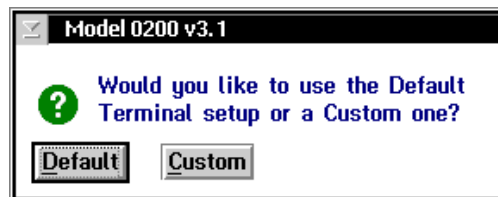
1. In the Session name field, enter a meaningful name for the session.
2. In the Terminal mode field, click the down arrow on the right side of the field. A list that contains the different terminal modes appears. Select the type of terminal mode that you want to use for this terminal session.
3. In the Host Name box, click the down arrow on the right side of the field. A list that contains existing TCP/IP host names appears. Select the host that you want to connect with for this session.

Or, you can add, edit, or delete a host. For help, see “Adding a TCP/IP Host” later in this section.

4. In the Number of sessions field, enter the number of terminal sessions that you want to run on the controller.
5. In the Port number field, enter the port number on which this session will communicate with the telnet daemon on the host.

Note: Telnet uses port number 23 (default).

6. Choose OK to save your changes. This message box appears:

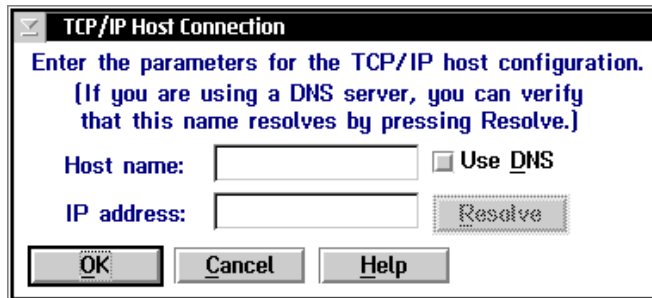


7. Choose Default to use the default terminal setup. The message box closes and you return to the Terminal Session List dialog box.

Or, choose Custom to customize the terminal setup. The VT Setup dialog box appears. For help, see "Customizing the VT Terminal Setup" later in this chapter.
8. Choose Close to close the Terminal Session List dialog box and to return to the main menu.

Adding a TCP/IP Host

To communicate with TCP/IP hosts, the Model 200 Controller must know their IP addresses. You can either use DNS to resolve these IP addresses or you can enter them in manually.



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.	Check, Clear	Clear
IP address	The address that identifies the TCP/IP host to the network.	xxx.xxx.xxx.xxx where xxx is a value between 0 and 255	None

To determine the host's IP address using DNS

1. From the Terminal Session Definition dialog box, choose Add. The TCP/IP Host Connection dialog box appears.
2. In the Host name field, enter the abbreviated or long host name. If you enter the abbreviated name, the controller searches the domain names in the DNS Configuration dialog box to determine the long host name.
3. Enable the Use DNS check box.

Note: Before you enable this check box, you must first configure a DNS server in the DNS Configuration dialog box.

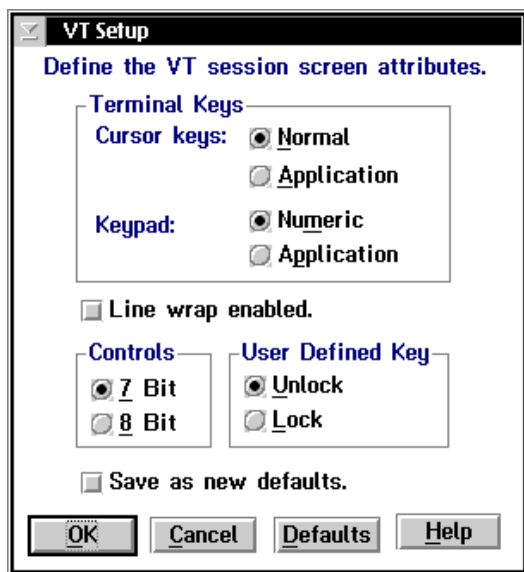
4. (Optional) Choose Resolve. The server searches for the host name in the domains that are listed in the DNS Configuration dialog box and resolves the IP address.
5. Choose OK to save your changes and return to the Terminal Session Definition dialog box.

To configure the host's IP address manually

1. From the Terminal Session Definition dialog box, choose Add. The TCP/IP Host Connection dialog box appears.
2. In the Host name field, enter the host name.
3. Make sure the Use DNS check box is disabled.
4. In the IP address field, enter the host's IP address.
5. 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 you choose Custom, the VT Setup dialog box automatically 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.



Field	Description	Value	Default
Cursor keys	Determines whether the arrow keys on the terminal control cursor movement or they send their application control functions.	Normal, Application	Normal
Keypad	Determines whether the number keys on the terminal send their keycap characters or they send their programming functions.	Numeric, Application	Numeric
Line wrap enabled	This check box determines if text automatically wraps to the next line when it reaches the right margin.	Check, Clear	Clear
Controls	Defines the type of control characters that your terminal uses.	7 bit, 8 bit	7 bit
User-Defined Key	Determines whether or not the host can change the user-defined keys.	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

To customize the terminal setup

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

1. In the Terminal Keys box, choose Normal if you want to use the terminal cursor keys to move the cursor.
Choose Application if you want the cursor keys to send their application control function.
2. In the Terminal Keys box, choose Numeric if you want the terminal number keys to send their numbers.
Choose Application if you want the terminal number keys to send their programming functions.

Model 200 Controller User's Manual

3. Enable or disable the text to automatically wrap to the next line when it reaches the right margin.

If line wrap is disabled, 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.

4. In the Controls box, choose 7-bit if you want the terminal to use all the VT320 features. This mode also supports 8-bit graphic display characters and 7-bit control characters. Choose this setting for all VT220 applications.

Choose 8-bit if you want the terminal to use all the VT320 features in an 8-bit environment with 8-bit control characters. Choose this setting for VT220 applications that use 8-bit control characters.

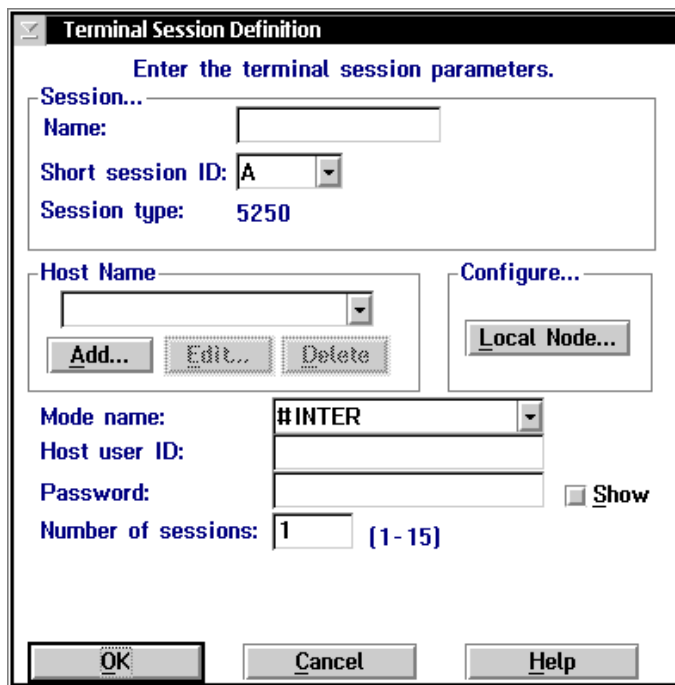
5. In the User-Defined Key box, choose Lock if you do not want the host to change the user-defined key definitions.

Choose Unlock if you want the host to be able to add or to change the user-defined key definitions.

6. Choose Defaults if you want to use the current custom terminal configuration as the default for all other terminals of the same type.
7. Choose OK to save your changes and to return to the main menu.

Adding a 5250 Terminal Session

Use this dialog box to configure 5250 terminal sessions between your Model 200 Controller and your host. You also need to define terminal sessions that you can use for screen mapping sessions.



The dialog box is titled "Terminal Session Definition" and contains the following fields and controls:

- Session...:** A section containing:
 - Name:** A text input field.
 - Short session ID:** A dropdown menu with "A" selected.
 - Session type:** A dropdown menu with "5250" selected.
- Host Name:** A dropdown menu with a list of host names.
- Configure...:** A section containing:
 - Local Node...:** A button.
- Buttons:** "Add...", "Edit...", and "Delete" buttons are located below the Host Name dropdown.
- Mode name:** A dropdown menu with "#INTER" selected.
- Host user ID:** A text input field.
- Password:** A text input field with a "Show" checkbox to its right.
- Number of sessions:** A text input field with "1" and a range indicator "(1-15)".
- Bottom Buttons:** "OK", "Cancel", and "Help" buttons.

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.

Model 200 Controller User's Manual

Field	Description	Value	Default
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. 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 <i>DCS 300 Technical Reference Manual</i> .	Predefined	#INTER
Host user ID	The user ID that lets you log into the host.	1 to 10 alphanumeric characters	None
Password	The password that goes with the user ID that lets you log in to the host.	1 to 10 alphanumeric characters	None
Show	This check box determines if your password appears in the Password field.	Check, Clear	Clear
Number of sessions	The number of terminal sessions you want to configure to this host.	See Step 9.	1

To add a terminal session

1. In the Terminal Session List dialog box, choose 5250. The Terminal Session Definition dialog box appears.
2. In the Session box, enter a unique long session ID for the session.
3. In the Session box, enter the Short session ID. The ID defaults to the next available alpha character.
4. In the Host Name box, click the down arrow on the right side of the field. A list that contains existing host names appears. Select the host that you want to connect with for this session.

Or, if you do not have any host names in the list box, follow the instructions for “Adding an IBM SNA Host” in the next section. You can also edit and delete hosts.

5. If you have not identified the controller to the SNA network, choose Local Node. The SNA Local Node Information dialog box appears. For help, see “Configuring the Controller SNA Node” later in this chapter.
6. In the Mode name field, click the down arrow on the right side of the field. A list of IBM modes appears. These modes define the class of service and other session characteristics that you may want for your network design. Select a mode name.
7. In the Host user ID field, enter the user ID that allows you to log in to the AS/400.
8. In the Password field, enter the password that goes with your user ID that allows you to log in to the AS/400.

If you do not enable the Show check box, asterisks appear instead of the keys you are typing.

If you enable the Show check box, the keys you are typing appear in the field.

9. In the Number of sessions field, enter the number of terminal sessions you want to run on the controller.

Type	Coax	Non-Coax
5250	N/A	1-14

10. Choose OK to save your changes and return to the Terminal Session List dialog box.

Adding an IBM SNA Host

You need to identify any hosts you want the Model 200 Controller 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 that is associated with that session still exists. Only one host connection is allowed for coaxial, twinaxial, and SDLC network adapter cards.

The controller 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, twinaxial, SDLC	Ethernet 1

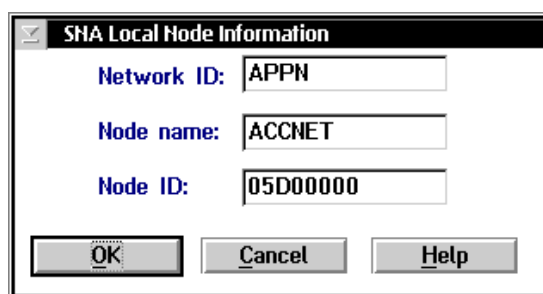
Field	Description	Value	Default
Network ID	Identifies the network ID on which the host resides. This ID must match the network ID configured on the host.	1 to 8 alphanumeric characters	Controller's network ID from the SNA local node definition
Host LU	The LU name that identifies the host. This parameter 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 controller that allows it to communicate, when running TE, with more than one host.	8 uppercase alphanumeric or special characters 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.	Token ring MAC address format	None

To add a host

1. In the Terminal Session Definition dialog box in the Host Name box, choose Add. The Host Connection Configuration dialog box appears.
2. (Optional) In the Host name field, enter a meaningful name for the host.
3. In the Adapter card field, click the down arrow on the right side of the field. Select the adapter that you are using to connect to the host.
4. In the Network ID field, enter the network ID of the network on which the host resides.
5. In the Host LU field, enter the LU name that identifies the host.
6. In the Address field, enter the LAN adapter address of the remote host. For help, see "Converting Ethernet Addresses to Token Ring MAC Format" in Appendix B.
7. Choose OK to save your changes and return to the 5250/3270 Terminal Session Definition dialog box.

Configuring the Controller SNA Node

These parameters identify the Model 200 Controller to the SNA network. Once configured, these parameters apply system-wide for all SNA connection types and you do not need set them again.



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 controller. 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.	8 hexadecimal characters	05D00000

To configure the controller SNA node

1. From the Terminal Session Definition dialog box, choose Local Node. The SNA Local Node Information dialog box appears.
2. In the Node name field, enter the name that other nodes will use to address the Model 200 Controller.
3. In the Network ID field, enter the network name used to create a unique SNA network.

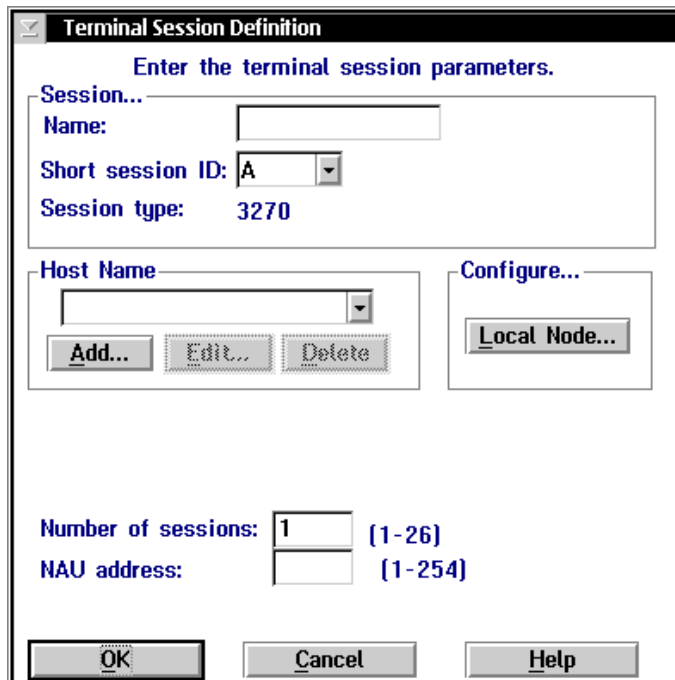
4. In the Node ID field, enter the last eight characters in the XID that establish a host connection. The Node ID is the same as the XID.

Note: When establishing a connection, the host or controller with the higher Node ID number is the primary workstation.

5. Choose OK to save your changes and return to the Terminal Session Definition dialog box.

Adding a 3270 Terminal Session

Use this dialog box to configure terminal sessions between your Model 200 Controller and your host. You also need to define terminal sessions that you can use for screen mapping sessions.



The image shows a dialog box titled "Terminal Session Definition". The title bar includes a close button (X) and the text "Terminal Session Definition". Below the title bar, the text "Enter the terminal session parameters." is displayed. The dialog box contains several input fields and buttons:

- Session...:** A group box containing:
 - Name:** An empty text input field.
 - Short session ID:** A dropdown menu with "A" selected.
 - Session type:** A text input field containing "3270".
- Host Name:** A dropdown menu with a downward arrow.
- Configure...:** A group box containing a button labeled "Local Node...".
- Buttons:** Three buttons labeled "Add...", "Edit...", and "Delete" are positioned below the Host Name dropdown.
- Number of sessions:** A text input field containing "1" followed by the range "(1-26)".
- NAU address:** An empty text input field followed by the range "(1-254)".
- Bottom Buttons:** Three buttons labeled "OK", "Cancel", and "Help" are located at the bottom of the dialog box.

Model 200 Controller User's Manual

Field	Description	Value	Default
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.	Predefined	None
Number of sessions	The number of terminal sessions you want to configure to this host.	See Step 6.	1
NAU address	The network addressable unit (NAU) that is specified for the workstation LU name.	001 to 254	None

To add a terminal session

1. In the Terminal Session List dialog box, choose 3270. The Terminal Session Definition dialog box appears.
2. In the Session box, enter a unique long session ID for the session.
3. In the Session box, enter the Short session ID. The ID defaults to the next available alpha character.
4. In the Host Name box, click the down arrow on the right side of the field. A list that contains existing host names appears. Select the host that you want to connect with for this session.

Or, if you do not have any host names in the list box, follow the instructions for "Adding an IBM SNA Host" later in this chapter. You can also edit and delete hosts.
5. If you have not identified the controller to the SNA network, choose Local Node. The SNA Local Node Information dialog box appears. For help, see "Configuring the Controller SNA Node" earlier in this chapter.

6. In the Number of sessions field, enter the number of terminal sessions you want to run on the controller.

Type	Coax	Non-Coax
3270	1-4	1-25

7. In the NAU address field, enter the NAU address that is specified for the workstation LU name.
8. Choose OK to save your changes and return to the Terminal Session List dialog box.

Adding an IBM SNA Host

You need to identify any hosts you want the Model 200 Controller 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 controller 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.

Model 200 Controller User's Manual

Host Connection Configuration
 Configure the host to adapter connection.

Host name:

Adapter card:

Network ID:

Host LU:

Local PU:

Address:

Node ID:

OK Cancel Help

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 controller that allows it to communicate, when running TE, with more than one host.	8 uppercase alphanumeric or special characters 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.	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 controller.	8 hexadecimal characters	05D00000

To add a host

1. In the Terminal Session Definition dialog box in the Host Name box, choose Add. The Host Connection Configuration dialog box appears.
2. (Optional) In the Host name field, enter a meaningful name for the host.
3. In the Adapter card field, click the down arrow on the right side of the field. A list that contains the available adapters appears. Select the adapter you are using to connect to the host.
4. In the Address field, enter the LAN adapter address of the remote host. For help, see “Converting Ethernet Addresses to Token Ring MAC Format” in Appendix B.
5. In the Node ID field, enter the unique ID of the host. The Node ID is the same as the XID.

Note: When establishing a connection, the host or controller with the higher Node ID number is the primary workstation.

6. Choose OK to save your changes and return to the Terminal Session Definition dialog box.

Saving and Activating Your Run-Time Configuration

When you finish configuring your terminal sessions, you should save your changes. If you are done configuring your controller, activate your run-time configuration. When the activate is complete, a message box appears if you need to reboot the controller.

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 controller 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.

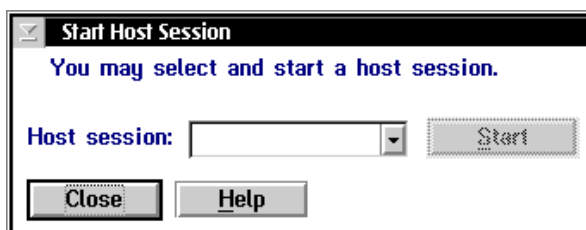
Starting a Host Session

You can start host sessions between the controller and your host. Use the session on the controller to access your host directly from the controller. 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 Model 200 Controller Keyboard

Use these diagrams to help you map terminal emulation keys to the Model 200 Controller keyboard.

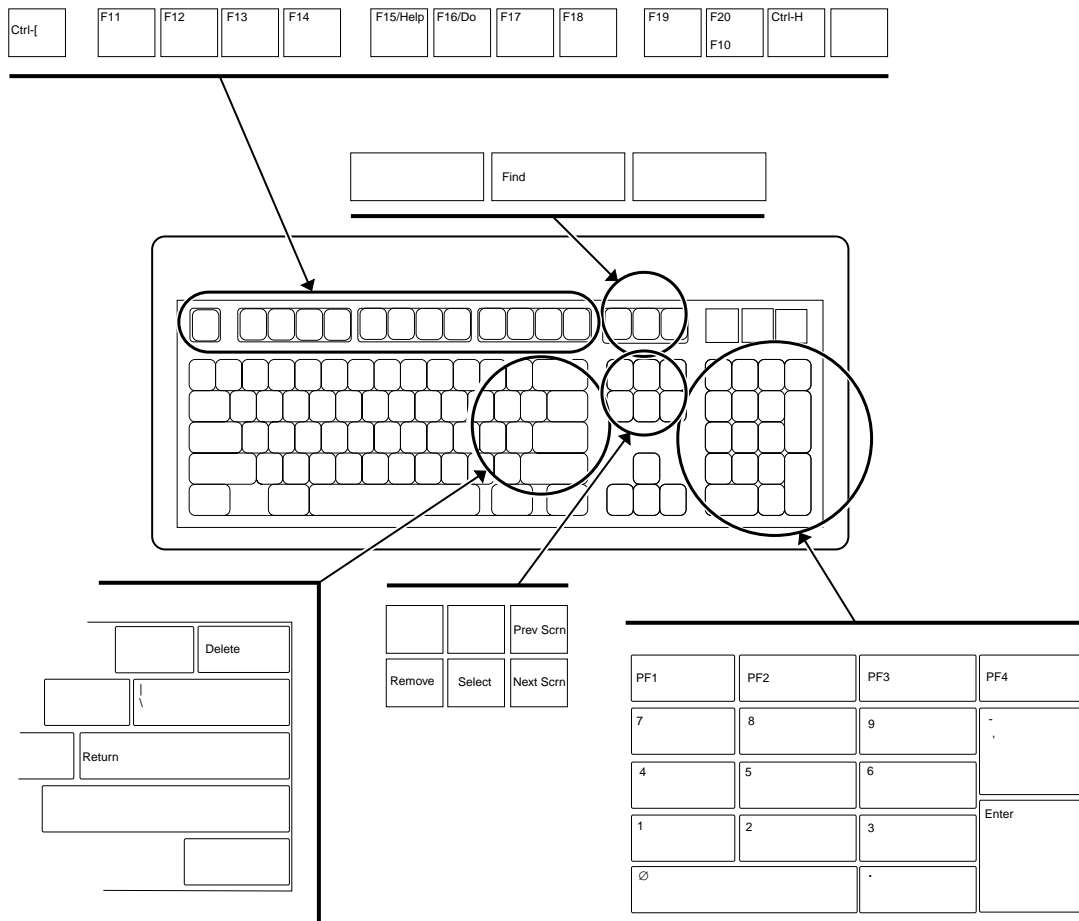
To use the diagrams

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 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**.

Model 200 Controller User's Manual

VT/ANSI Terminal Keyboard

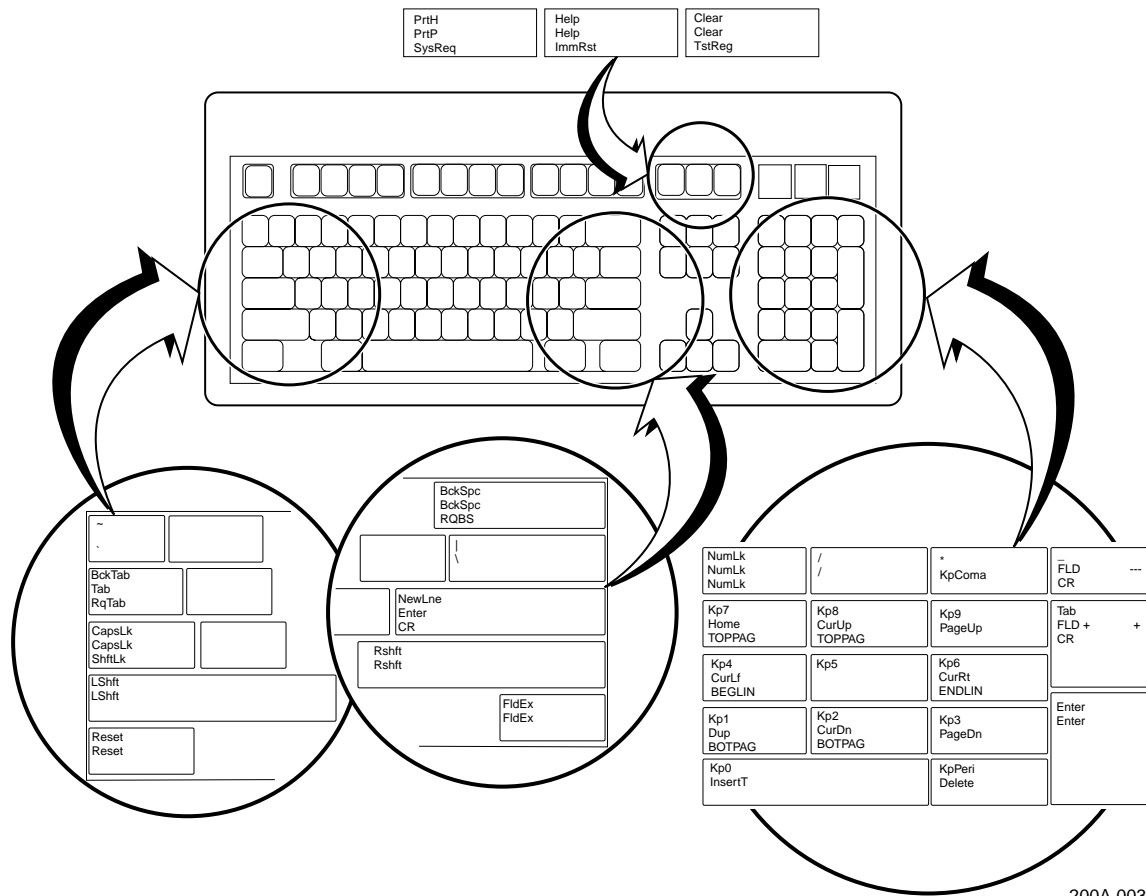


200A.004

Key Combination Legend

Shift
Base

5250 Terminal Keyboard



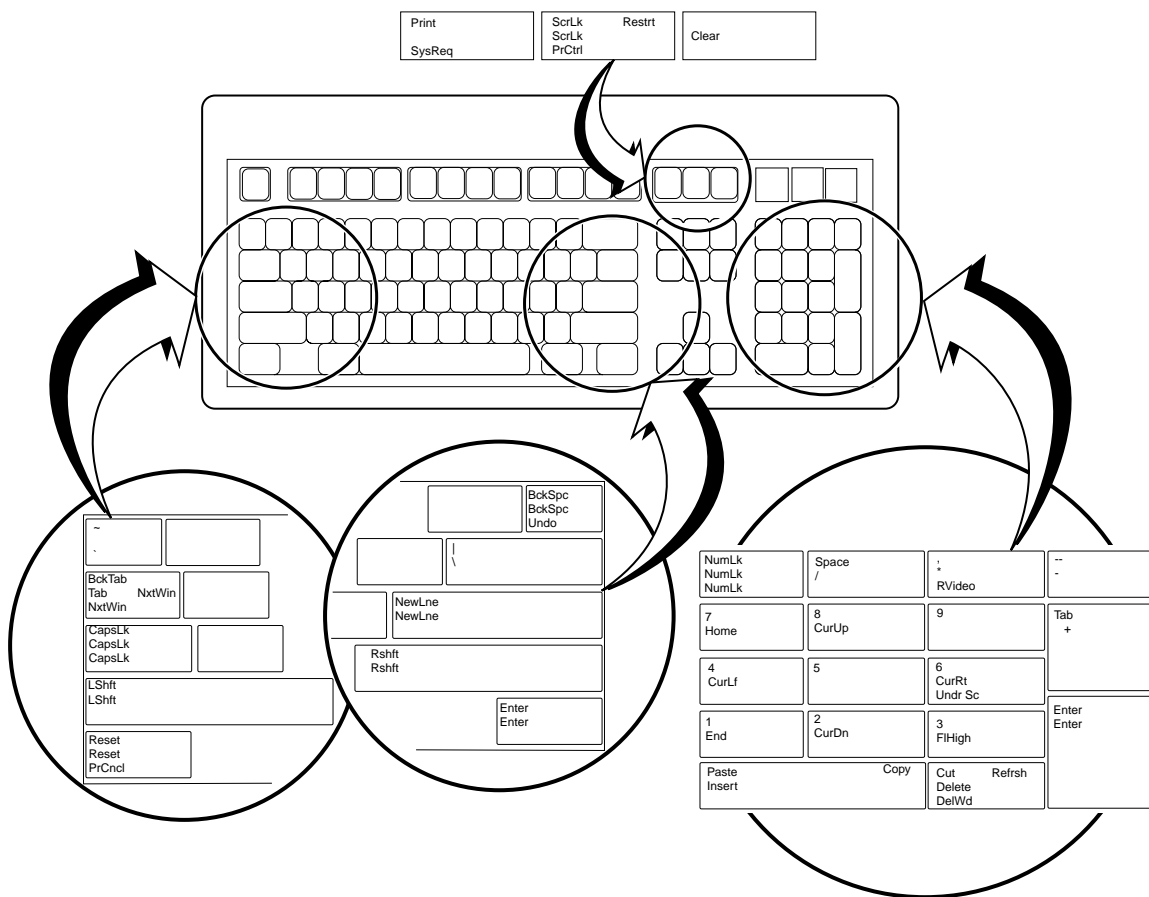
200A.003

Key Combination Legend

Shift	Ctrl
Base	AltGr
Alt	

Model 200 Controller User's Manual

3270 Terminal Keyboard



200A.002

Key Combination Legend

Shift	Ctrl
Base	AltGr
Alt	Alt+Shift

11

Using Screen Mapping

Now that you have configured the Model 200 Controller to communicate with your LAN and you have configured your controller to communicate with your Intermec network, you are ready to tie the entire data collection network together using an application, such as 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 build templates for screen mapping and 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.

Chapter Checklist

Done?	Task	Page
<input type="checkbox"/>	Create a new or open an existing script file.	11-7
<input type="checkbox"/>	Set global options for the current script.	11-22
<input type="checkbox"/>	Create standard sequences for starting and ending screen mapping sessions.	11-26
<input type="checkbox"/>	Define all transactions that the current script uses.	11-34
<input type="checkbox"/>	Select a current transaction.	11-34
<input type="checkbox"/>	Define all the host screens that receive data from the current transaction.	11-63
<input type="checkbox"/>	Select a current host screen.	11-36
<input type="checkbox"/>	Define all host screen fields, regions, and messages for the current host screen.	11-39

Chapter Checklist (continued)

Done?	Task	Page
<input type="checkbox"/>	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.	
<input type="checkbox"/>	Repeat the preceding six steps until you have defined all transactions.	
<input type="checkbox"/>	Determine the order of events.	11-59
<input type="checkbox"/>	Define user blocks.	11-65
<input type="checkbox"/>	View and check the script.	11-69
<input type="checkbox"/>	Configure the screen mapping sessions on the Model 200 Controller.	11-76
<input type="checkbox"/>	Build the terminal screens and group them into menus.	11-83
<input type="checkbox"/>	Generate the terminal templates from the menus.	11-102
<input type="checkbox"/>	Map the transaction fields to the host screen fields.	11-80
<input type="checkbox"/>	Save the configuration.	11-83
<input type="checkbox"/>	Download the reader program to your JANUS devices.	11-109
<input type="checkbox"/>	Download the template to your JANUS devices and your TRAKKER Antares terminals.	11-113 11-118

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

About Screen Mapping

Screen mapping lets you map transaction fields from a JANUS device or a TRAKKER Antares terminal to different host screen fields in a host application. On the Model 200 Controller, you use the Script Builder Tool to create a script file that the controller uses to map transaction fields from the data collection 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.

While defining your script, you build the screens for the terminals, group them into menus, and generate each menu into a terminal template. This terminal template runs on your JANUS device or TRAKKER Antares terminal. You can either use the reader program to request the terminal template from the controller or you can download the template from the controller to your data collection devices.

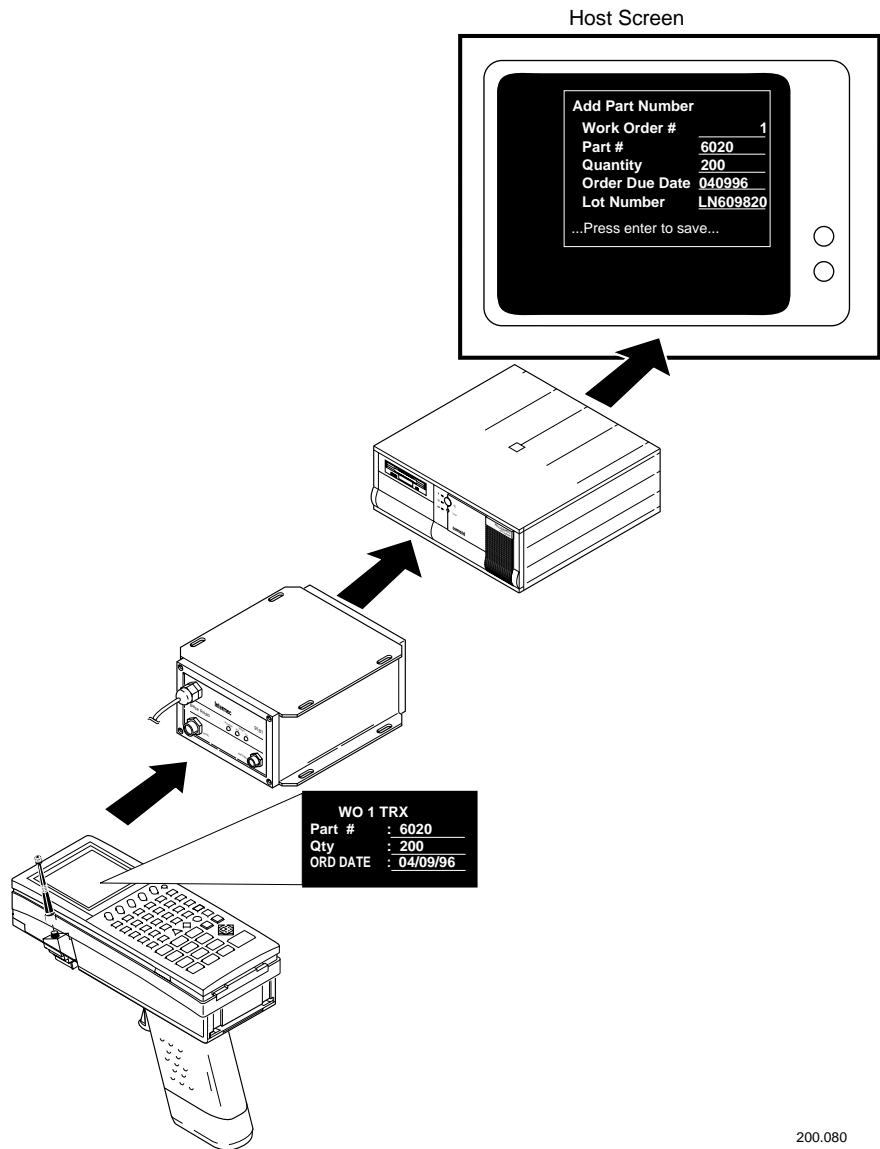
You also need to create screen mapping sessions that define specific transactions to be sent to a specific host terminal session using a specific script file. Screen mapping sessions allow multiple terminal sessions on the controller to simultaneously communicate with multiple terminal emulator sessions running on different hosts.

Before you run screen mapping, you need to download the terminal template application (RDRPGM.EXE) to your JANUS devices. Intermecc has already loaded this program on your TRAKKER Antares terminals.

Model 200 Controller User's Manual

This figure shows data originating from a JR2020 being sent through a BRU to the controller to a host application running in a terminal emulator.

Typical Screen Mapping Application



200.080

About Script Files

Script files contain the logic for mapping the transaction data that is exchanged between data collection devices and a host. Using script files, the controller 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. The Script Builder Tool also helps you build your terminal application and generate it before you download it to your data collection devices.

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

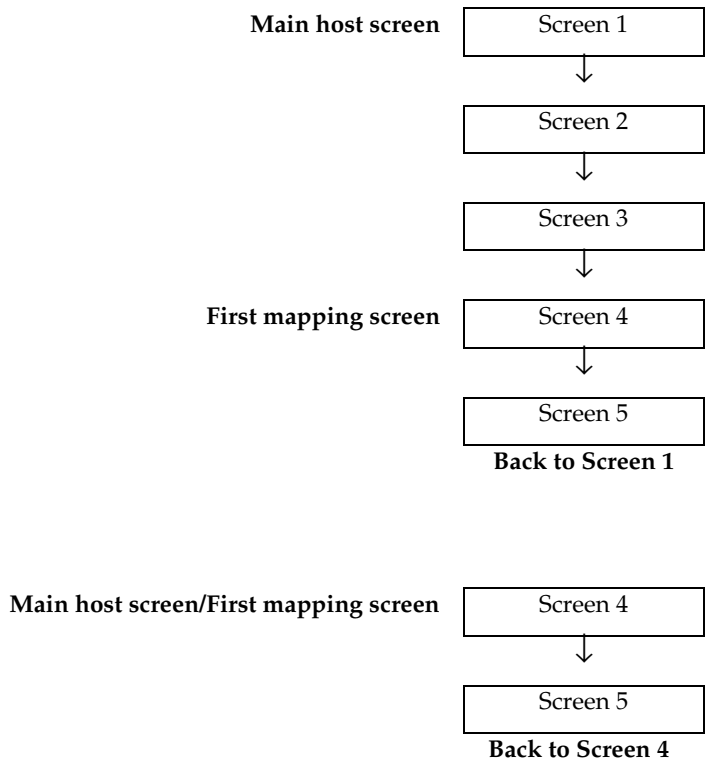
You can build a script file that contains only one transaction or you can build a script file that contains many transactions, as long as they all branch from one host screen. A single transaction script file is the easiest to build. However, if you have too many single transaction script files running at the same time, you can use up system resources and the controller 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.

This example shows how using a single transaction script file can reduce overhead on the system. The first figure 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 figure 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

```

A - A - 5250 Emulator
File Edit Settings Keyboard Help
Sign On
System . . . . . : BIGBLUE
Subsystem . . . . : QINTER
Display . . . . . : MAGICA

User . . . . . : BHSU
Password . . . . . :
Program/procedure . . . . . :
Menu . . . . . :
Current Library . . . . . :

(C) COPYRIGHT IBM CORP. 1988, 1996.
20*# 5250PLU A 0-0
```

Screen 2

```

A - A - 5250 Emulator
File Edit Settings Keyboard Help
MAIN AS/400 Main Menu System: BIGBLUE

Select one of the following:

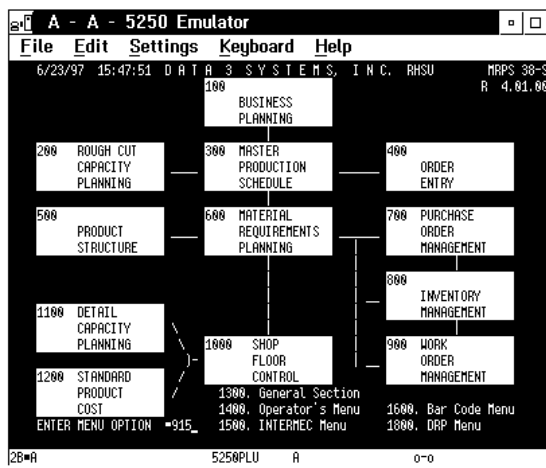
1. User tasks
2. Office tasks
3. General system tasks
4. Files, libraries, and folders
5. Programming
6. Communications
7. Define or change the system
8. Problem handling
9. Display a menu
10. Information Assistant options
11. Client Access tasks

90. Sign off

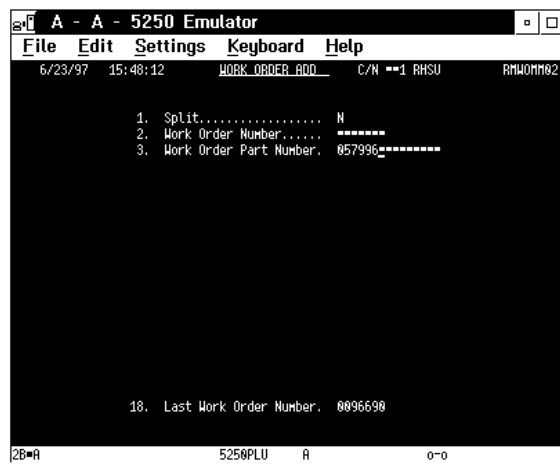
Selection or command
==> CALL C1SIGNON

F3=Exit F4=Prompt F9=Retrieve F12=Cancel F13=Information Assistant
F23=Set initial menu
(C) COPYRIGHT IBM CORP. 1988, 1996.
20*# 5250PLU A 0-0
```

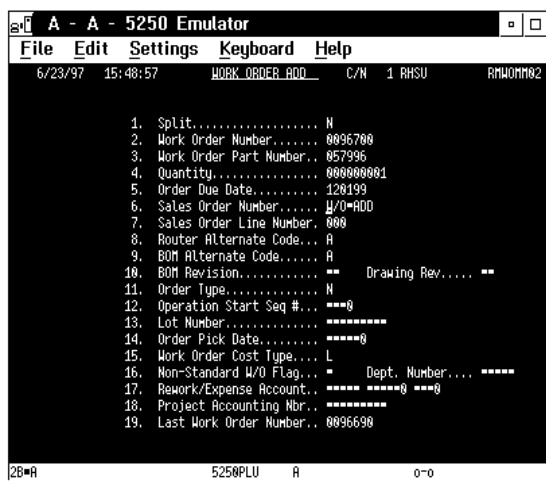
Screen 3



Screen 4 (Main Host Screen)



Screen 5



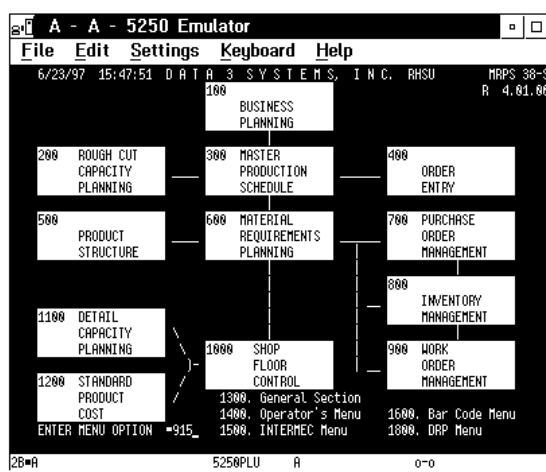
Example 2 - Multiple Transaction Script File

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)

```

A - A - 5250 Emulator
File Edit Settings Keyboard Help
6/23/97 15:48:12 WORK_ORDER_ADD C/N **1 RHSU RHWOM02

1. Split..... N
2. Work Order Number..... *****
3. Work Order Part Number. 057996*****

18. Last Work Order Number, 0096690

2B#A 5250PLU A 0*0
    
```

Screen 5

```

A - A - 5250 Emulator
File Edit Settings Keyboard Help
6/23/97 15:48:57 WORK_ORDER_ADD C/N 1 RHSU RHWOM02

1. Split..... N
2. Work Order Number..... 0096700
3. Work Order Part Number.. 057996
4. Quantity..... 00000001
5. Order Due Date..... 120199
6. Sales Order Number..... W/O#00
7. Sales Order Line Number. 000
8. Router Alternate Code... A
9. BOM Alternate Code..... A
10. BOM Revision..... ** Drawing Rev.... **
11. Order Type..... N
12. Operation Start Seq #... ==0
13. Lot Number..... *****
14. Order Pick Date..... *****
15. Work Order Cost Type... L
16. Non-Standard W/O Flag... Dept. Number... *****
17. Rework/Expense Account. *****0 *****
18. Project Accounting Nbr., *****
19. Last Work Order Number.. 0096690

2B#A 5250PLU A 0*0
    
```

Screen 6 (Menu Option 910)

```

A - A - 5250 Emulator
File Edit Settings Keyboard Help
7/16/97 15:41:35 WORK_ORDER_SUMMARY FTLE INDUPLY C/N **1 RHSU RHWOM02
BY WORK_ORDER_NUMBER
WORK ORDER: 0065060_

2B#A HW 5250PLU 0*0
    
```

Screen 7

```

A - A - 5250 Emulator
File Edit Settings Keyboard Help
7/16/97 15:42:03 WORK_ORDER_SUMMARY FTLE INDUPLY C/N 1 RHSU RHWOM02
BY WORK_ORDER_NUMBER
WORK ORDER: 0065060
ACTIVE PART NUMBER: J020200 LOT NUMBER
DESCRIPTION COMMUNICATION DOCK J2020 BUYER/PLANNER 475
SEL ORDER # ORD DATE ORDER QTY QTY OPEN DUE DATE SALES # IPZ/SIS
- 0065060 10/18/96 5 5 1/01/98 W/O ADD N 00

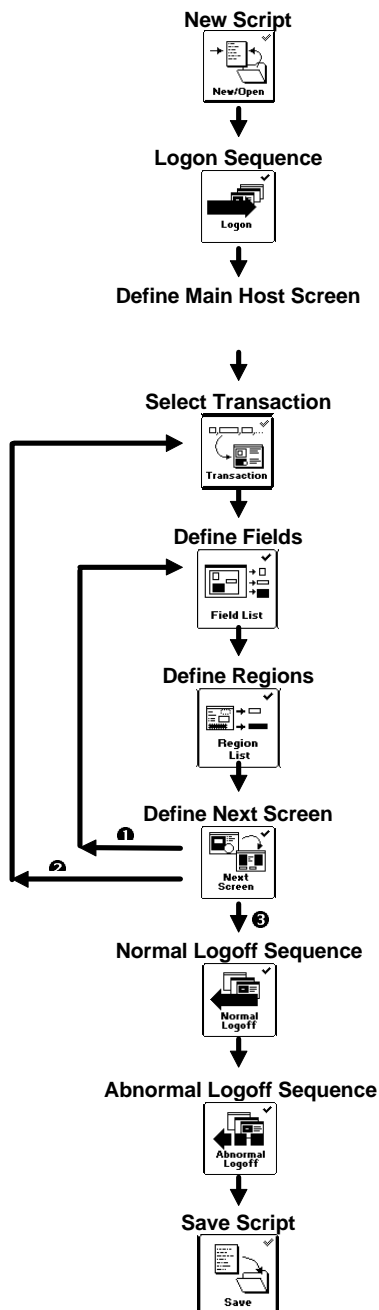
2B#A HW 5250PLU 0*0
    
```

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 Name	Description
1	New/Open	Start data collection on the controller. Create a new script file and select a temporary host session for capturing keystrokes.
2	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 a current transaction by either adding a new transaction or selecting an existing transaction and choosing Current.
4	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	Define the regions for the current screen. Regions can handle errors on the host screen and they can output data.
6	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	Capture the keystrokes that take the user from the main host screen to the logoff screen.
8	Abnormal Logoff (Optional)	Capture the keystrokes that take the user from any screen to the logoff screen.
9	Save	Save the script file. You should save the script file periodically while you work.

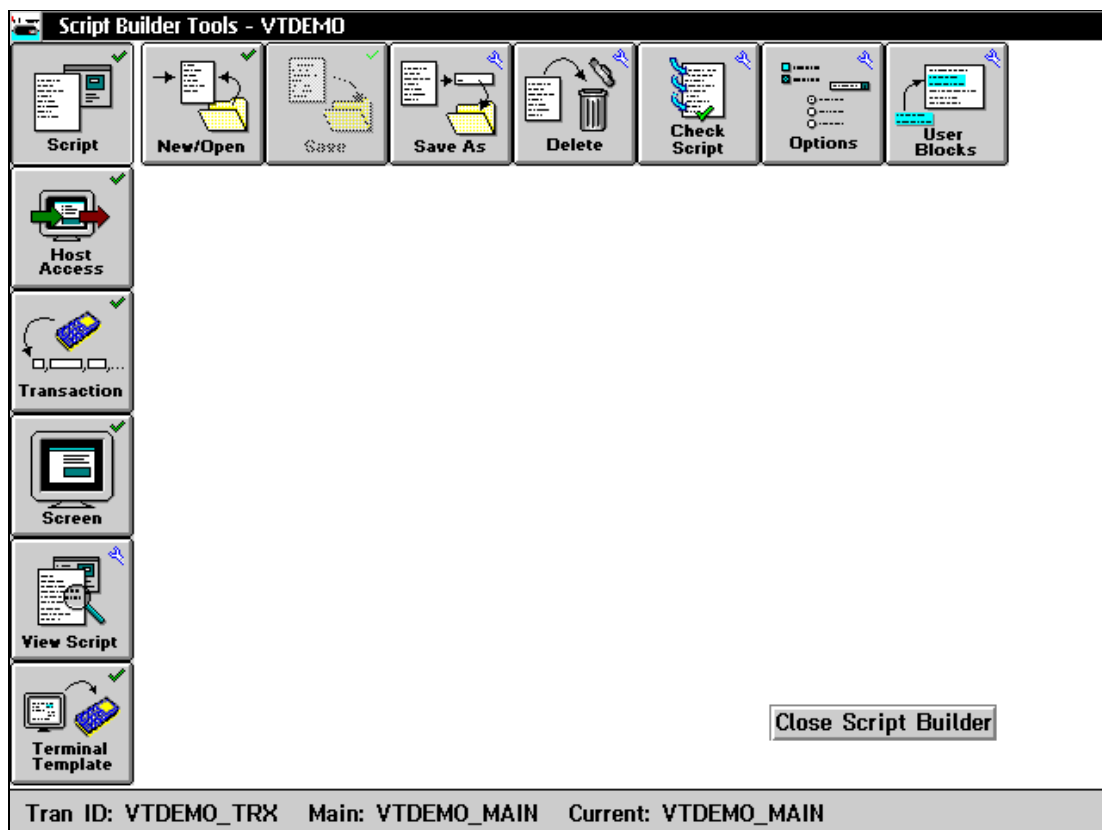
Script Builder Tool Flow Chart



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

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.	Predefined	None

To create a new script file

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, enter a unique name for the script.
4. (Optional) In the Description box, enter a description for the script.

5. (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: 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.

6. (Optional) Choose Start Session. The host window opens.
7. Choose OK to return to the Script Builder Tools window.

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 controller, 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.

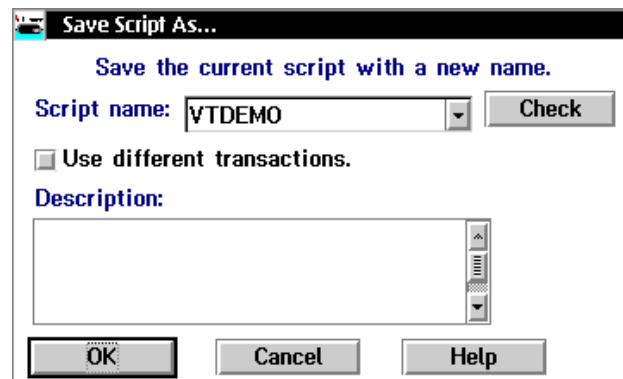
Note: This toolbar button will not be available until you make changes to a new or existing script file.

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.

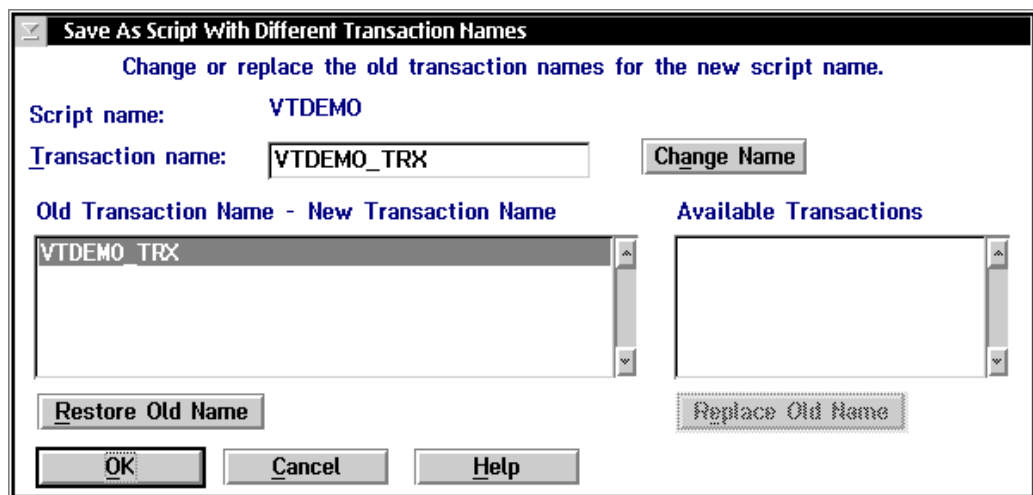


6. In the Script name field, enter a unique name for the new script.
Or, click the down arrow on the right side of the field. A list of existing script names appears. Select one.
7. In the Description box, enter a new description for the script.

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.



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.

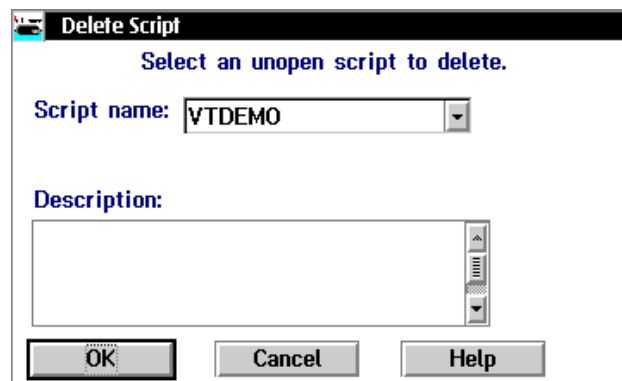
10. If you want to restore the old transaction name or if you want to choose another new transaction name, select the old transaction name from the Old Transaction Name - New Transaction Name list box and choose Restore Old Name.

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.

Field	Description	Value	Default
Response timeout	Sets the number of minutes that the controller waits for a "host busy" condition to clear.	1 to 9999	2
Reset on timeout	This check box determines if the controller 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 controller 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 controller to wait before it assumes that the host is ready for more data.	100 to 99999	500
EHELLAPI mnemonic	EHELLAPI 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.	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 controller sends a message to the source of the transaction when the last transaction is received in batch mode.	Check, Clear	Check
Audit Options	Determines the level of auditing the controller performs.	Off, On, No continue	Off

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.
3. In the Response timeout field, enter the number of minutes you want the controller to wait for a host busy condition to clear.
4. Enable the Reset on timeout check box if you want to send a Reset key to the host when it is busy.
5. Choose the appropriate option button that determines if the controller retries the connection to the host application when an error occurs. If you choose Limit, enter the number of times you want the controller to retry the connection.
6. In the EHLLAPI mnemonic field, enter the character that you want to represent special keys. This character must not occur in any static text of a message or in any script keystroke name.
7. (VT/ANSI only) In the Data response timeout field, enter the number of milliseconds of inactivity you want the controller to wait before it assumes that the host is ready for the next transaction.
8. In the Concatenation char field, enter the character that you want the script to use to concatenate components of a message. This character must not occur in any explicit string of the script. However, this character may appear in transaction data.
9. Enable the Process batch transactions check box if you want the controller to process batch transactions.
10. Enable the Send to source when batch transaction received check box if you want the controller to send a message to the source of the transaction when the last transaction in batch mode is received.

***Note:** If the Process batch transactions check box is not enabled, this check box is disabled.*

11. Choose the level of auditing you want the controller to perform. If you enable auditing, when a non-fatal error occurs, the controller 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.
12. Choose OK to return to the Script Builder Tools window.
Choose Defaults if you want to set this dialog box to default values.

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 controller waits before it assumes that the host is finished sending data. That is, the controller listens on the TCP/IP socket and if there is no activity and the timeout period expires, the controller performs the next action. However, there is no guarantee that the host is finished sending data.

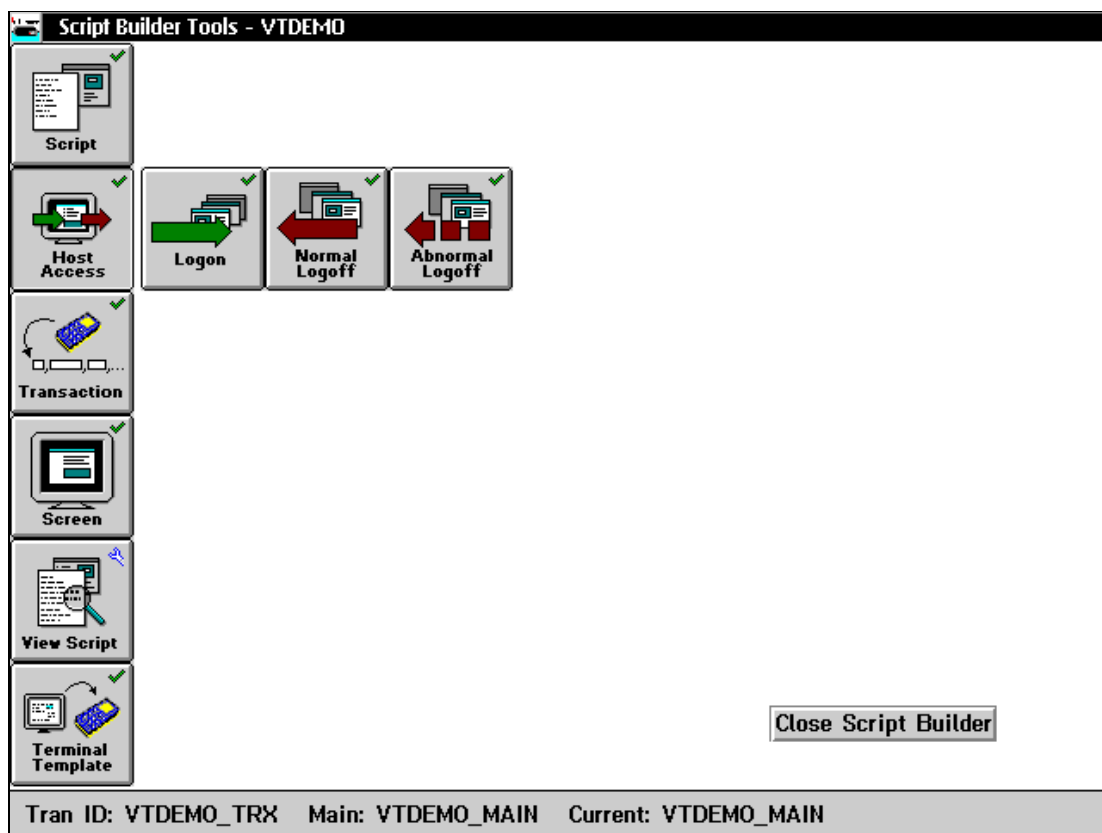
Note: The controller may not wait the entire timeout period if an action is performed successfully. For example, the PUT_TRANS_FIELD command waits until the cursor is at the field location or it may wait for the data response timeout to expire, whichever comes first.

You set the data response timeout field when you set the script options. Use this field to tune the controller to your network environment. If you set the data response timeout too long, it will affect controller 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 controller encounters a critical error.

Before you can capture keystrokes, you need to start a temporary host session. For help, see "Creating a New Script File" earlier in this chapter.



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.

The screenshot shows a dialog box titled "Logon Sequence". At the top, it says "Capture the keystrokes to logon and navigate to the main host screen. Select or define the screen below." Below this is a "Control Capture" section with instructions: "Press Start to begin capturing keystrokes entered in the host screen. Press Stop to end capture." There are "Start" and "Stop" buttons. The "Captured Keystrokes" section contains a list box with the following text: ""INTERMEC", "NEWLN", ""D:", "NEWLN", and ""CD". To the right of the list box are buttons for "Delete", "Delete All", "Change", "Before", and "After". Below the list box is a "Selected Keystroke" label and an empty text field. At the bottom, there are fields for "Main screen:" (set to "VTDEMO_MAIN"), "Row, Column:" (set to "1,27"), and "Screen ID:" (set to "Add Part Number"). There is a "Define..." button next to the "Main screen:" field. At the very bottom are "OK", "Cancel", and "Help" buttons.

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.

Normal Logoff Sequence

Capture the keystrokes to normally exit the host application and logoff.

Control Capture

Press Start to begin capturing keystrokes entered in the host screen. Press Stop to end capture.

Start **Stop**

Captured Keystrokes

PF4
"EXIT"
NEWLN

Delete
Delete All
Change
Before
After

Selected Keystroke **Insert**

OK **Cancel** **Help**

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 controller encounters a critical error.

Note: Some host applications may not allow abnormal logoff sequences.

The screenshot shows a dialog box titled "Abnormal Logoff Sequence". The dialog contains the following elements:

- Title Bar:** Abnormal Logoff Sequence
- Instructions:** Capture the keystrokes to exit the host application and logoff when unknown errors occur.
- Control Capture Section:**
 - Text: Press Start to begin capturing keystrokes entered in the host screen. Press Stop to end capture.
 - Buttons: Start, Stop
- Captured Keystrokes Section:**
 - A list box for capturing keystrokes.
 - Buttons: Delete, Delete All, Change
- Selected Keystroke Section:**
 - Text: Selected Keystroke
 - Text: Insert
 - Buttons: Before, After
- Bottom Buttons:** OK, Cancel, Help

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.

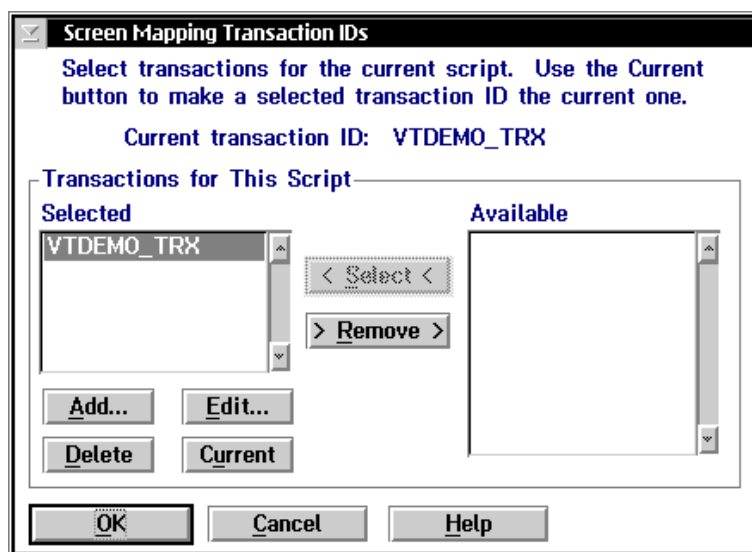
Inserting New Lines in the Captured Keystrokes Box

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. 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.

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.



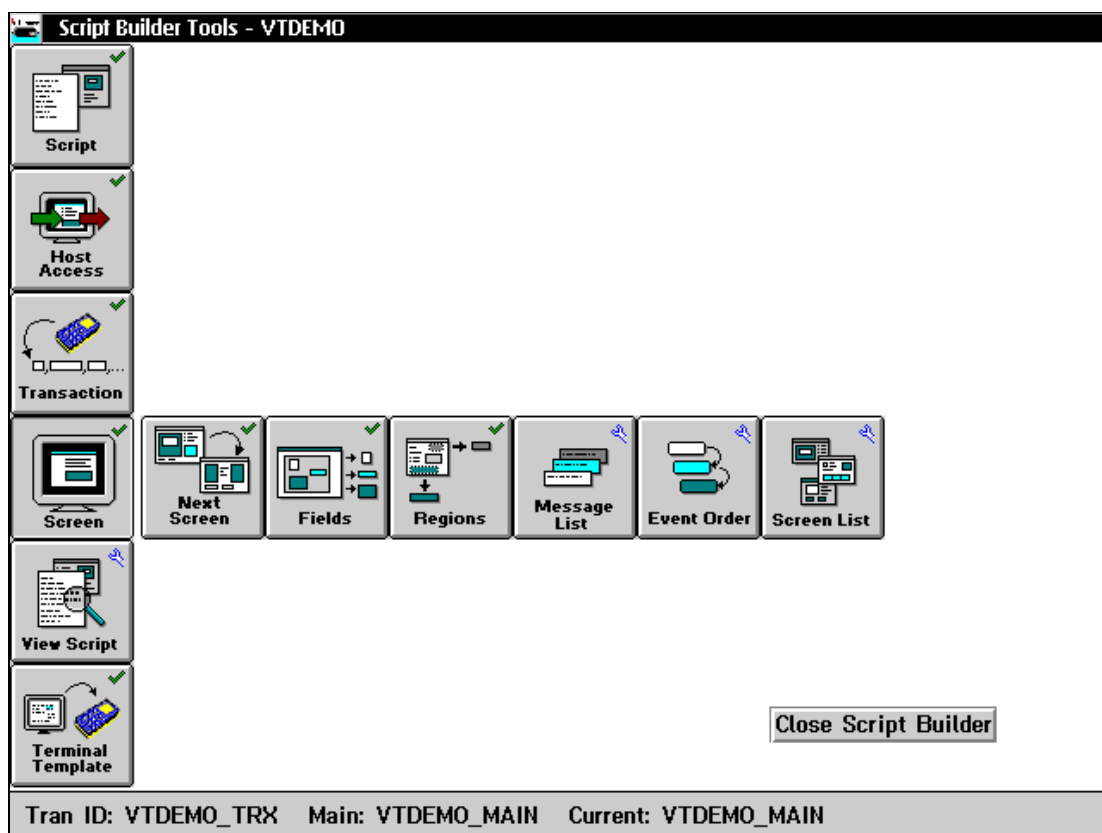
Field	Description	Value	Default
Selected	This list box contains the transactions that this script handles.	None	None
Available	This list box contains all the transactions that are available to use with this script.	Predefined	None

To select the transactions for the script

1. From the Script Builder Tools window, choose Transaction. The Screen Mapping Transaction IDs dialog box appears.
2. Add all transactions that you want to use for this script to the Selected list box.
 - a. From the Available list box, select a transaction to be added to the Selected list box.
 - b. Choose Select.
3. Remove any transactions that you do not want to use for this script from the Selected list box.
 - a. From the Selected list box, select a transaction to be removed.
 - b. Choose Remove.
4. Add, edit, or delete any transactions that are listed in the Selected list box. For help, see “Adding a Transaction” in Chapter 9.
5. In the Selected list box, select the transaction whose fields you want to map to host screen fields and choose Current.
6. Choose OK to return to the Script Builder Tools window.

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.

Choose Yes in the Next Screen? 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.

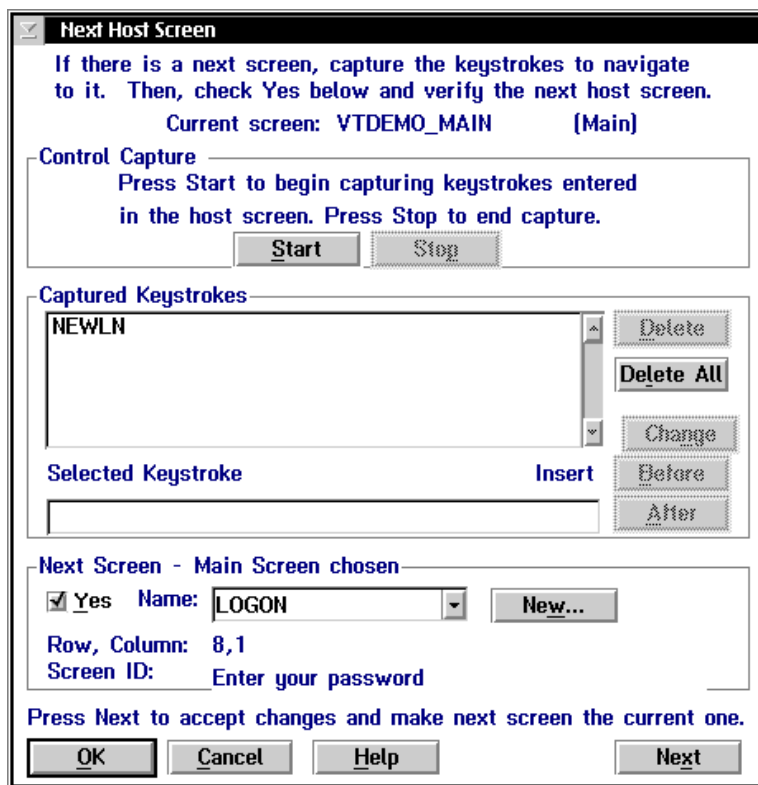
Note: Before you can use the capture keystrokes feature, you must start a temporary host session. For help, see “Starting a Host Session” in Chapter 10.

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.



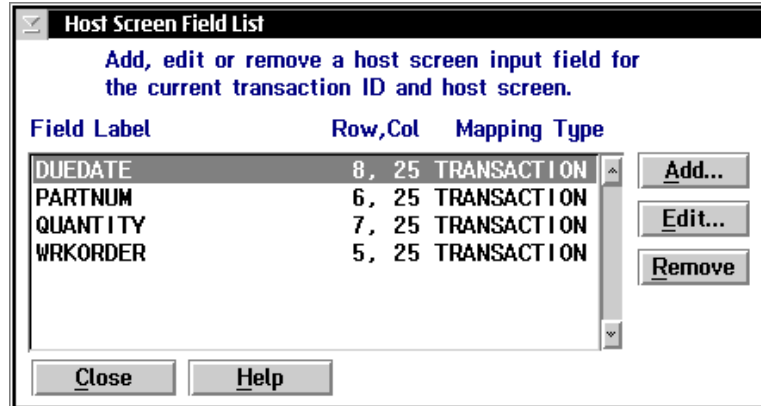
7. Check Yes in the Next Screen box if you want to assign the next screen.
To select an existing host screen for the next screen, click the down arrow on the right side of the field. A list of host screens appears. Select the host screen that you want to follow the Current screen.
Or, to define a new 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 need to 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.

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

Field	Description	Value	Default
Transaction field number	The number of the transaction field whose data is mapped to the host screen field.	Predefined	(new)
Static string	The string that is mapped to the host screen field.	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

To add a host screen field

1. From the Host Screen Field List dialog box, choose Add. The Host Screen Field Definition dialog box appears.
2. In the Field label field, click the down arrow on the right side of the field. A list of all the available host screen fields for the current host screen in other transactions appears. Select a field label. The row, column, and length information for the field is automatically entered.
Or, enter a unique name for the host screen field.
3. If you started a temporary host session for this script, use the Get Field feature to automatically detect the location of the field. For help, see “Getting Host Screen Field Attributes From a Host Screen” later in this chapter.
 - a. On the host window, position your cursor on the field.
 - b. In the Host Screen Field Definition dialog box, choose Get Field. The Row, Column, and Length fields are filled with values.
4. If you did not start a temporary host session, enter the position of the first character of the field and enter the length of the field.
 - a. In the Row and Column fields, enter the position of the first character of the field.
 - b. In the Length field, enter the maximum number of characters the field accepts.

5. Determine how the host screen field will receive its data.
 - Choose Transaction field number, if the data for the host screen field is mapped from a transaction field sent by a terminal. Click the down arrow on the right side of the field. A drop-down list of all the existing transaction field numbers appears. Select the number of the transaction field that sends data to this host screen field.

Or, 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.
 - Choose Static string if the data for the host screen field comes from a static string. Enter the string.
6. In the Keystrokes to exit field, click the down arrow on the right side of the field. A list of keystroke mnemonics appears. Choose the mnemonic that exits the field, or enter a new mnemonic.
7. Choose OK to return to the Host Screen Field List dialog box.

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 selected 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.

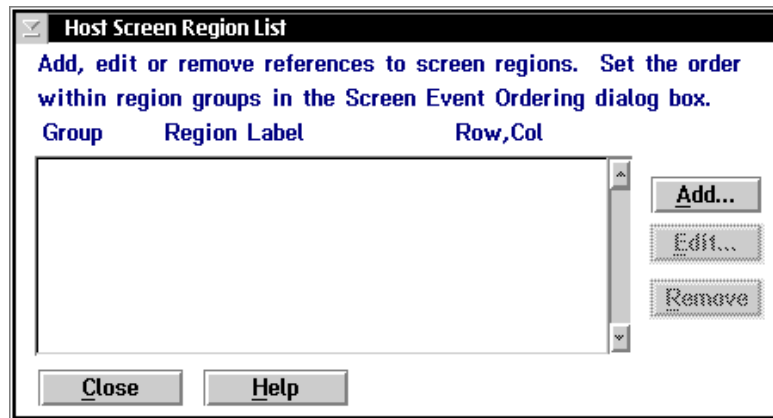
Selecting Regions for the Current Host Screen

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. You may not need to define any actions. 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 Region List. 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

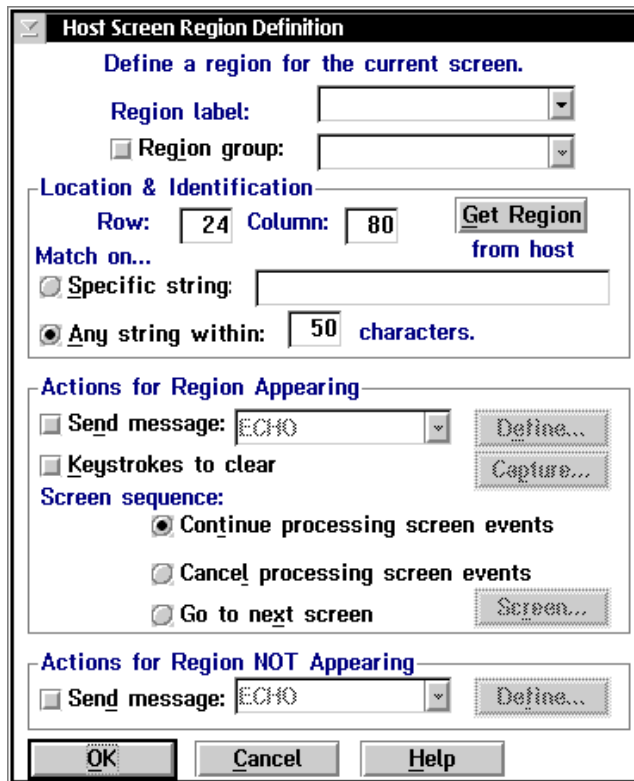
There are three types of actions that you can define when a region appears:

- 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.



The dialog box is titled "Host Screen Region Definition" and contains the following sections:

- Define a region for the current screen.**
 - Region label: [text box]
 - Region group: [text box]
- Location & Identification**
 - Row: [24] Column: [80]
 - Match on...
 - Specific string: [text box]
 - Any string within: [50] characters.
- Actions for Region Appearing**
 - Send message: [ECHO]
 - Keystrokes to clear
 - Screen sequence:
 - Continue processing screen events
 - Cancel processing screen events
 - Go to next screen
- Actions for Region NOT Appearing**
 - Send message: [ECHO]

Buttons at the bottom:

Model 200 Controller User's Manual

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 controller uses to identify the region.	Specific string, Any string within	Any string within
Specific string	From the specified row and column positions, this option button defines a specific string the controller must identify before it recognizes the region.	1 to 80 alphanumeric characters	None
Any string within	From the specified row position, this option button and field specify the length of the region. The controller identifies the region if any string appears within this length.	1 to 999	50
Send message (Optional)	This check box indicates that if the region is recognized, a message is sent to the source.	Check, Clear	Clear
Keystrokes to clear (Optional)	This check box lets you define a keystroke sequence that clears the region.	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

Field	Description	Value	Default
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.		
Go to next screen	This option button indicates that the script file goes to another host screen.	Check, Clear	Clear
Send message	This check box determines if a message is sent to the source of the transaction if the region does not appear.	Check, Clear	Clear

To add a region

1. From the Host Screen Region List dialog box, choose Add. The Host Screen Region Definition dialog box appears.
2. In the Region label field, click the down arrow on the right side of the field. A list of all the available regions for the current host screen appears. Select a region. The row, column, and length information for the field is automatically entered.
3. (Optional) Enable the Region group check box and click the down arrow on the right side of the field. A list of existing groups appears. Select a group. Groups of regions share the same actions in the Action for Region NOT appearing box if none of the regions in the group appear.
Or, enter a new group name in the field.
4. Choose the option button that tells the controller how to recognize the region.
 - Choose Specific string and enter the string if the region is only recognized if the string appears at the specified location.
 - Choose Any string within characters and enter a number of characters. A region is recognized if any string exists with the specified number of characters.

Model 200 Controller User's Manual

5. 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. For help, see "Getting a Region From a Host Screen" later in this chapter.
 - a. On the host window, position your cursor on the first character of the region.
 - b. In the Host Screen Region Definition dialog box, choose Get Region. The Row, Column, and Specific String fields are filled with values.
6. If you did not start a temporary host session, enter the location of the first character of the region in the Row and Column fields.
7. (Optional) Enable the Send message check box to send a message to the source of the transaction when the region appears. Click the down arrow on the right side of the field. Choose the message you want to send.
Or, choose Define to create a new message. For help, see "Creating Screen and Region Messages" later in this chapter.
8. (Optional) Enable the Keystrokes to clear check box and then choose Capture to specify keystrokes to clear the region when it appears. For help defining the keystrokes, see "Capturing Keystrokes" later in this chapter.
9. Choose the event that occurs when the region is finished performing its actions.
 - Choose Continue processing screen events if you want the script file to remain on the host screen to continue processing any other defined screen events.
 - Choose Cancel processing screen events if you want the script file to remain on the host screen, but you do not want it to process any other defined screen events.
 - Choose Go to next screen if you want the script file goes to another host screen.
10. Enable the Send message check box if you want to send a message to the source of the transaction when the region does not appear. Click the down arrow on the right side of the field. Choose the message you want to send.
Or, choose Define to create a new message. For help, see "Creating Screen and Region Messages" later in this chapter.
11. Choose OK to return to the Host Screen Region List dialog box.

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.

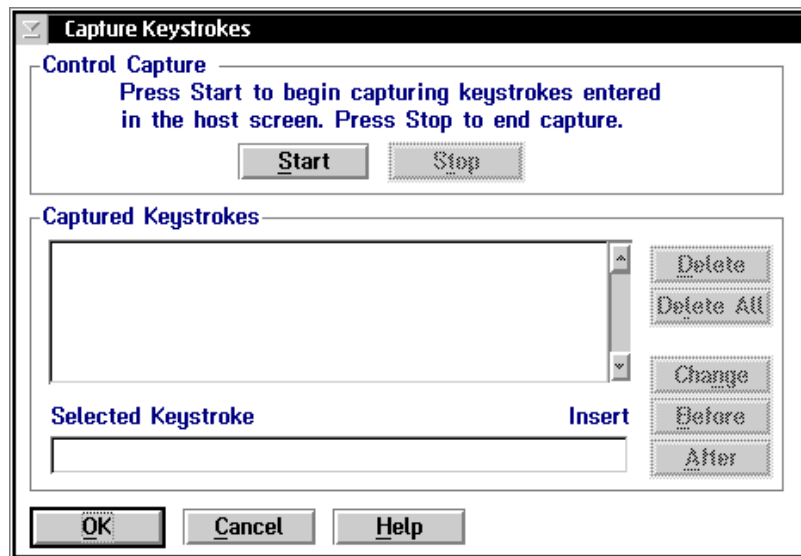
4. In the Host Screen Region Definition dialog box, choose Get Region. The Location & Identification box is populated with the attributes of the region.
5. If necessary, edit the information in the fields.
6. Choose OK to save your changes and return to the Host Region List dialog box.
7. Repeat Steps 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, enable 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.

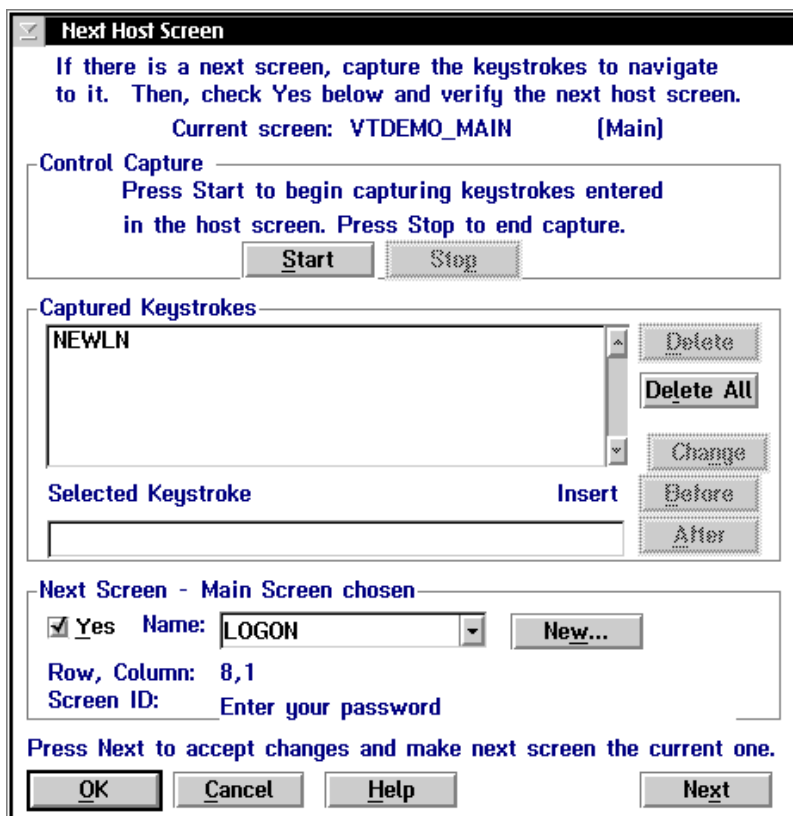
Note: Before you can use the capture keystrokes feature, you must start a temporary host session. For help, see “Starting a Host Session” in Chapter 10.

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. 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 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.

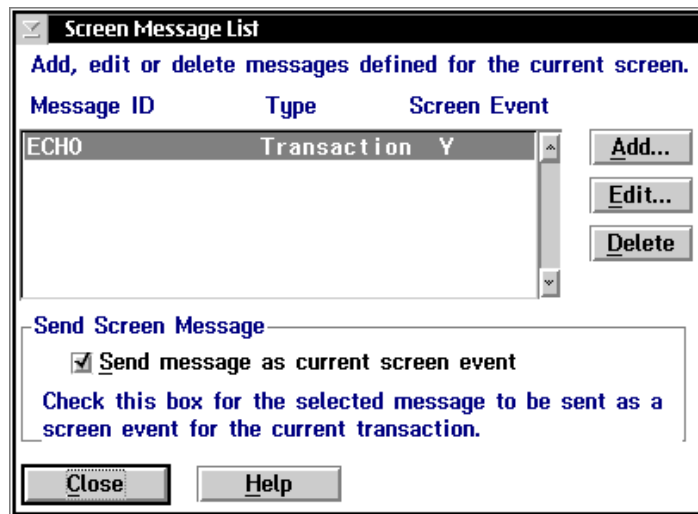
However, if you define a region message, it can be sent to the source of the transaction when a region appears or it can be sent when a region does not appear. Region messages do not appear in the Screen Event Ordering dialog box.

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 enable this check box, the message will be sent as a screen message. If you do not enable 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.

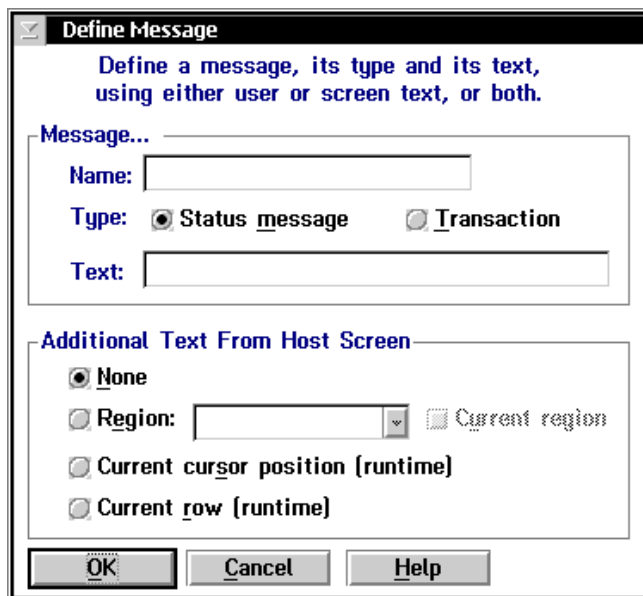
Adding a Message

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 the 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.



The image shows a dialog box titled "Define Message". The dialog box has a title bar with a close button and the text "Define Message". Below the title bar, there is a blue instruction: "Define a message, its type and its text, using either user or screen text, or both." The dialog is divided into two main sections. The first section is labeled "Message..." and contains a "Name:" text box, a "Type:" section with two radio buttons: "Status message" (which is selected) and "Transaction", and a "Text:" text box. The second section is labeled "Additional Text From Host Screen" and contains four radio button options: "None" (selected), "Region:" (with a dropdown menu and a "Current region" checkbox), "Current cursor position (runtime)", and "Current row (runtime)". At the bottom of the dialog, there are three buttons: "OK", "Cancel", and "Help".

Model 200 Controller User's Manual

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
Text	The text of the message.	1 to 119 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.	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

To add a message

1. From the Screen Message List dialog box, choose Add. The Define Message dialog box appears.
2. In the Name field, enter a unique name for the message.

3. Choose the type of message you are defining.
 - Choose Status message if you are defining 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.
 - Choose Transaction if you are defining a transaction in the Text field that will be mapped back to the terminal screen fields that originated the transaction.
4. In the Text field, enter the message.
 - 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 (,).
5. In the Additional Text From Host Screen box, choose an option button.
 - Choose None if no text from the host screen is in the message.
 - Choose Region if a region is in the message. Click the down arrow on the right side of the field. A list of regions appears. Choose the region to include with the message.

If you are defining a region message while you are defining a region, it is not listed in the region list. If you want to include the current region in the message, check the Current region check box.
 - Choose Current cursor position if the entire host screen field where the cursor is positioned at runtime is included in the message.
 - Choose Current row if the entire row where the cursor is positioned at runtime is included in the message.
6. Choose OK to return to the Screen Message List dialog box.

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:

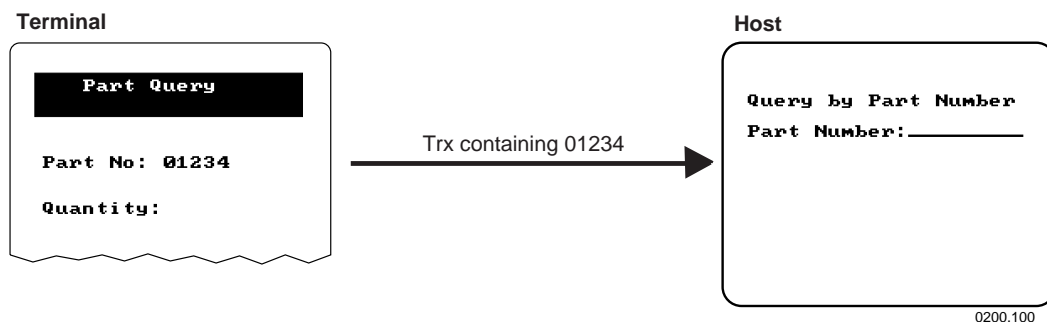
1 means that transaction field number 1 contains the same value as the original transaction field 1.

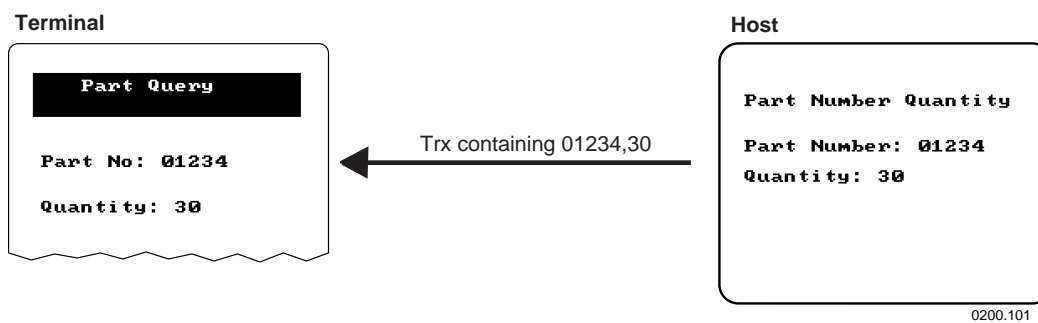
"," is the transaction field delimiter.

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



Transaction Message Example (continued)

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

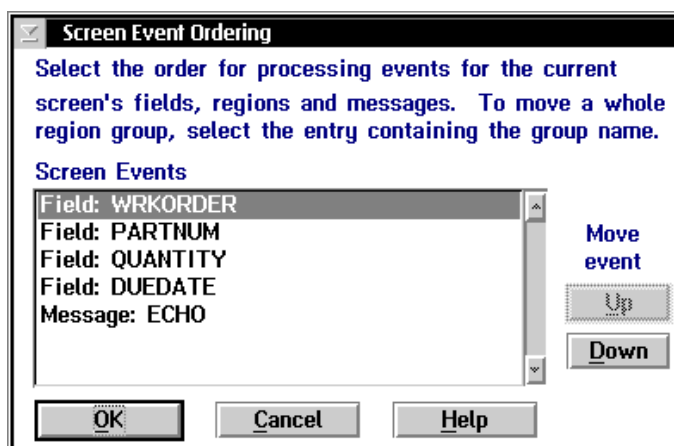
- mapping terminal (transaction) fields to host screen fields.
- handling regions in the host screen.
- sending screen messages.

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.

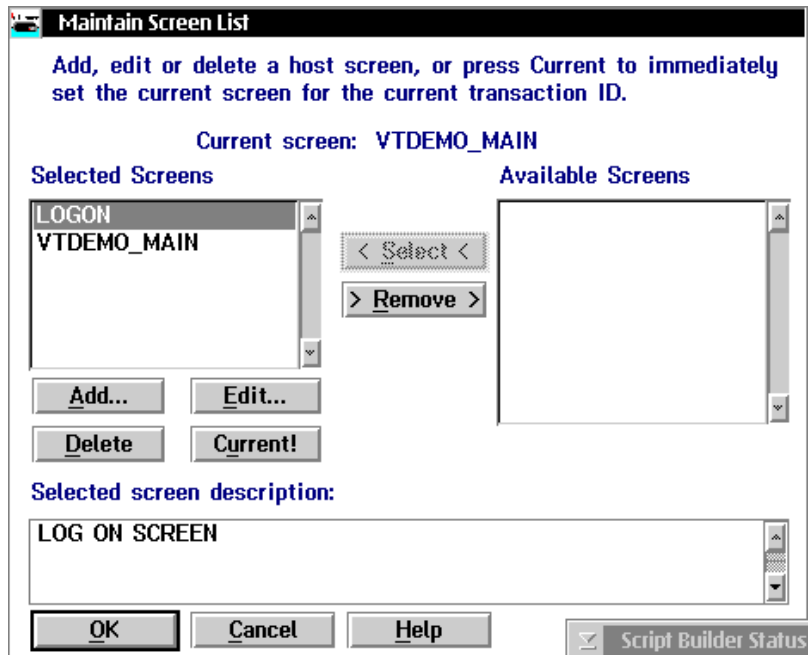
Note: Regions that match on a specific string are checked before regions that match on any string. You may need to be aware of this feature if you have regions that overlap.

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.

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.



Model 200 Controller User's Manual

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

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.
3. Add to the Selected Screens list box all the host screens that receive transaction data from the current transaction.
 - a. From the Available Screens list box, select a host screen to be added to the Selected list box.
 - b. Choose Select.
3. Remove from the Selected Screens list box any host screens that do not receive transaction data from the current transaction.
 - a. From the Selected Screens list box, select a host screen to be removed.
 - b. Choose Remove.
4. Add, edit, or delete any host screens in the Selected list box. 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.

5. (Optional) In the Selected list box, select a current host screen and choose Current! The description of the screen appears in the Selected Screen Description box and you can now define host screen fields and regions for it.
6. Choose OK to return to the Script Builder Tools window.

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.

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	None

To add a host screen

1. In the Maintain Screen List dialog box, choose Add. The Host Screen Definition dialog box appears.
2. In the Screen label field, enter a unique name for the host screen.
3. (Optional) In the Description box, enter a paragraph of text that describes the host screen.
4. Enter the position of the first character and contents of the screen identification string.
 - a. In the Row and Column fields, enter the position of the first character of the screen identification string.
 - b. In the Screen ID field, enter the screen identification string. Spaces are allowed.

Or, use the Get Field feature to automatically select the location and contents of the screen identification. For help, see "Getting the Screen Identifier From the Host Screen" later in this chapter.

5. Choose OK to return to the Maintain Screen List dialog box.

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 *Model 200 Controller Technical Reference Manual*.

Note: If you open your script file in any text editor, Script Builder will no longer recognize the file. However, you can still use your script file for screen mapping.

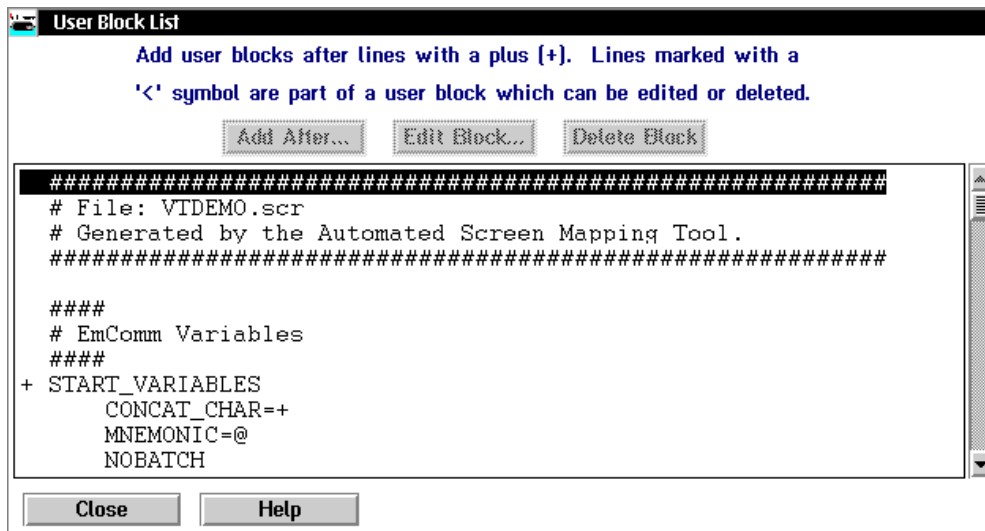
Model 200 Controller User's Manual

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.



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

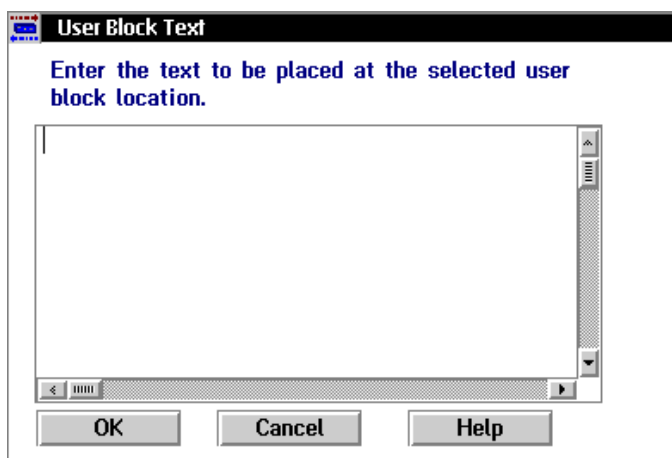
You can add user blocks after any line in the script that has a plus (+) sign in the left margin. Make sure you use the pound (#) character before any script comment.

*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.

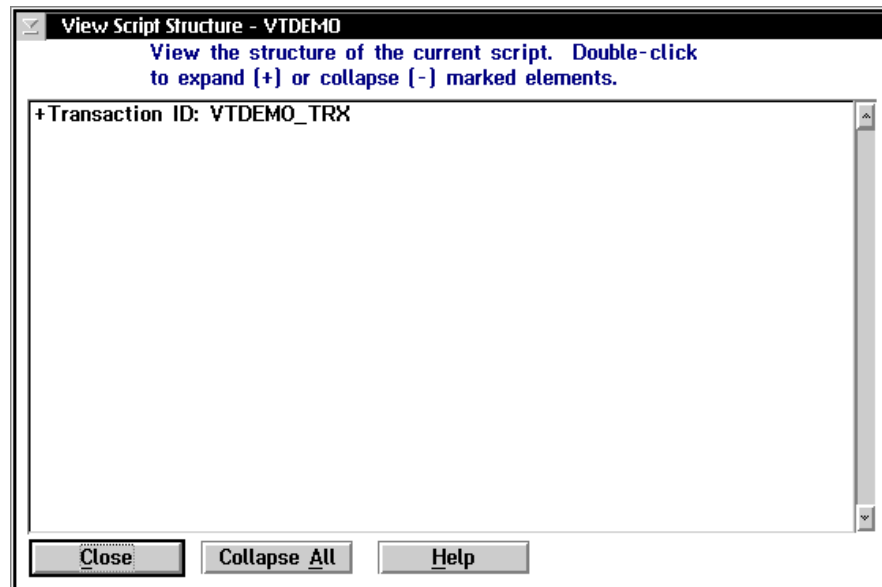
Viewing the Script

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 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 Model 200 Controller View Results window appears listing the errors that the script checker found. Refer to an example window on the next page.
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 Model 200 Controller View Results window lists no more errors.

(Part 1) To verify the logic of a script file

1. Set up your test environment.
 - 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.

Note: If you already have started a host terminal session, make sure that the host terminal session is at the logon screen.

- 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 controller.

(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 Model 200 Controller 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.

Model 200 Controller User's Manual

Problem

The script file is stuck in a host screen and cannot finish processing the transaction data.

Nothing happens on the host screen

(VT only)

Solution

Make sure that the keystrokes that you captured that move you from one host screen to the next screen are correct.

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.

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

The script file is stuck in a host screen.

The message received is not what you expect.

(VT only) The script file does not catch the region even though you can see it on the host screen.

Solution

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.

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.

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 controller, you can try downloading the template to the terminal template application and then running it. Verify the template as much as possible before you use it with the script file. The most common errors occur when the template 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 terminal template application will get out of sync messages.

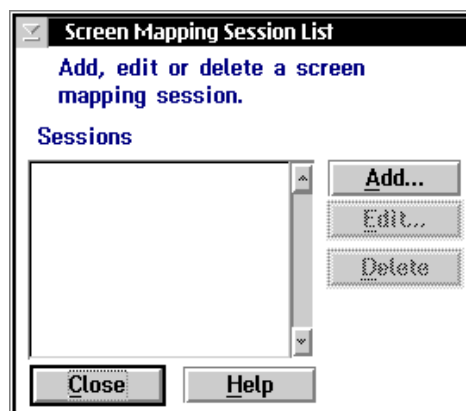
Setting Up Screen Mapping Sessions

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 controller 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

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 controller 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 controller.

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 controller starts the screen mapping session and is ready to accept transactions from data collection devices.

The screenshot shows the "Screen Mapping Session Definition" dialog box. The title bar reads "Screen Mapping Session Definition". Below the title bar, the text "Configure a screen mapping script, session, and transactions." is displayed. The dialog contains several fields and controls:

- Name:** A text input field.
- Visible when data collection started?**
- Start session at data collection start**
- Hot Standby timeout:** A text input field containing "20" followed by "seconds [1-9999]".
- Script File:** A dropdown menu showing "INV_CTRL.SCR". Below it are buttons for "Create", "Edit", and "Check".
- Host Terminal Session:** A dropdown menu and a "Start" button.
- Transactions for This Session:** A section with two list boxes: "Selected" and "Available". Between them are "< Select <" and "> Remove >" buttons. Below the "Selected" list are "Add...", "Edit...", "Delete", and "Map..." buttons.

At the bottom of the dialog are "OK", "Cancel", and "Help" buttons.

Model 200 Controller User's Manual

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 Model 200 Controller 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.	None	None
Available	This list box contains all the available transactions that you can use.	Predefined	None

To add a screen mapping session

1. From the Screen Mapping Session List dialog box, choose Add. The Screen Mapping Session Definition dialog box appears.
2. In the Name field, enter a meaningful name for this screen mapping session.
3. Check the Visible when data collection started? check box if you want a host terminal session to start when you start data collection. Use this check box when you are debugging your script file.

4. Check the Start session at data collection start check box if you want your screen mapping application to automatically start when you start data collection.
5. In the Hot Standby timeout field, enter the number of seconds the controller waits for a response.
6. In the Script File box, click the down arrow on the right side of the field. A list of script files appears. Choose the script file associated with this screen mapping session.

Note: Intermec highly recommends that you use the Script Builder Tool for creating and editing script files. If you choose Create or Edit in this dialog box and then you save your changes, the Script Builder Tool will not recognize the script file. In other words, you will not be able to open this script file using the Script Builder Tool.

7. In the Host Terminal Session box, click the down arrow on the right side of the field. A list of terminal sessions you have configured appears. Select a host terminal session for your screen mapping session.
8. Add all transactions that you want to route to this screen mapping session to the Selected list box.
 - a. From the Available list box, select a transaction to be added to the Selected list box.
 - b. Choose Select.
9. Remove any transactions from the Selected list box that you do not want to route to this screen mapping session.
 - a. From the Selected list box, select a transaction to be removed.
 - b. Choose Remove.
10. Add, edit, or delete any transactions that are listed in the Selected list box. For help, see “Adding a Transaction” in Chapter 9.
11. (Optional) Map transactions fields to screen fields. For help, see “Mapping Transaction Fields” in the next section.
12. Choose OK to save your changes and return to the Screen Mapping Session List dialog box.

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.

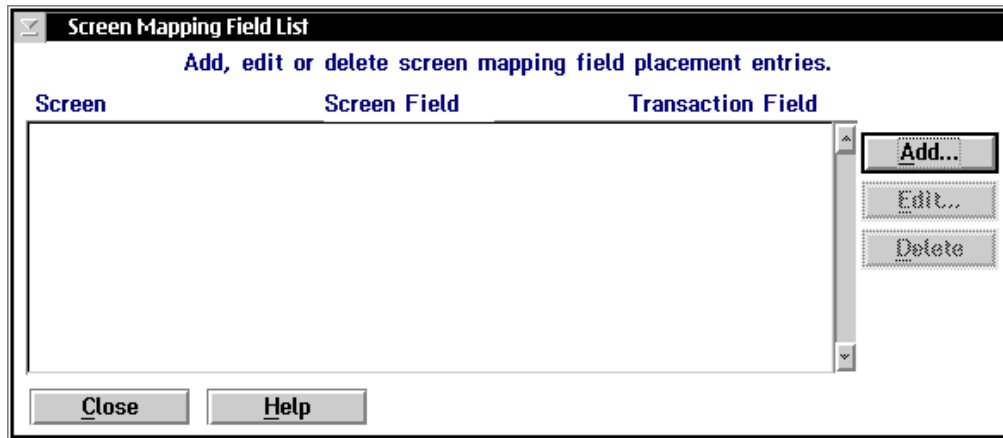
The Script Builder uses the command PUT_TRANS_FIELD, which explicitly maps a transaction field to a host screen field. If you use the Script Builder to generate your script files, you usually do not need to map transaction fields. **Intermec highly recommends that you use the Script Builder Tool to generate your script files.**

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. 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.

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

Screen Mapping Field Placement
Specify the transaction field and screen information.

Transaction field...

Name: DUEDATE

Number: 4

Screen...

Name: ITP_MENU

Field name: FIELD1

OK Cancel Help

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 a section, you should save any changes you have made to disk. If you have finished configuring your controller, activate your run-time configuration. When the activate is complete, a message box appears if you need to reboot the controller.

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 controller 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.

Building Terminal Screens for Data Collection Devices

Before you can run screen mapping, you need to create the terminal screens for the data collection devices. You group these terminal screens into a menu and then you generate the menu into a terminal template that you download to the terminals. The templates are displayed on a terminal screen such as on the JANUS 2020.

***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.*

Model 200 Controller User's Manual

When you run the template on your terminal, it displays the menu that lists terminal screens into which you can enter data. The data is packaged into a transaction and sent to the controller. The controller forwards the transaction to the appropriate screen mapping session. The screen mapping session connects specific transactions to a specific host application that uses a specific script file. When the script file receives a transaction, it maps the transaction fields to the host screen fields.

However, there is no direct link between terminal screen fields and host screen fields. They are linked through transaction fields. That is, a terminal screen field is linked to a host screen field if they are both mapped to the same transaction field number. Therefore, when you define a host screen field or a terminal screen field, you also need to specify transaction field mapping information. Since a linked host screen field and a terminal screen field share field attributes and transaction field mapping information, you can choose the Screen Mapping button in the Terminal and Fields dialog box to populate a terminal screen field with information from an existing host screen field.

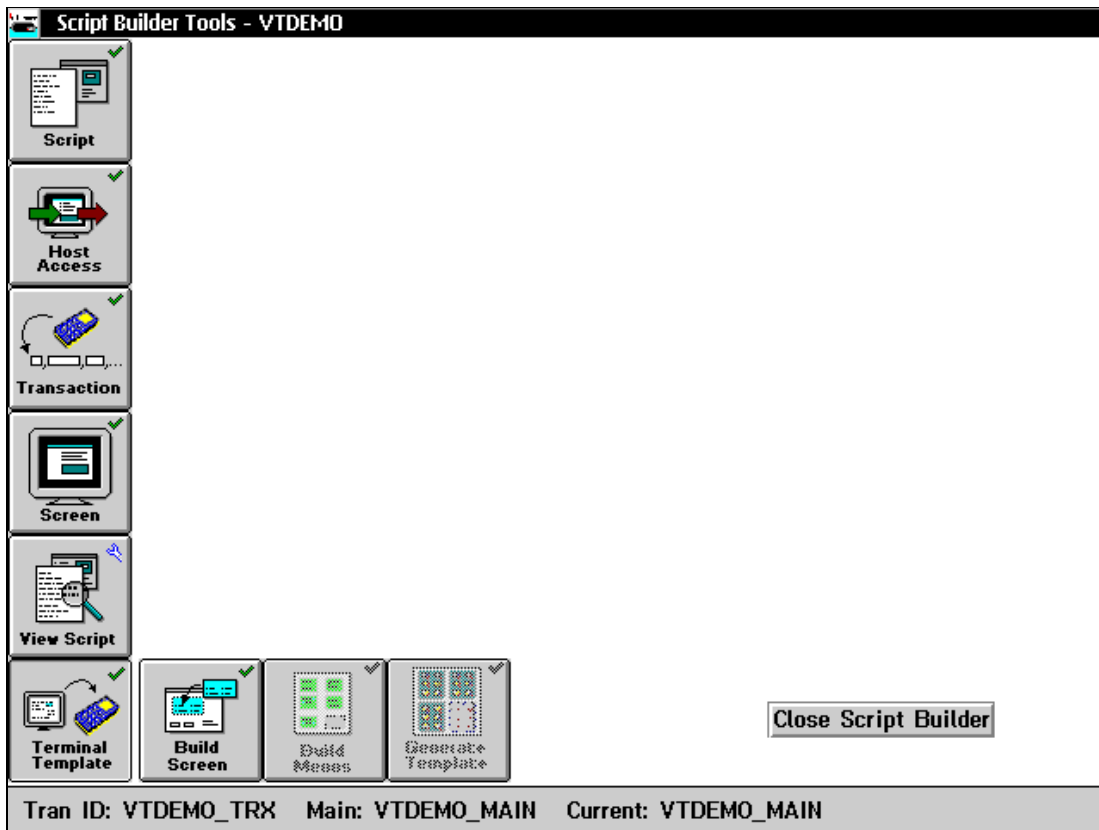
Note: If you want to get the terminal screen field information from a host screen field, you must first create your script file.

When you build a new terminal screen, you may want to open two other windows on the Model 200 Controller screen.

Terminal display The terminal display shows you what the screen will look like on your terminals. It shows the character positions on a terminal screen, it displays the picture field validation characters for input and output fields, and it displays any fixed fields. It does not show the default values you set for your input fields. To open the terminal display, choose View.

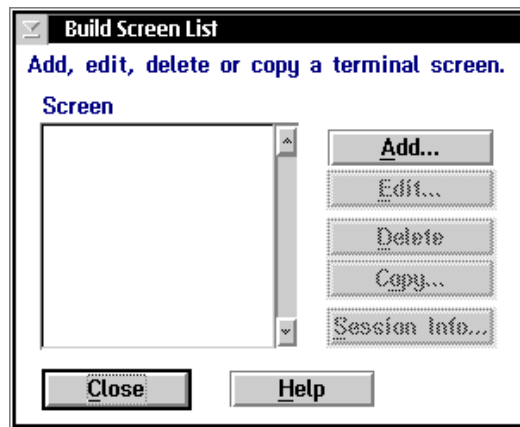
Host window The host window can display the host node application screen. If the host screen is field-formatted, you can use the Get Field feature to obtain information about fields directly from the host screen. For help, see "Getting Terminal Field Attributes From a Host Screen" later in this chapter.

This section explains how to build screens and menus and how to generate templates using the terminal template tools in the Script Builder Tools window. From the main menu choose Screen Mapping, and then choose Script Builder.



To build a new terminal screen

1. From the Script Builder Tools window, choose Terminal Template.
2. Choose Build Screen. The Build Screen List dialog box appears.



3. Add, edit, or delete terminal screens. For help, see “Adding a Terminal Screen” later in this chapter.

Or, copy a terminal screen and then edit it. For help, see “Copying a Terminal Screen” later in this chapter.

4. Choose Close to close the dialog box and return to the Script Builder Tools window.

Adding a Terminal Screen

Field	Description	Value	Default
Name	The unique name for the terminal screen.	1 to 16 alphanumeric characters	None
Size	The screen size of the terminal that the screen will be displayed on.	80x25, 40x13, 20x16, 20x8, 10x16, 10x8	20x16
Menu title (Optional)	The name you want to appear for the screen in the menu on the terminal.	1 to 50 alphanumeric characters	Name

Model 200 Controller User's Manual

Field	Description	Value	Default
Transaction	The transaction ID of the transaction that is created by this screen and that is sent to the Model 200 Controller.	1 to 20 alphanumeric characters	Name_tx
Auto send	This check box determines if the screen automatically sends the transaction when all of its fields are populated.	Check, Clear	Check
Wait for response	This check box determines if the screen waits for a transaction response before it allows further processing.	Check, Clear	Clear

To add a terminal screen

1. From the Screen List dialog box, choose Add. The Terminal Screens and Fields dialog box appears.
2. In the Name field, enter a unique name for the terminal screen.
3. In the Size field, click the down arrow on the right side of the field. A list of the available screen sizes appears. Choose the size of the terminal screen on the data collection device.
4. (Optional) In the Menu title field, enter the name that you want to appear for the screen in the menu on the terminal. If you do not enter a menu title, the screen name is used.
5. In the Transaction field, click the down arrow on the right side of the field. A list of the available transactions appears. Choose the transaction ID of the transaction that is created by this screen.

If you do not enter a transaction, a transaction is created with the name "name_tx" where name is from the Screen Name field.

6. If you want another terminal screen to automatically appear when this terminal screen is populated, choose Screen.

For help, see "Defining Next Screen Sequence for Terminal Screens" later in this chapter.

7. Enable or disable the Auto send and Wait for response check boxes.

If you enable the Wait for response check box, the controller waits for 20 seconds before it places the application in Hot Standby mode. The device waits for 60 seconds before it times out and attempts to resend the transaction.

If you disable the Wait for response check box, the screen will not be able to accept data for output fields, nor will it be able to accept system messages such as SEND_MESSAGE.

8. The Screen Field box lists all the screen fields that are already defined for this screen. You can add new fields to the screen, or you can edit and delete existing fields, or you can get a field from the host window. For help, see “Adding a Terminal Field” earlier in this chapter.

Or, to get the attributes of a field from a host window, follow the instructions for “Getting Terminal Field Attributes From a Host Screen” later in this chapter.

Or, to get the attributes of a field from the related host screen field attributes, choose Screen Mapping.

9. Choose View to open the Terminal Display.
10. Choose OK to save your changes and return to the Build Screen List dialog box.

Adding a Terminal Field

There are several different types of fields you can add to your terminal screen.

Field type - input These fields accept data. The data can be from input from a user or it can be output from a host (using the SEND_MESSAGE command). The data can be scanned or typed. You can make this field required. If this field is required and the user does not enter any information, the screen transaction cannot be sent. You can validate input fields. If the user does not enter data that falls within the validation, an error message appears on the terminal screen.

Field type - output These fields display data from a host. Output fields are populated from transaction fields sent by the script file. These fields are also known as regions.

Model 200 Controller User's Manual

Field type - fixed These fields display the data that you enter in the Value field. Fixed fields contain static text and they do not change as the data entered in the input or output field changes. Use these fields as terminal prompts for input or use them as descriptions for output fields.

Data type - date If you choose date as your data type, you cannot set the length or the picture. The controller accepts dates in these formats:

MMDDYY	DDMMYY	YYMMDD
MM.DD.YY	DD.MM.YY	YY.MM.DD
MM/DD/YY	DD/MM/YY	YY/MM/DD
MM-DD-YY	DD-MM-YY	YY-MM-DD
MMDDYYYY	DDMMYYYY	YYYYMMDD
MM.DD.YYYY	DD.MM.YYYY	YYYY.MM.DD
MM/DD/YYYY	DD/MM/YYYY	YYYY/MM/DD
MM-DD-YYYY	DD-MM-YYYY	YYYY-MM-DD

Data type - time If you choose time as your data type, you cannot set the length or the picture. The controller accepts times in these formats:

HHMM	HH.MM	HH:MM
HHMMSS	HH.MM.SS	HH:MM:SS

Picture This field, when combined with the length field, describes the format for an input field. For example, if the maximum length of the input field is 5, and there is one X in the Picture field, the user must enter at least one character before moving on to the next input field. If there are five Xs in the Picture field, the user must enter five characters.

Field	Description	Value	Default
Field name	A unique identifier for the terminal field.	1 to 16 alphanumeric characters	None
Row	The row position that indicates where the field starts on the terminal screen.	1 through 25, based on screen size selected	1 or the next available row.
Column	The column position that indicates where the field starts on the terminal screen.	1 through 80 based on screen size selected	1
Type	The type of field. Fixed fields are always the same value. Input fields accept input from the user. Output fields display information only.	Fixed, Input, Output	Fixed

Model 200 Controller User's Manual

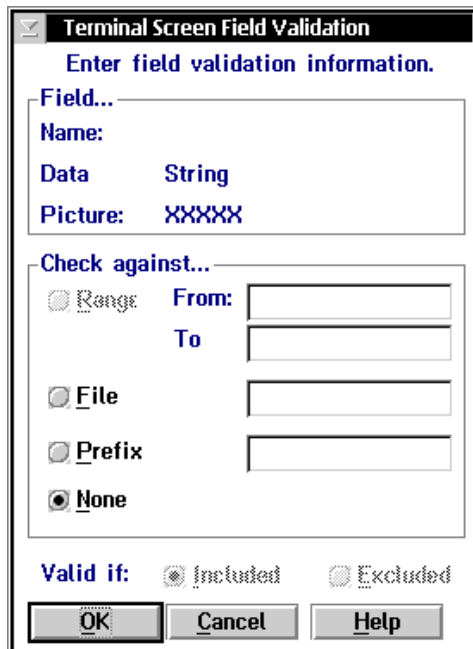
Field	Description	Value	Default
Data type	The type of data that you can enter into this field.	Date, Time, Numeric, String	String
Attribute	The physical attributes of the data type field.	Blink, Hidden, Inverse, None	None
Length	The maximum length of the field.	String is 1 to 80 Numeric is 1 to 11 including a sign (+ or -) and a decimal point.	5
Trx field number	The position of the field in the transaction sent by this screen.	1 to 9999	None
Required	This check box indicates if the field is required to be filled in before the user can proceed to another screen.	Check, Clear	Check
Picture	The character-by-character validation string for an input field.	X - any character A - alpha only 9 - numeric only Y - Yes/No Special characters	XXXXX
Value	The default value for an input field or the value for a fixed field.	None	None

To add a terminal field

1. From the Terminal Screen and Fields dialog box, choose Add. The Screen Field Parameters dialog box appears.
2. In the Field name field, enter the unique name for the terminal field.
3. In the Origin box, define the row and column of the upper left corner of the field.
4. In the Field box, define the type, data type, length, picture, and default value.
5. In the Attribute field, click the down arrow on the right side of the field. A list of attributes appears. Choose the attribute you want to use for the Data type field.

6. Enable or disable the Required check box that determines if this field is required. A check in the check box means that this field is required.
7. In the Trx field number field, enter the order or position (for example, 1, 2, or 3) of this field in the transaction that the screen sends. Fields start at 1.
8. If you want validation performed on an input field, choose Validation. The Screen Field Validation dialog box appears. For help, see “Validating a Terminal Field” later in this chapter.
9. Choose OK to save your changes and return to the Screen Definition dialog box.

Validating a Terminal Field



The image shows a dialog box titled "Terminal Screen Field Validation". The dialog box has a title bar with a close button and the text "Terminal Screen Field Validation". Below the title bar, there is a section titled "Enter field validation information." with a "Field..." label. Under this label, there are three fields: "Name:" (empty), "Data" (set to "String"), and "Picture" (set to "XXXXX"). Below these fields is a section titled "Check against..." with four radio button options: "Range", "File", "Prefix", and "None". The "None" option is selected. To the right of the "Range" option are two input fields labeled "From:" and "To:". To the right of the "File" and "Prefix" options are single input fields. Below the "Check against..." section is a "Valid if:" section with two radio button options: "Included" (selected) and "Excluded". At the bottom of the dialog box are three buttons: "OK", "Cancel", and "Help".

Model 200 Controller User's Manual

Field	Description	Value	Default
Range	Enable or disable checking the field against a numeric range.	Enable, Disable	None
From	The beginning numeric value in the range.	-999999999 to 999999999	None
To	The ending numeric value in the range.	-999999999 to 999999999	None
File	The name of the file on the terminal that contains valid values. Data entered in the input field is validated against these values.	Enable, Disable	None
Prefix	The characters that the data in an input field must begin with or not begin with to be valid.	1 to 6 characters	None
None	This option button indicates that no validation will occur on the field.	None	None
Valid if	These option buttons indicate that the value in the input field is valid if it is included or excluded in the range or file.	Included, Excluded	Included

To validate a terminal field

1. From the Screen Field Parameters dialog box, choose Validation. The Terminal Screen Field Validation dialog box appears.
2. In the Field box, make sure that you are configuring validation for the correct field.
3. In the Check against box, choose the type of validation you want to perform on the field.
4. Enter the range, file, or prefix.

Note: If you choose a decimal range, the value becomes a sign (+,-) a decimal point, and nine numbers.

5. Choose if the data in the input field is included or excluded in the range or file.
6. Choose OK to save your changes and return to the Screen Field Parameters dialog box.

Getting Terminal Field Attributes From a Host Screen

In 5250 field-formatted host screens, there are two types of fields: protected and unprotected. To get terminal field attributes from a host screen field, position the host cursor anywhere in a protected or an unprotected field and then choose Host Session. The Script Builder fills in the Type, Data type, Attribute, Length, Picture, and Value (if any string exists) fields.

3270 field-formatted host screens do not differentiate between protected and unprotected fields. To get terminal field attributes from a host screen field, position the host cursor at the beginning position of a field and then choose Host Session. The Script Builder fills in the Type, Length, Picture, and Value (if any string exists) fields.

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 field before you choose Host Session. If nothing is selected when you choose Host Session, an error message occurs.

To get terminal field attributes from a host screen field

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 fields you are using to build the terminal screen.
3. In the host window, place your cursor on the field whose attributes you want to use for the terminal screen field.
4. In the Terminal Screen and Fields dialog box, choose Host Session. The Origin, Field, and Value boxes are populated with the attributes of the host screen field.
5. If necessary, edit the information in the fields.

6. Choose OK to save your changes and return to the Screen Definition dialog box.
7. Repeat Steps 3 through 6 until you have added all the fields from the host window to the terminal screen.

Getting Terminal Field Attributes From the Script File

You can get terminal field attributes from a defined host screen field in the script file.

To get terminal field attributes from a script file

1. In the Script Builder Tools window, open a script file you will use with the template.
2. From the Script Builder Tools window, choose Terminal Template.
3. Choose Build Screen. The Build Screen List dialog box appears.
4. In the Screen list box, select the screen that contains the terminal field whose attributes you want to define and then choose Edit. The Terminal Screen and Fields dialog box appears.
5. In the Transaction field, click the down arrow on the right side of the field. A list of the available transactions appears. Choose the transaction ID of the transaction that is created by this screen.
6. Choose Screen Mapping.

For each of the transaction fields, the Script Builder Tool checks to see if a host screen field is mapped to it. The Script Builder Tool then checks to see if a terminal field is mapped to that transaction field. If a terminal field does not exist, it automatically creates one from the host screen field definition. The new terminal field has a field type of input and is added to the next row on the terminal screen.

Defining Next Screen Sequence for Terminal Screens

This feature lets you identify a linked screen to appear on the terminal when a condition is met after you send a screen transaction. When you set up a Next screen, the terminal compares data in the selected Screen field to a value in the Value field. If the logic is true, then the Next screen appears on the terminal.

- If you want the screen in the Next screen field to appear when specific data is entered in the screen field, use the Operator and Value fields to create the logic that determines when the linked screen appears.
- If you want the screen in the Next screen field to always appear after the user sends the current screen transaction, you need to make the Screen field a required field in the Screen Field Parameters dialog box. Then choose the operator to be NOT BLANK. You do not have to enter a value in the Value field.

Next Screen

Enter next screen information.

Current screen: SCREEN1

Next Screen Information

If data = value goto next_screen

Screen field: FIELD1

Operator: =

Value:

Next

OK Cancel Delete Help

Model 200 Controller User's Manual

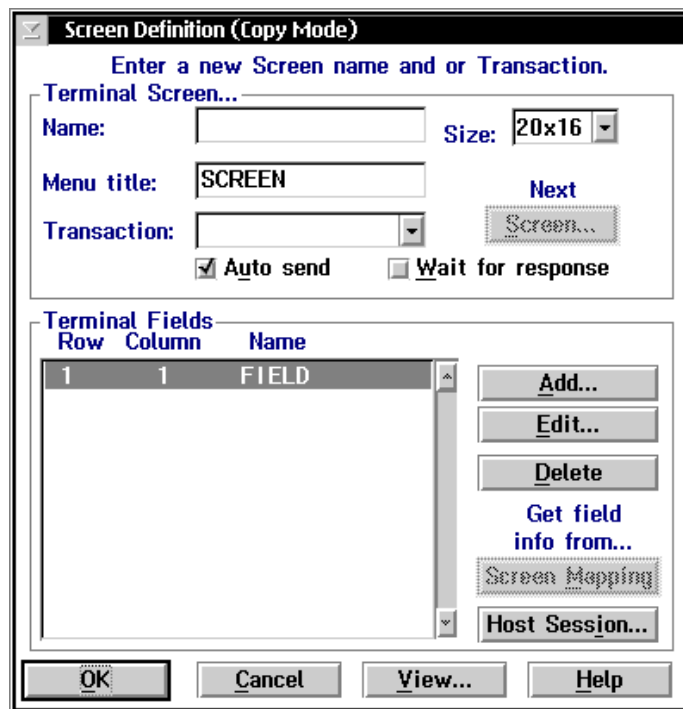
Field	Description	Value	Default
Screen field	The field from the current screen whose data is compared to the Value field. The results of the comparison determine whether or not the screen in the Next field appears.	Predefined	None
Operator	The list of valid operators that you can use to compare the Screen field against the Value field.	=, >, <, !=, >=, <=, BLANK, NOT BLANK	=
Value	The value that is compared to the data in the Screen field that determines whether or not the screen in the Next field appears.	None	None
Next	The name of the screen that is displayed if the Screen field and Value logic is true.	Predefined	None

To configure a next screen

1. From the Terminal Screen and Fields dialog box, choose Screen. The Next Screen dialog box appears.
2. Make sure that the Current screen field contains the original screen.
3. In the Screen field, enter the field whose data the controller compares to the Value field to determine whether or not the next screen appears.
4. In the Operator field, click the down arrow on the right side of the field. Select the operator.
5. In the Value field, enter the value the controller uses to compare against the Screen field to determine whether or not the next screen appears.
6. In the Next field, enter the name of the linked screen that you want to display.
7. Choose OK to save your changes and return to the Screen Field Parameters dialog box.

Copying a Terminal Screen

1. From the Script Builder Tools window, choose Terminal Template Tools.
2. Choose Build Screen. The Build Screen List dialog box appears.
3. In the Screen list box, select the screen that you want to copy.
4. Choose Copy. The Screen Definition dialog box appears. The new screen carries over most of the attributes of the old screen. However, you must enter a new screen name in the Name field. See the example on the next page.



5. In the Name field, enter a unique name for the terminal screen.
6. Edit the information in the fields. For help, see “Adding a Terminal Screen” earlier in this chapter.

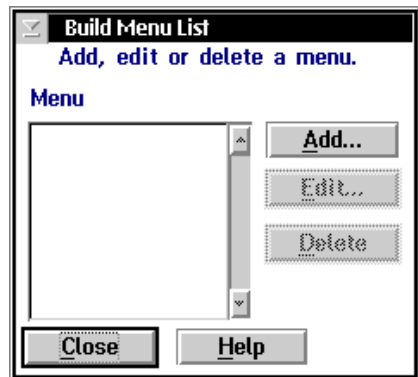
Building Menus From Screens

After you finish creating the screens, group them into logical menus that, when generated, turn into templates that are downloaded to the JANUS devices and TRAKKER Antares terminals.

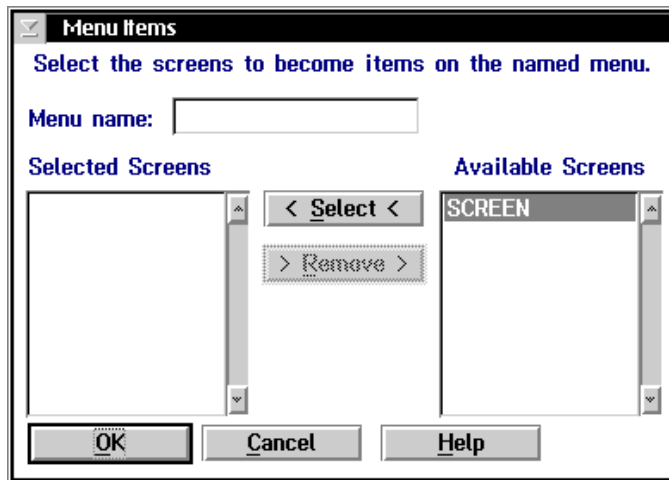
Note: Make sure you add all the screens (including any screens configured as Next screens) to the menu list.

To build a menu

1. From the Script Builder Tools window, choose Terminal Template.
2. Choose Build Menus. The Build Menu List dialog box appears.
3. Add, edit, or delete menus. For help, see "Adding a Menu" later in this chapter.
4. Choose Close to close the dialog box and return to the Script Builder Tools window.



Adding a Menu



To add a menu

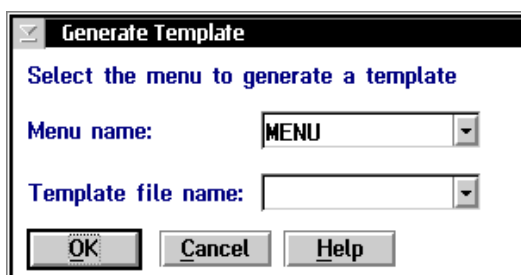
1. From the Menu List dialog box, choose Add. The Menu Items dialog box appears.
2. In the Menu name field, enter a name for the group of screens you are selecting that you will generate into a template.
3. In the Selected Screens list box, add screens to the menu by selecting a screen in the Available Screens list box and choosing Add.
4. In the Selected Screens list box, remove screens from the menu by selecting the screen and choosing Remove.
5. Choose OK to save your changes and return to the Menu List dialog box.

Generating Menus Into Templates

When you have built the menus from the screens, you need to generate them into terminal templates. Each menu generates into one terminal template. You can use the download server feature to download this terminal template to your data collection devices or you can use the reader program on your devices to request it. For help, see "Configuring Your JANUS Devices" and "Configuring Your TRAKKER Antares Terminals" later in this chapter.

To generate a terminal template

1. From the Script Builder Tools window, choose Terminal Template.
2. Choose Generate Templates. The Generate Template dialog box appears.



3. In the Menu name field, click the down arrow on the right side of the field. A list of the menus that you have created appears. Select the menu that you want to generate into a terminal template.
4. In the Template file name field, click the down arrow on the right side of the field. A list of existing terminal template filenames appears. Select the terminal template you want.

Or, enter a new terminal template filename. The default value is the first eight characters of the menu name with a .TPL extension.

5. Choose OK. The menu is generated into a terminal template that you download to your devices.

Saving and Activating Your Run-Time Configuration

When you finish configuring screen mapping, you should save your changes. If you are done configuring the controller, activate your run-time configuration. When the activate is complete, a message box appears if you need to reboot the controller.

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 controller 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.

Model 200 Controller User's Manual

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 allow you to 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 NEWLNL, 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 controller screen cannot show blinking text. If the host application sends blinking text to a VT terminal session, the controller shows the text as white text on a dark red background. If it sends blinking text to a VT window, the controller 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 Model 200 Controller keyboard and to the script keystroke names. For a diagram of how the VT keyboard maps to the controller keyboard, see Chapter 8, "Using Terminal Emulation."

VT Keyboard	Controller 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
F6	F6	PF6
F7	F7	PF7

VT Keyboard Map (continued)

VT Keyboard	Controller Keyboard	Script Name
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

VT Keyboard Map (continued)

VT Keyboard	Controller Keyboard	Script Name
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 controller.

Key	Mnemonic	Key	Mnemonic
Enter	ENTER	Cursor Right	CUR_RT
Left Tab	LTAB	Cursor Left	CUR_LFT
Right Tab	RTAB	System Request	SYSREQ
Clear	CLEAR	Reset	RESET
Delete	DEL	Page Up	PAGEUP
Insert	INS	Page Down	PAGEDN
New Line	NEWLN	Attention	ATTN
Space	SPACE	Field Exit	FLDEXIT
Home	HOME	Erase EOF	ERS_EOF
End	END	Test	TEST
Cursor Up	CUR_UP	No Keystroke	NONE
Cursor Down	CUR_DN	PA1, PA2, PA3	PA1, PA2, PA3
		Function Keys F1 - F24	PF1 - PF24

Configuring Your JANUS Devices

Your Model 200 Controller lets you perform screen mapping between your remote host and your JANUS devices.

Configuring Communications

You need to configure each JANUS device for 900 MHz RF or 2.4 GHz RF communications. Run the Interactive Configuration application (IC.EXE) on your JANUS 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 900 MHz RF Communications

1. In the Com menu, choose RF and press .
2. Choose Activate.
3. In the RF Protocol field, select Enabled.
4. Choose Primary Cfg.
5. In the Device Address field, enter the address of the JANUS device. This address must match an address that is enabled in the Model 200 Controller.
6. Configure the Channel Select and the Network ID.
7. In the File menu, choose Exit.
8. Choose Yes to save your configuration.

Configuring for UDP Plus Communications

You need to configure each JANUS 2.4 GHz RF 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: *If the access points are using a security ID, you must set the same security ID on the JANUS devices.*

Downloading the Terminal Template Application

You need to download the terminal template application (RDRPGM.EXE) from the Model 200 Controller to each JANUS device that will be using screen mapping. This application allows the JANUS device to run the templates for screen mapping. Depending on the type of communications your JANUS devices are using and which firmware version is loaded, you can load the terminal template application on 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.

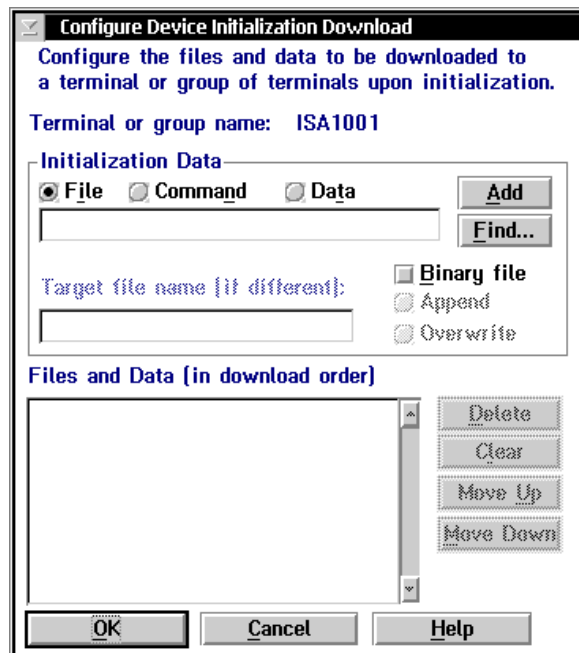
Note: Your JANUS devices must have FTA.EXE and FTA.INI loaded on drive C. Copy these files from Application companion disk 3. For help, see your JANUS user's manual.

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

- If your JANUS 900 MHz RF device has an earlier firmware version than 3.01, use Interlnk.
- 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 the download server to download the terminal template application

1. If you want to send the terminal template application to more than one JANUS device, define a group in the download server. For help, see “Adding a Group in the Download Server” in Appendix B.
2. From the main menu sidebar buttons, choose System Maintenance. The System Maintenance dialog box appears.
3. Select Configure Download Server and choose Start. The Terminal Download Configuration dialog box appears.
4. In the Terminals and Groups list box, select the terminal address or group that needs the terminal template application.
5. Choose Edit. The Configure Device Initialization Download dialog box appears.



6. In the Initialization Data box, choose File.

Model 200 Controller User's Manual

7. In the field, type:
`\userdata\termapps\tta\janus\rdrpgm.exe`
8. Enable the Binary file check box.
9. Choose Overwrite if you want to overwrite any existing file with the same name on the JANUS devices. Do not choose Append.
10. Choose Add. The file appears in the Files and Data list box with a B in the left column.
11. Choose OK to save your changes and return to the Terminal Download Configuration dialog box.
12. In the Terminals and Groups list box, choose the terminal or group you configured.
13. Choose Download. The terminal template application is downloaded to the terminal or group.

To use Interlnk to load the terminal template application

1. Insert a 3.5-inch disk into the floppy disk drive of the controller.
2. From the main menu sidebar buttons, choose File Handling. The File Handling dialog box appears.
3. In the File Handling list box, select Back up User Files and then choose Start. The Backup User Files dialog box appears.
4. From the JANUS subdirectory, select RDRPGM.EXE and choose Select. The file appears in the Selected Files list box.
5. Choose Backup Files. The file is copied to the disk.
6. Insert the disk into a floppy disk drive of a PC.
7. Run Interlnk on the PC and your JANUS device. For help, see your JANUS user's manual.
8. Copy RDRPGM.EXE to the E drive on the JANUS device.

To use FTP to load the terminal template application

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

1. Make sure that the JANUS device is on a writable DOS prompt. Type `F T P space IPaddress` where *IPaddress* is the IP address of the controller 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 termapps\tta\janus` and then press `enter ↵`.
4. Type `B I N` and press `enter ↵`.
5. Type `G E T space R D R P G M . E X E` and press `enter ↵`.
6. When the terminal template application has finished loading on the JANUS device, type `Q U I T` and press `enter ↵`.

Downloading the Template

You need to download the template that was generated on the Model 200 Controller to each JANUS device that will be using screen mapping. The template is an ASCII file. Each JANUS device needs a template to run before you can enter data and send transactions. When running the template, the JANUS device prompts you for each field and it edits the data for data type, length, inclusion/exclusion in a file, and pattern matching. The controller maps the transaction fields to a host application screen.

To load the template on your JANUS devices, you can

- send the template to your JANUS 900 MHz RF devices if they have firmware v3.01 or later by using the download server.
- send the template to your JANUS UDP Plus devices by using the download server or FTP. To use FTP, you must have an FTP client loaded on your JANUS device.
- request the template from the controller by using the terminal template application that is running on your JANUS device.

Model 200 Controller User's Manual

To use the download server to download the template

1. Follow Steps 1 through 6 in the procedure for using the download server to download the terminal template application in "Downloading the Terminal Template Application" earlier in this chapter.
2. In the Initialization Data box field, type:
`\path\template.tpl`
where:
path is the location of the template on the controller.
template is the name of the template.
3. Clear the Binary file check box.
4. Choose Add. The file appears in the Files and Data list box with an F in the left column.
5. Choose OK to save your changes and return to the Terminal Download Configuration dialog box.
6. In the Terminals and Groups list box, choose the terminal or group you configured.
7. Choose Download. The template is downloaded to the terminal or group.

To use FTP to load the template

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

1. Make sure that the JANUS device is on a writable DOS prompt. Type `F T P IPaddress` where *IPaddress* is the IP address of the controller and press .
2. In the login name field, type `A N O N Y M O U S` and press .
3. Type `C D path` where *path* is the location of the template on the controller and press .

3. Then, type `G E T` `template.tpl` where `template.tpl` is the name of the template and press `enter`.
4. When the template has finished loading on the JANUS device, type `Q U I T` and press `enter`.

To request the template from the controller

1. Make sure that the host is running the application.
2. Make sure that you have started data collection on the Model 200 Controller.
3. Press `(/O)` to resume the JANUS device.
4. On the JANUS device, load RWTSR by typing `R W T S R` and pressing `enter`.
5. Load the Intermec RF protocol handler by typing `R F P H` `4`.
6. Identify the COM port that the JANUS device is using to communicate by typing `SET COMPORT=IM_COM4`
7. Identify the type of JANUS device you are using by typing `SET READERTYPE=n`
where:

<i>n</i>	900 (900 MHz)
	24 (2.4 GHz)
8. Change to the E directory by entering `E` `≡` `F`.
9. At the E prompt, type `R D R P G M` `template.tpl` where `template.tpl` is the name of the template that you want to run.

The template main menu appears. The main menu lists all the screens you can access to send data.

Hint

You can write a batch file on the JANUS device to make it easier for the user to start the template. For example, you may want the user on shift 1 to start the template by typing his shift number at the JR2020 prompt. The batch file, SHIFT1.BAT may look like:

```
rwtsr
RFPH 4
set comport=im_com4
set readertype=900
rdrpgm shift1.tpl
```

Loading a Validation File

You may need to download a validation file to your JANUS devices. The validation file performs validation on input fields in JANUS screens. This file is an ASCII file that has one entry per line. Since the file is read sequentially, you should try to keep the file small. The last line in the ASCII file must be <EOF>.

To load a validation file on your JANUS devices, you can

- load the file on the DCS 300 and send the file to a JANUS device by using the download server.
- load the file on the DCS 300 and send the file to a JANUS UDP Plus device by using the download server or FTP. To use FTP, you must have an FTP client loaded on your JANUS device.
- run Interlnk on the PC and a JANUS device.

Running the Application

Once you have selected a screen, you can send data from the screen, reset the screen without sending data, and exit the screen. While you are entering data into screens, you may notice these events:

- Data may appear in an output field that was previously empty.
- A linked screen may appear if data in a field in the current screen meets some predefined value.
- Data that came from a transaction that was sent to your JANUS device may appear in your input fields on the screen.
- A message that is sent to you from another application may appear in the system message area.

To enter data into a screen

1. From the menu, use the **▲** and **▼** keys to select the screen in which you want to enter data.
2. Press **F2**. The screen you selected appears on the JANUS display and the screen name is in the title bar.
3. Type or scan data into the fields. Use the **▲** and **▼** or press **enter** to accept the data for each field.
4. When you have finished filling in the fields:
 - If Auto send was chosen when the screen was defined, the transaction is automatically sent to the controller.
 - Press **F1** to send the transaction to the controller.
 - Press **F3** to reset the screen and reposition the cursor to the first input field without sending the data.
 - Press **F4** to exit the screen without sending the data and return to the main menu.

Configuring Your TRAKKER Antares Terminals

With the Model 200 Controller, you can run screen mapping between your remote host and your TRAKKER Antares terminals.

Configuring the Terminals for the First Time

Before the terminal can communicate with the Model 200 Controller, you need to configure each terminal. On the T2425, press **[F] [↩] [T] [2] [M]** to access the TRAKKER Antares 2400 Menu System. On the T248X, press **[F] [↩] [2] [4] [8]** to access the TRAKKER Antares 2400 Menu System. For help, see your TRAKKER Antares terminal user's manual. You need to set these parameters on each terminal:

- Time and date
- Network activate
- Network port (must match the Model 200 Controller)
- Controller IP address (must match the Model 200 Controller)
- Terminal IP address
- RF domain (same as the access point)
- RF security identification (same as the access point)

The terminal also needs to know where to send transactions. Choose one of these options:

- Explicitly link the terminals to a host. For help, see "Configuring the Controller" in Chapter 8.
- Identify a host name on each terminal. To set the host name, you access the TE Configuration menu by pressing **[F] [F1]** and then **[↩]** on the terminal when the TE welcome screen is displayed on the terminal. You can also access the TE Configuration menu by pressing the same key sequence once a terminal session is established. For help, see your TRAKKER Antares terminal user's manual.

Note: You cannot enter the TE Configuration Menu when the terminal is trying to connect to the Model 200 Controller.

Downloading the Template

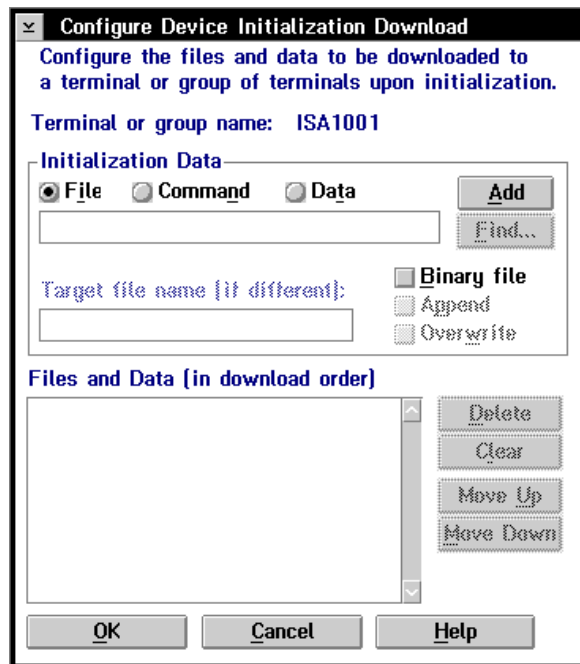
You need to download the template that was generated on the Model 200 Controller to each TRAKKER Antares terminal that will be using screen mapping. The template is an ASCII file. Each terminal needs a template to run before you can enter data and send transactions. When running the template, the terminal prompts you for each field and it edits the data for data type, length, inclusion/exclusion in a file, and pattern matching. The controller maps the transaction fields to a host application screen.

You can load the template on your terminals by

- sending the template to your terminals using the download server.
- requesting the template from the controller using the terminal template application running on your terminal.

To use the download server to download the template

1. If you want to send the template to more than one terminal, define a group in the Download Server. For help, see “Adding a Group in the Download Server” in Appendix B.
2. From the main menu sidebar buttons, choose System Maintenance. The System Maintenance dialog box appears.
3. Select Configure Download Server and choose Start. The Terminal Download Configuration dialog box appears.
4. In the Terminals and Groups list box, select the terminal address or group that needs the template.
5. Choose Edit. The Configure Device Initialization Download dialog box appears.



6. In the Initialization Data box, choose File.
7. In the field, type:
`\tpl\template.tpl`
where *template.tpl* is the name of the template that you want to download.
8. Clear the Binary file check box.
9. Choose Add. The file appears in the Files and Data list box with an F in the left column.
10. Choose OK to save your changes and return to the Terminal Download Configuration dialog box.

11. In the Terminals and Groups list box, choose the terminal or group you configured.
12. Choose Download. The template is downloaded to the terminal or group.

To request the template from the controller for the first time

1. Make sure that the host is running the application.
2. Make sure that you have started data collection on the Model 200 Controller.
3. Press Ⓜ to resume the terminal.
4. At the Enter file name? prompt, type:

```
template.tpl
```

where *template.tpl* is the name of the template you want to run.

The template main menu appears. The main menu lists all the screens you can access to send data.

To request a new template from the controller

1. Make sure that the host is running the application.
2. Make sure that you have started data collection on the Model 200 Controller.
3. Press Ⓜ to resume the terminal.
4. Press F4 to request a new template.
5. At the File name? prompt, type:

```
template.tpl
```

where *template.tpl* is the name of the template you want to run.

The template main menu appears. The main menu lists all the screens you can access to send data.

Loading a Validation File

You may need to download a validation file to your terminal. The validation file performs validation on input fields in terminal screens. This file is an ASCII file that has one entry per line. Since the file is read sequentially, you should try to keep the file small. The last line of the ASCII file must be <EOF>.

To load a validation file on your terminals

1. Make sure that you transfer the validation file to the controller. For help, see "Restoring Your User Files" in Chapter 2.
2. If you want to send the validation file to more than one terminal, define a group in the Download Server. For help, see "Adding a Group in the Download Server" in Appendix B.
3. From the main menu sidebar buttons, choose System Maintenance. The System Maintenance dialog box appears.
4. Select Configure Download Server and choose Start. The Terminal Download Configuration dialog box appears.
5. In the Terminals and Groups list box, select the terminal address or group that needs the validation file.
6. Choose Edit. The Configure Device Initialization Download dialog box appears.
7. In the Initialization Data box, choose File.
8. In the field, type:
`\filename`
where *filename* is the filename of the validation file.
9. Clear the Binary file check box.
10. Choose Add. The file appears in the Files and Data list box with an F in the left column.
11. Choose OK to save your changes and return to the Terminal Download Configuration dialog box.

12. In the Terminals and Groups list box, choose the terminal or group you configured.
13. Choose Download. The validation file is downloaded to the terminal or group.

To request a validation file from the controller

Note: The validation file cannot have the extensions *.irl*, *.exe*, *.cmd*, or *.img*.

1. Make sure that you transfer the validation file to the controller. For help, see “Restoring Your User Files” in Chapter 2.
2. Make sure that you have started data collection on the Model 200 Controller.
3. Press Ⓜ to resume the terminal.
4. Press F4 to request a validation file.
5. At the File name? prompt, type:

filename

where *filename* is the name of the validation file.

Running the Application

Once you have selected a screen, you can send data from the screen, reset the screen without sending data, and exit the screen. While you are entering data into screens, you may notice these events:

- Data may appear in an output field that was previously empty.
- A linked screen may appear if data in a field in the current screen meets some predefined value.
- Data that came from a transaction that was sent to your TRAKKER Antares terminal may appear in your screen’s input fields.
- A message that is sent to you from another application may appear in the system message area.



Troubleshooting



This appendix explains the troubleshooting tools provided with your Model 200 Controller. It also lists problems and solutions for error messages that may appear in message boxes or in the error log.

General Troubleshooting

These problems are general system problems that may occur while you are using the Model 200 Controller.

Problem

The external Intermec controller is not communicating with the Model 200 Controller.

The green LED on the Ethernet card is not lit and the card is not communicating with the network.

The green LED on the token ring card is not lit and the card is not communicating with the network.

Solution

Make sure you have defined the correct configuration for the external controller on the Model 200 Controller.

Make sure you are using the correct Intermec cable.

Replace the cable.

Replace the serial card.

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.

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.

Model 200 Controller User's Manual

Problem

The green LED on the RF controller card is not lit and the card is not communicating with the network.

The external Intermec controllers are not communicating with the network.

Keystrokes are not displayed in a field.

The mouse does not work.

Solution

Verify that the data collection devices are communicating.

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.

Make sure that the configuration for the external controller in the Model 200 Controller GUI matches the configuration in the controller.

Make sure that you are using the correct cables to connect your external controller to your network.

Contact your local Intermec representative.

Make sure your keyboard connector is securely seated in the keyboard port on the controller.

With the keyboard connected, shut down the controller 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.

Make sure that your mouse connector is securely seated in the mouse port on the controller.

When the controller has 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 run-time configuration Shows you the active (run-time) configuration. Use this feature 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 controller. 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.

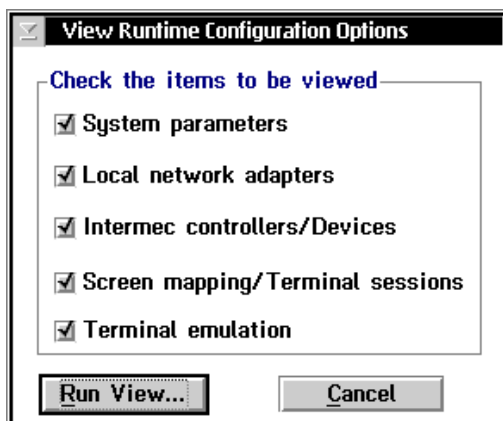
Message boxes and error log file The message boxes and error log file provide a list of messages pertaining to error conditions in the system and in the script. For help, see “Message Box Error Messages” and “Error Log Error Messages” later in this chapter.

Viewing the Configuration

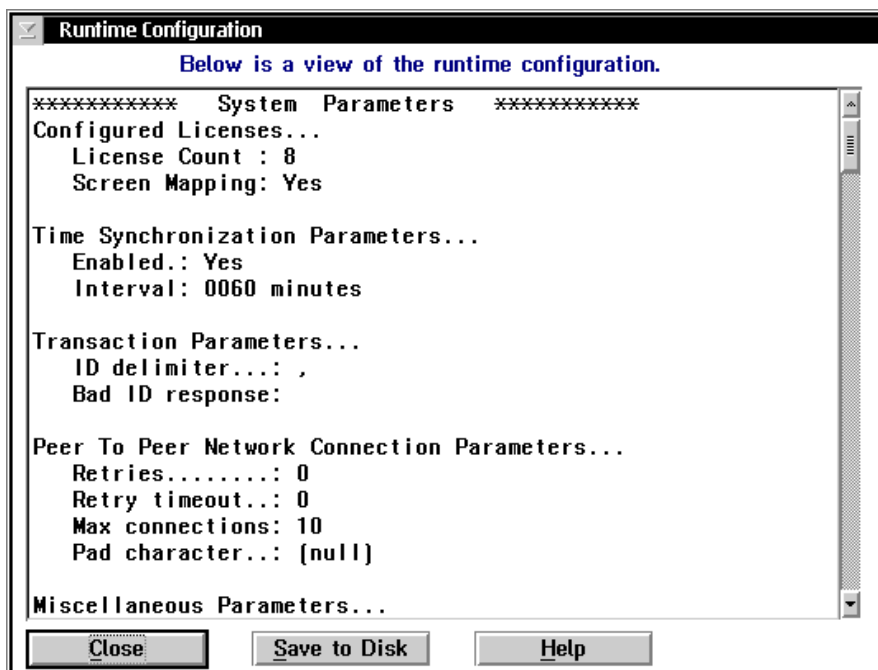
The Model 200 Controller produces a configuration file that you can view to verify the parameters that you have defined for the active configuration.

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. Enable the configuration items that you want to view. A check in a check box will display the item in the Runtime Configuration dialog box.
4. Choose Run View. The Runtime Configuration dialog box appears.



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 controller, choose Save to Disk.
7. Choose Close to close the dialog box and return to the System Reporting dialog box.
8. Choose Close to return to the main menu.

Viewing and Clearing the Hot Standby Files

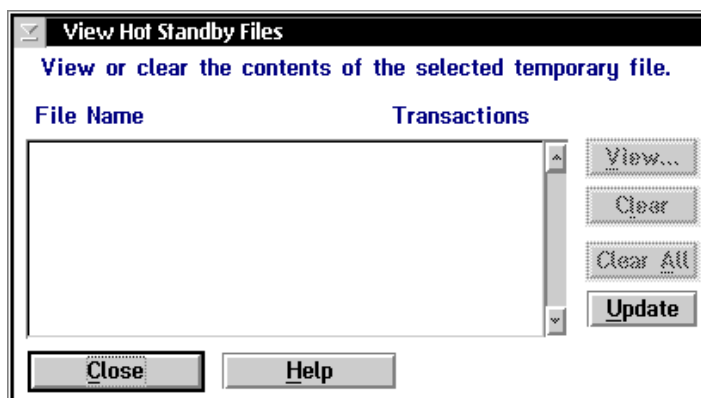
You can view the contents of the Hot Standby files that the Model 200 Controller creates when it places an application or device in Hot Standby mode. The controller waits a certain period of time, which is set in the Hot Standby timeout, after delivering a transaction to an application or device to receive an acknowledgment for the transaction. If it does not receive an acknowledgment, the controller 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.



Message Box Error Messages

These error messages may appear in message boxes on your controller display. If your error message refers to the error log, then you must view the message in the error log. Refer to the next section, “Error Log Error Messages.”

This section contains all the error and event messages in alphabetical order, a brief description of the possible problem, and possible course(s) of action.

If you cannot find 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. For help, see “Understanding the Error Messages” later in this chapter.

Locate the error message in “Understanding the Error Messages” later in this chapter. Check the Problem and Solution columns for information on how to correct the error messages.

3. Contact your network administrator to help you solve the problem.
4. Contact Intermec Technical Support to help you solve the problem.

Note: If the % character appears in an error message in the following table, it identifies a word that is a variable depending on the context of the message box.

Error Message	Solution
% is using this. You must remove all usages before it can be deleted.	You cannot delete an item until you have removed all the references for this item.
% cannot be removed from the Selected Screen list for the next screen references still exist.	You are attempting to delete a screen that is part of a next screen sequence. Unattach the screen from the sequence and try deleting the screen again.
% edit box field requires '-' or uppercase letters.	Enter a '-' (dash) or use uppercase letters to enter data into the field.
% edit box field requires '@', '#', '\$', or alphanumeric data type.	Enter alphanumeric or special characters in the field.
% edit box field requires 12 hexadecimal numbers.	Enter a 12-digit hexadecimal number.

Model 200 Controller User's Manual

Error Message

% edit box field requires 8 hexadecimal numbers.

% edit box field requires alphanumeric data type, beginning with an alphabet.

% edit box field requires hexadecimal data type.

% edit box field requires numeric data type.

A device must be selected to download a terminal template file.

A drive specification is not allowed.

A host screen already exists with this name, enter a unique name.

A host screen field already exists with this name, enter a unique name.

A host screen field has been defined with this name under the current transaction. Please re-enter or select from the drop down list.

A host session must be selected before a connection to the session screen can be made.

A name identifying the field must be entered.

A one character string field can have a picture of X, A or Y.

A problem occurred while saving. Try the 'Save as' choice with a different path.

A screen field already exists with this name, enter a unique name.

Solution

Enter an 8-digit hexadecimal number.

The first character you enter in the field must be an alpha character. The rest of the characters can be alpha or numeric.

Enter a hexadecimal number in the field.

Enter a number in the field.

The controller does not know where to download the template. Select a group or device and try to download the template again.

You are trying to select a drive on the controller. Use the list box to select a specific file on the controller.

Enter a unique, meaningful name for the host screen.

Enter a unique, meaningful name for the host screen field.

Enter a unique, meaningful name for the host screen field or click the down arrow on the right side of the field and select a host screen field.

Configure a host connection for the terminal session. Select a host session before choosing Start.

You have tried to choose OK without entering a name for the transaction field. Enter a unique, meaningful name, then choose OK.

You have assigned an incorrect picture to a 1-character field. You should choose X, A, or Y.

You may be using a reserved path or filename. You do not need to enter a path. Enter your script filename.

Enter a unique, meaningful name for each screen field.



Error Message

A screen must be added to the menu.

A screen with this name already exists, enter a unique screen name.

A Screen/Field combination is needed for mapping. This screen has no fields.

A script file must have an extension of .SCR

A session must be configured for screen mapping.

A terminal template file must have an extension of .TPL

A transaction name can not begin with a %.

An application already exists with this name, enter a unique name.

An error occurred and was logged during the save process. ...Continue?

An error occurred while saving the template file. Ensure you have enough disk space to save the file.

An error occurred while saving the trace file. Ensure you have enough disk space to save the file.

Backup failure: #%.

Solution

You must add a screen to the menu before you can choose OK. If you do not want to add a menu, choose Cancel to exit the dialog box.

Enter a unique, meaningful name for the screen.

You are trying to map transaction fields to a host screen that does not contain any screen fields. Select another host screen that contains screen fields to which you can map transaction fields.

You are trying to save a script file without the extension .SCR. Rename the file to include .SCR.

You must configure a host terminal session before you can define a screen mapping session. Configure a terminal session.

You have tried to save a template file with an incorrect extension. Save the template with the extension .TPL.

You have started the transaction ID with an invalid character. Use another transaction name.

Enter a unique, meaningful name for the application.

Choose Y to continue. View the error log. Locate the error message in "Understanding the Error Messages" later in this chapter. Check the Problem and Solution columns for information on how to correct the error messages.

You may not have enough room on your hard drive to save the template. Delete a template or another user file that you are not using and try saving the template again.

You may not have enough room on your hard drive to save the trace file. Delete a trace file or another user file that you no longer need and try saving the trace file again.

There is a problem with backing up your system or user files. Check your floppy disk and try again. Or, try using another disk. If the problem persists, contact Intermecc Technical Support.

Model 200 Controller User's Manual

Error Message

Before selecting another controller, should the changes for this controller be kept or discarded?

Cannot convert string to a directory.

Cannot delete a host with terminals linked to it.

Cannot delete the controller if the device % is linked to a host.

Cannot download file, ensure the controller is active.

Check the ENTIRE date or time indicated to be sure each field is complete and valid.

Coaxial host connection is not allowed for the 5250 terminal session. Please re-enter.

Column value must be a number from 1 thru 80.

Controller should be shutdown and restarted to fully restore backed up system files.

Could not connect short session id %. No session information is available.

Could not initialize session parameters. No session information is available.

Could not open default configuration file.

Solution

You have configured an external Intermecc controller and you have not chosen OK to save your configuration. Save or discard your changes.

You have not selected a valid directory. Use the root directory list box to open directories and find files.

You are trying to delete a host that you have explicitly linked to terminals. Unlink the host and terminals and then try deleting the host.

You are trying to delete a controller, RF card, or UDP Plus network that has devices that are explicitly linked to a host. Unlink these devices and then try deleting the controller.

You are trying to download a file before you have started data collection. From the main menu sidebar buttons, choose Start Data Collection. Try downloading your file again.

Refer to the online help or the user's manual for information on valid pictures for the date or time field.

You cannot configure a 5250 terminal session using a coaxial adapter card. Configure a 3270 terminal session or select another card to make the 5250 host connection.

In the Column field, enter a value between 1 and 80.

From the main menu sidebar buttons, choose Shutdown Controller. Enable the Save and activate check box and choose Shutdown. When the shutdown is complete, press **Ctrl-Alt-Del** to boot the controller.

The controller cannot find all the information it needs to configure a short session ID. Check your host terminal session configuration in the GUI.

The controller cannot find all the information it needs to configuring a terminal session. Check your configuration in the GUI.

From the main menu sidebar buttons, choose Shutdown Controller and reboot the controller. Try to restore the default configuration again.



Error Message

Solution

Could not open master system file list.

From the main menu sidebar buttons, choose Shutdown Controller and reboot the controller. If the problem persists, contact Intermec Technical Support.

Could not open the migration list file.

See previous solution.

Data collection start FAILED.

From the main menu sidebar buttons, choose Shutdown Controller. Enable the save and activate check box, choose Shutdown, and reboot the controller. Try to start data collection again.

Date value does not match picture string for this field.

You have entered a date into the Value field that does not match the picture you selected for the date in the Picture field. Refer to the online help or user's manual for valid date pictures.

Deletion failure: #%.

From the main menu sidebar buttons, choose Shutdown Controller and reboot the controller. If the problem persists, contact Intermec Technical Support.

Device missing IP Address.

All terminals in the UDP Plus network require an IP address before you can enable them for data collection. Obtain an IP address from your network administrator and enter it in the Controller Device Parameters dialog box.

ERROR - Access to drive denied

You are trying to access a drive that is unavailable. Use the root directory list box to access directories and subdirectories.

ERROR! Cannot delete the last IP Address if a UDP+ controller has been configured.

You are trying to delete the last IP address and the UDP Plus network is still valid. Delete the UDP Plus network from the controller list and then try deleting the IP address.

ERROR - Diskette is write protected

Remove the floppy disk you inserted in the floppy disk drive of the controller. Verify that the write-protect tab is in the Write position. Re-insert the floppy disk and try using it again. Or, try another disk.

ERROR - Not a DOS diskette

The disk you inserted may be configured for a Macintosh computer or it may not be configured. Remove the floppy disk you inserted in the floppy disk drive. Insert another DOS-formatted disk in the floppy disk drive and try again.

Error creating script template, dumpscrn.exe must reside on the controller

The controller cannot find the DUMPSCRN utility. From the Screen Mapping Session ID dialog box, choose Create. The DUMPSCRN window should appear. If it does not, contact Intermec Technical Support.

Model 200 Controller User's Manual

Error Message

Error during data collection stop, see Error Log. Stop procedure will continue...

Error retrieving field information from session %.

Error selecting template file.

Error spawning process, statmon.exe must reside on the controller.

Error spawning process, trace.exe must reside on the controller.

Error starting editor to modify script file.

Error starting host terminal session, ensure the configuration has been saved and activated

Error starting keystroke capturing.

Error verifying script template, scrcheck.exe must reside on the controller.

Failure reading upgrade diskette. Upgrade aborted.

Field position information for field %, does not correspond with defined screen size.

Solution

View the error log. Locate the error message in "Understanding the Error Messages" later in this chapter. Check the Problem and Solution columns for information on how to correct the error messages.

You are trying to use the get fields feature to create field parameters for your screen. Make sure that the host window that you are trying to get the field information from is field-formatted.

You have selected an invalid template. Make sure you have selected the correct template and try again.

The controller cannot find the status monitor program. From the main menu sidebar buttons, choose Shutdown Controller and reboot the controller. If the problem persists, contact Intermec Technical Support.

The controller cannot find the trace program. From the main menu sidebar buttons, choose Shutdown Controller and reboot the controller. If the problem persists, contact Intermec Technical Support.

The controller cannot find the manual editor for the script file. Intermec highly recommends that you use the Script Builder Tool to create and edit script files. From the main menu sidebar buttons, choose Shutdown Controller and reboot the controller. If the problem persists, contact Intermec Technical Support.

Make sure that you have configured a host connection. From the main menu, choose Activate to save and activate the runtime configuration. Try starting the terminal session again.

Make sure that you have started your host terminal session.

The controller cannot find the script checker utility. From the Script Builder Tool, open the script that you want to check and choose Check Script. If it does not check the script, contact Intermec Technical Support.

Verify that the correct upgrade disk is in the controller disk drive. Contact Intermec Technical Support.

Select a different value for the row, column, or field length so that it will fit in the screen. Run the Terminal Session Viewer to help you see what the screen you are building looks like.



Error Message

Field position values (row, column and length) will cause this field to overlap an existing field.

Field position values (row, column or length) are too large for a terminal screen.

File name must be between 1 and 8 characters in length

Frequencies must be unique for each BRU. Please select a different frequency.

Go to next screen was checked but one was not configured. Use the Screen button to select one.

If you delete this host, another host will be automatically selected to keep this session valid.

Illegal file name, enter a valid 8.3 file name.

Illegal picture for string field.

Input for the indicated field is incompatible with the specified data type.

Input for the indicated field is incomplete, invalid or out of range. Please re-enter.

Input for the indicated field is required and only alphanumeric or underscore characters are allowed. Please re-enter.

Input for this numeric field must from - 2147483648 through 2147483647. Please re-enter.

Solution

Run the Terminal Session Viewer so you can see where the fields on your screen are.

Select a smaller value for the row, column, or field length so that it will fit in the screen. Run the Terminal Session Viewer to help you see what the screen you are building looks like.

Enter a name that is no longer than eight characters.

Make sure that each BRU has a different frequency, even if the BRU is not enabled.

In the Next Screen? box, you checked the Yes check box, but you did not choose the next host screen. Click the down arrow on the right side of the Name field and select a next host screen, or click New to define a new host screen.

Make sure that you want to delete the host even though you are currently running a terminal session. If you delete the host, the controller picks another host to keep the terminal session valid.

Contact your network administrator for a valid 8.3 file name.

Refer to the online help or the user's manual for information on valid pictures for the string field.

Refer to the online help or the user's manual for information on data types. Enter a valid input for the field.

Refer to the online help or the user's manual for information on the value and default characters for the field. Try a new value for the field.

You have entered an invalid entry in a required field. Try entering a new value that contains only alphanumeric characters and underscores. Do not use special characters.

You have entered a number that is too large or too small for this field. Try a new number for the field.

Model 200 Controller User's Manual

Error Message

Invalid address format for % field.

Invalid data in initial value field for a numeric field.

Invalid IP address.

Invalid picture data for a date field.

Invalid picture data for a numeric field.

Invalid picture data for a time field.

Invalid upgrade disk in drive.

IP address % already in use.

LAN adapter & protocol activate may not have completed normally. Activate halted.

Maximum length for a numeric field is 11 including '+' or '-' and '.'

Maximum number of NAU addresses used. Cannot link any more terminals to the selected host.

Memory integrity error. Shutdown recommended.

Missing data entry for % edit box field.

Solution

Refer to the online help or the user's manual for information on the field. Try a new value for the field.

Make sure that you select a number for numeric fields. Enter a new value.

The format for IP addresses is *yyy.xxx.xxx.xxx* where *yyy* is from 1 to 126, 128 to 223 and *xxx* is from 0 to 255. Verify that you received the correct IP address from your network administrator.

Refer to the online help or the user's manual for information on valid pictures for date fields.

Refer to the online help or the user's manual for information on valid pictures for numeric fields.

Refer to the online help or the user's manual for information on valid pictures for time fields.

You are trying to upgrade your terminal license or screen mapping license with an incorrect disk. Verify you have the correct disk in the controller disk drive and try again.

You are assigning an existing IP address to a network adapter card or device. Each IP address must be unique. Enter a new IP address.

You cannot activate the changes that you have made. Contact Intermec Technical Support.

You are trying to enter more than 11 characters into a numeric field. Make sure that the length of the field does not have more than 11 characters, including symbols.

There are 254 NAUs available. Any NAUs in the NAU pool cannot be used to explicitly link hosts and terminals. You may be able to link more hosts and terminals by removing NAUs from the NAU pool.

From the main menu sidebar buttons, choose Shutdown Controller. Enable the save and activate check box, choose Shutdown, and reboot the controller.

You chose OK without entering information in all the required fields for the dialog box. Refer to the online help or the user's manual to find out which fields are required.



Error Message

Must have one or more entries in the % list box.

No disk or wrong disk in drive A. Try again?

No field is highlighted. Please highlight a field on the VT terminal by double clicking or dragging using the mouse.

No terminal screen was chosen. Choose one, create a new one, or uncheck the box.

No transaction IDs are available to be configured for an OUTPUT transaction. You must create a new transaction ID.

Not a Controller generated System Backup diskette.

One or more terminals must be configured for a group.

Out of range. Valid range is 10-9999.

Picture and initial value do not match, modify picture or initial value.

Range To value must be greater than range From value.

Remove diskette's protection and press OK to continue with upgrade.

Restore failure: #%d

Row value must be between 1 and 24.

Solution

You need to add at least one item from the Available list box to the Selected list box before you choose OK. Choose Cancel to exit the dialog box.

Make sure that you have the correct disk in drive A.

To get attributes from a VT/ANSI host screen, you must highlight the entire area on the host screen.

You enabled the From terminal screen check box, but did not enter which terminal screen the transaction will come from. Click the down arrow on the right side of the field and select a terminal screen or choose New and define a new one.

You do not have any more transaction IDs to use for the output transaction for the screen. Define a new transaction ID for the screen.

You are trying to restore the system files and runtime configuration using a disk that the controller did not generate. Verify you are using the correct disk and contact Intermecc Technical Support.

When configuring a group, you need to add at least one terminal from the Available Terminals list box to the Selected Terminals list box before you choose OK. Choose Cancel to exit the dialog box without creating a group.

Enter another value between 10 and 9999 in the field.

The prefix that you defined does not match the characters in the Picture field. Enter a new prefix or change the characters in the Picture field.

When specifying a numeric range, you must enter a larger number in the To field than in the From field.

The disk in drive A is write-protected. You need to remove this protection before the upgrade process can continue. Refer to your disk manufacturer's documentation.

The controller cannot restore your files. Make sure your floppy disk is not write-protected. Copy your files to another disk and try again.

In the Row field, enter a value between 1 and 25.

Model 200 Controller User's Manual

Error Message

Screen fields must exist to define a screen.

Script file name cannot use illegal special characters..

Script file name must be between 1 and 8 characters in length.

Selected host session is already active.

Specify file name only. No path or drive information is needed.

Specify static value and data type.

Stop time must be later than Start time. Please re-enter.

Target directory creation error.

Target file must contain full file path information.

Terminal emulation session is already started.

Terminal session activation may not have completed normally. Activate halted.

The 3-letter prefix entered is reserved. Please re-enter.

The address entered is already in use.

The address entered is already used by the same adapter card. Please re-enter.

The backup diskette created is specific to this controller. Restoring to a different controller with this diskette may cause unpredictable results.

Solution

You need to define screen fields for the screen before you choose OK. Choose Cancel to exit the dialog box.

You have entered a name for the script file that contains special characters that you are not allowed to use. Choose another name.

You have entered a name for the script file that is more than eight characters. Choose a shorter name.

You are trying to start a host session that is already active.

You have entered the drive and path name. Enter the filename only.

These are required fields. Refer to the online help or the user's manual for information.

The stop time that you entered is earlier than the start time. Enter a new start time or stop time.

The controller could not create the target directory. Enter a new target directory and try again. If the problem persists, contact Intermec Technical Support.

Enter the complete path name including drives, directories, and file name in the field.

You are trying to start a host session that is already active.

Verify that you set all the correct terminal session parameters. Choose Shutdown Controller. Enable the Save and activate check box and choose Shutdown. When the shutdown is complete, press **Ctrl-Alt-Del** to boot the controller.

The controller uses a few special 3-letter prefixes. Use another unique, meaningful prefix.

See previous solution.

Verify the address you entered. Contact your network administrator for another address.

Intermec does not recommend that you use the system backup disk in a new controller.



Error Message

The cursor position is in a protected (read-only) area that is not valid for an input field. Do you want to get the field info anyway?

The cursor position is in an unprotected (writeable) area that is not recommended for a screen ID. Do you want to get the field info anyway?

The cursor position on the host screen is invalid.

The controller must now reboot for activate to complete. Since the auto-start system parameter is %.

The controller must now reboot for this action to complete. Since the auto-start system parameter is %.

The default value is not within the defined validation range.

The Define terminal prompt box is unchecked. Do you want to delete the existing prompt field %?

The device connection entered is already in use. Please re-enter.

The file is empty.

The file name specified does not exist.

The first character for a %s cannot be a numeric value.

The Host LU entered is already in use by another adapter card. Please re-enter.

Solution

In 5250 field-formatted host screens there are protected fields and unprotected fields. To get attributes for a host screen field, you should place your cursor on an unprotected field.

In 5250 field-formatted host screens there are protected fields and unprotected fields. To get the screen ID for a host screen, you should place your cursor on a protected field that contains static text.

The cursor on the host screen is positioned where you cannot get any attributes. Move the cursor to a protected or unprotected field and try getting the attributes again.

From the main menu sidebar buttons, choose Shutdown Controller. Enable the Save and activate check box and choose Shutdown. When the shutdown is complete, press **Ctrl-Alt-Del** to boot the controller.

From the main menu sidebar buttons, choose Shutdown Controller. Enable the Save and activate check box and choose Shutdown. When the shutdown is complete, press **Ctrl-Alt-Del** to boot the controller.

You have entered a value in the Default field that is not within the range you specified.

You have information in the Define terminal prompt box, but you have not enabled this prompt. Enable the prompt or delete the existing prompt field.

Enter another device connection.

You are using a file that has no contents. Verify you selected to correct file. Select another file.

The controller cannot find the file that you entered. Verify that you entered the correct file name. Select another file.

Enter a new value that starts with an alpha character.

Enter another unique host LU name.

Model 200 Controller User's Manual

Error Message

The initial value specified is longer than the defined field length.

The Keystrokes box is checked but no keystrokes were configured.

The Local and Network ports must be unique.

The logical name entered is already in use. Please re-enter.

The maximum link stations value must be between 1 and 255. Please re-enter.

The maximum Picture length is 11 including a leading sign of '+' or '-'

The message cannot be deleted, it is referenced by region: %s.

The message cannot be deleted, it is used as a screen event for tran ID: %s.

The name or label entered is already in use. Please re-enter.

The network adapter address must be between 020000000000 and FFFFFFFF. Please re-enter.

The network adapter address must be between 400000000000 and 7FFFFFFF. Please re-enter.

The picture field length must be less than or equal to the field length.

Solution

The prefix you defined is longer than the field length. Enter a shorter prefix or a longer field length.

You enabled a keystrokes check box, but you did not define the keystrokes. Make sure that you have started a host terminal session. Capture the keystrokes that you need. Refer to the online help or user's manual.

You have entered the same UDP port number for the local and network ports. Enter a different port numbers for the local and network ports.

Enter a unique, meaningful name for the logical name of the object.

Enter a value between 1 and 255 into the maximum link stations field.

You are trying to enter more than 11 characters into a Picture field with a numeric data type. Make sure that the length of the field does not have more than 11 characters, including symbols.

You are trying to delete a message that a region sends as an action. Go to the Host Screen Region Definition dialog box and choose another action. Then, you can delete the message.

You are trying to delete a message that is being used as a screen event.

Enter a unique, meaningful name for the item.

You have entered an incorrect network adapter address. Enter another address that is a hexadecimal number between 020000000000 and FFFFFFFF.

You have entered an incorrect network adapter address. Enter another address that is a hexadecimal number between 400000000000 and 7FFFFFFF.

The value in the Picture field contains more characters than you have specified in the Length field. Enter a fewer characters in the Picture field or more characters in the Length field.



Error Message

The Picture length is greater than the length specified for a Range.

The Picture value specified doesn't match the value specified for the Range.

The Range value specified is longer than the defined field length.

The range values are incompatible. Change the 'from' or 'through' value.

The region button was checked but a valid region was not specified.

The screen cannot be deleted. It is referenced by other screens or regions as the next screen.

The screen cannot be deleted. It is referenced by transaction %.

The Screen/Field name combination is already specified. Enter a unique combination.

The selected Host cannot be deleted, it is referenced by the terminal session.

The selected host session name is used by another screen mapping session.

The selected screen is the main screen. You MUST uncheck the main screen attribute before removing it.

Solution

The range that you specified for the field contains more characters than the number of characters that are in the Picture field. Change the range for the field or increase the number of characters in the Picture field.

The range that you specified for the field contains a different number of characters than the number of characters that are in the Picture field. Change the range for the field or change the number of characters in the Picture field.

The range that you specified for the field contains more characters than the number you defined for the length of the field. Change the length of the field or decrease the number of characters in the range.

The range that you have entered is not valid. Make sure that the value in the From field is less than the value in the To field.

You are defining a message that requires additional text from a host screen region. You need to click the down arrow on the right side of the Region field and select a region or check the Current region check box.

You are trying to delete a host screen that is part of a next screen sequence. Remove the screen from the next screen sequence before you delete it.

You are trying to delete a host screen that the transaction maps its fields to. Change the mapping or remove the transaction before you delete the screen.

You can map each screen field to only one transaction field.

You are trying to delete a host that the controller is using for the terminal session.

Enter a unique, meaningful name for the host session name.

You are trying to delete a host screen that is the main host screen. Select the screen and clear the Main screen check box before you delete it.

Model 200 Controller User's Manual

Error Message

The selected transaction field % has already been mapped in this host screen.

The Send Message box is checked but no message was configured.

The starting address must have the same subnet address as a currently configured ethernet card.

The starting IP address plus the number of terminals to enable results in a invalid IP address.

The Subnet Address entered is already in use by another adapter card. Please re-enter.

The temp file cannot be cleared since it is currently in use.

The terminal screen is used by the current open script.

The terminal session cannot be deleted since it is currently used for screen mapping.

The total data length of a trx for a screen is limited to 254 characters. Please remove or shorten an input field.

The total number of screens in a menu is limited to 19. Please remove one or more screens.

The transaction can not be deleted, it is in use by %.

Solution

You are trying to map a transaction field to a second host screen field in the same host screen.

You enabled a check box that sends a message to the source of the transaction, but you did not define the message. Click the down arrow on the right side of the field and select a message or choose Define to define a new message.

The IP addresses of the devices in the UDP Plus network must have the same subnet address as the Ethernet network adapter card. Verify the IP address with your network administrator.

You have entered a starting IP address that does not contain enough sequential valid IP v4 addresses for the number of UDP Plus terminals that you want to enable. Choose a new starting IP address or manually enter the terminal IP addresses.

Enter a unique subnet address for the card.

You are trying to delete a file that is currently in use. Check the contents of the file before you delete it.

You are trying to delete a terminal screen that is being used by the script file.

You are trying to delete a terminal session that is being used by a screen mapping session. Select another terminal session for the screen mapping session. Then, you can delete the terminal session.

You have created a terminal screen whose output transaction will be greater than 254 characters. Redefine your terminal screen.

You are trying to include more than 19 screens in the menu. Try combining some screens or rethinking your application definition.

You need to remove the transaction from the object that is using it before you can delete it.



Error Message

The transaction cannot be deleted, screen mappings exists for this screen mapping session.

The transaction field entered is already in use. Please re-enter.

The transaction field selected cannot be removed while it is referenced in a field mapping.

The transaction ID entered is already in use. Please re-enter.

The transaction is used by a terminal template screen definition.

The trx field is in use for the following terminal template screen/field:

The Upper bound must be greater than the Lower bound value.

The value entered is already being used by another RF Card.

The value string must be at least as long as the picture string.

This group name is already in use, enter a different name.

This is the only host so it cannot be deleted now. Add a new host, then retry deleting this host.

This item is being used. You must remove all references to it before it can be deleted.

Time value does not match picture string for this field.

Solution

You cannot delete the transaction because you have mapped its fields to screen fields. You need to remap the screen fields before you can delete the transaction.

Enter a unique, meaningful name for the transaction field.

You cannot delete the transaction field because you have mapped it to a screen field. You need to remap the transaction field before you can delete it.

Enter a unique, meaningful name for the transaction ID field.

You are trying to delete a transaction that is used as an output transaction for a terminal screen.

Select another transaction field to use or redefine the existing terminal screen field.

You need to enter a larger number in the Upper limit field than in the Lower limit field.

Enter a unique value.

The value that you entered in the Value field does not match the Picture field. Change the Value field or the Picture field so they match.

Enter another unique, meaningful group name.

You must have at least one host configured. If you want to delete the current host, you must configure a new host. Then, you can delete the existing host.

You are trying to delete an item that is being used by another item. Remove the reference to the item and then you can delete it.

You have entered a time into the Value field that does not match the picture you selected for the time in the Picture field. Refer to the online help or user's manual for valid time pictures.

Model 200 Controller User's Manual

Error Message

Twinaxial host connection is not allowed for the 5250 terminal session using S/36 host type. Please re-enter.

Unable to access file specified to fill choice lists. Check Screen Mapping Interface definition.

Unable to allocate memory for this action. Try removing unneeded items before retrying.

Unable to create new script file

Unable to create the condition list.

Unable to establish communications with Message Handler. There may be another instance of it running.

Unable to load NEXTGEN configuration file (%u%u).

Value does not match picture defined for the field.

VT data timeout cannot exceed the host transaction timeout (1 minute = 60000 milliseconds).

You have not chosen an OUTPUT transaction ID. The default choice will be used.

You have unsaved configuration changes. Should they be saved now or discarded?

Solution

You cannot configure a 5250 terminal session for an S/36 host using a twinaxial adapter card. Configure a 3270 terminal session or select another host type to make the 5250 host connection.

Verify that your terminal session and screen mapping session contains correct information. Contact Intermecc Technical Support.

Try deleting any items that you do not need for your runtime configuration. Choose Shutdown controller. Enable the save and activate changes check box. Reboot your controller and Contact Intermecc Technical Support.

View the error log. Locate the error message in "Understanding the Error Messages" later in this chapter. Check the Problem and Solution columns for information on how to correct the error messages.

See previous solution.

Choose Shutdown Controller. Enable the Save and activate check box. Choose Shutdown Controller and then Choose Start Data Collection. If the problem persists, contact Intermecc Technical Support.

View the error log. Locate the error message in "Understanding the Error Messages" later in this chapter. Check the Problem and Solution columns for information on how to correct the error messages.

The value that you specified for the Value field contains a different picture than the picture defined in the Picture field. Change the value in one of the fields so that the Value field and Picture field match.

You have entered a larger value in the Data response timeout field than in the host transaction timeout. Decrease the data response timeout or increase the host transaction timeout.

The default for an output transaction ID is filename_tx. Enter a unique transaction ID if this one is not acceptable.

You are closing the Script Builder tool without choosing the Save button. Choose Save to save your changes and Discard to not save your changes.



Error Message

You must check one of the Region Appearing or Region Not Appearing boxes.

You must configure an ethernet adapter before configuring the UDP Plus Network.

You must create field definitions for this transaction before specifying placement information.

You MUST select a next screen. Use the New button if you need to create a screen.

You MUST use the Current button to select a current screen before proceeding.

You MUST use the Current button to select a current transaction before proceeding.

You MUST use the Main screen check box to select a main screen before proceeding.

Solution

When you add a region, Script Builder requires that you define actions for the region appearing or not appearing. Refer to the online help or user's manual for configuring actions.

Configure at least one of your Ethernet TCP/IP cards before configuring the UDP Plus network. Refer to your online help or user's manual.

You need to define the transaction field for the transaction before you can give it a field position number.

You are defining a next screen sequence, but you have not chosen a the next screen. Click the drop-down arrow on the right side of the field and select a next screen or choose New to create a new screen.

Script Builder needs to know the host screen for which you are defining host screen fields, regions, and messages. Select a screen from the Selected Screens list box and choose Current.

Script Builder needs to know the transaction whose fields it will map to host screen fields. Select a transaction from the Selected list box and choose Current.

Script Builder needs to know the main host screen which is the first host screen that receives all transactions for this script. Select a screen from the Selected Screens list box and enable the main screen check box.

Error Log Error Messages

Error messages are generated by the Model 200 Controller. The controller sends these messages to the status monitor and to the error log.

Viewing the Error Messages

The controller 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 controller 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

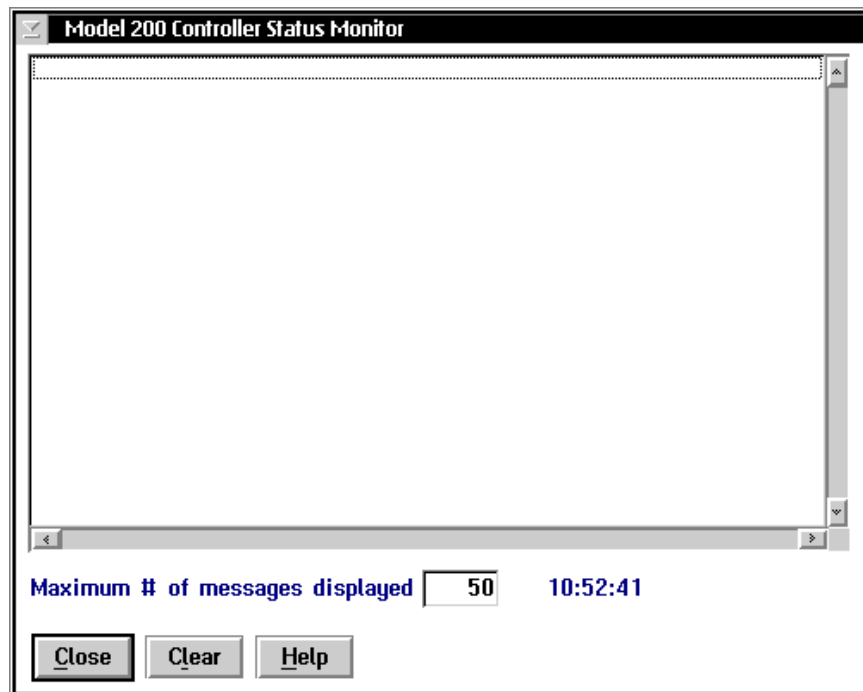
```
1996-08-25 11:28:55 7-952-248
EMCOMM ERROR - The transaction Id was not found in
configuration file
  FATAL ERROR 10
  INSIDE: TEST002
  FUNCTION CODE: 6 [Bad Data from Config File]
```

Using the Status Monitor

The 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 Model 200 Controller 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 troubleshooting the error messages, see "Understanding the Error Messages" later in this chapter.

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.
6. Choose Close to return to the main menu.

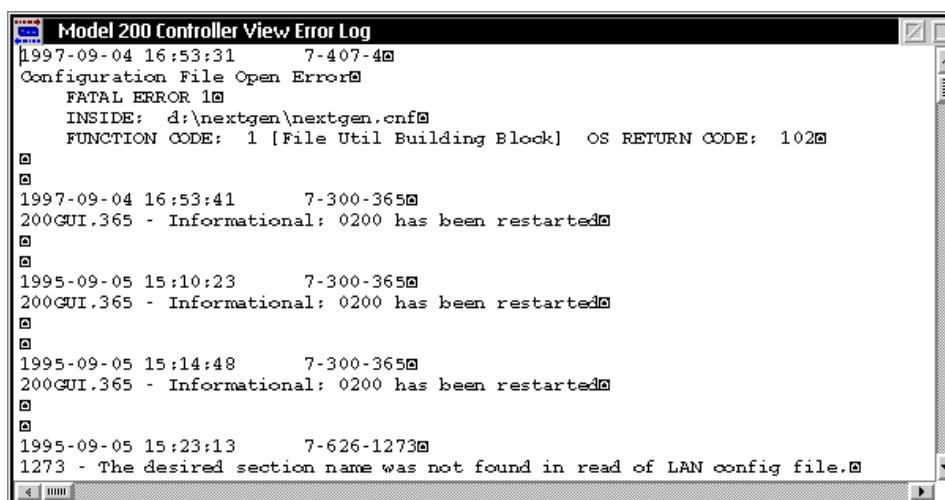
Using the Error Log

The error log, NGERERROR.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 re-open the error log. When messages are logged to this file, no message box appears on the screen.

The error log is limited to 700K and has two backup versions. When NGERERROR.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, NGERERROR.LOG becomes NGERLOG1.BAK. NGERLOG2.BAK is not backed up.

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 Messages. The Model 200 Controller View Error Log dialog box appears.



3. Use the horizontal and vertical scroll bars to view your error messages. For help troubleshooting the error messages, see "Understanding the Error Messages" later in this chapter.



4. Double-click on the box in the upper left corner to close the dialog box and return to the System Reporting dialog box.
5. Choose Close to return to the main menu.

Understanding the Error Messages

This section contains all the error and event messages in alphabetical order, a brief description of the possible problem, and possible course(s) of action.

If you cannot find an error message:

1. Write down the entire message that is in the error log.
2. Contact your network administrator to help you solve the problem.
3. Contact Intermec Technical Support to help you solve the problem.

Error Number	Error Message	Solution
2	Unable to allocate memory for device table pointers	<p>Problem There is not enough memory to allocate space for the device and the communication parameter tables. The communication parameter tables require two pointers configured for each device plus two pointers for a null device. If you encounter errors while allocating small tables like these, it may indicate a significant system problem or severe memory shortage.</p> <p>Action Shut down and reboot the controller.</p>
3	Unable to allocate memory - memory not available	<p>Problem A memory allocation command was unable to execute successfully. This problem occurred while allocating space for a specific system table. If you encounter errors while allocating small tables like these, it may indicate a significant system problem or severe memory shortage.</p> <p>Action Shut down and reboot the controller.</p>
4	Configuration File Open Error	<p>Problem A system error occurred when the controller was trying to open the configuration file.</p> <p>Action Check the system error code for more information. Make sure that you have activated your runtime configuration. Verify the contents of the configuration file using the View Configuration feature and reboot the controller. If necessary, restore the default configuration file and reconfigure your system.</p>

Model 200 Controller User's Manual

Error Number	Error Message	Solution
5	Configuration File Read Error	<p>Problem A system error occurred when the controller was trying to read its configuration file.</p> <p>Action Check the system error code for more information. File read errors usually indicate a corrupt file. Verify the contents of the configuration file using the View Configuration feature and reboot the controller. If necessary, restore the default configuration file and reconfigure your system.</p>
6	MsgHandler. App id not found - no ACK response sent to safer mode devcom	<p>Problem The message handler could not find the source name of the Safer mode in its internal memory tables. Therefore, the message handler could not send a response to the DevComm.</p> <p>Action The message handler logs this error message along with the source application name from the original transaction. This error usually indicates that an invalid transaction was sent by an application trying to emulate a DevComm.</p>
7	Configuration File Close Error	<p>Problem A system error occurred when the controller was trying to close the handle to the configuration file.</p> <p>Action Check the system error code for more information.</p>
10	Invalid data in DCMSENDFIL system transaction	<p>Problem A DcmSendFil system transaction was received with missing or invalid data. The request was not processed and no file or data was downloaded to a device.</p> <p>Action Retransmit the system transaction to the Receive channel with valid data. See the <i>Model 200 Controller Technical Reference Manual</i> for more information about the format of this transaction.</p>
11	Could not get license information from license file.	<p>Problem This informational message is generated by the message handler informing you that your device license file is missing or corrupt. The message is followed by supplemental information that gives the name of the file the message handler tried to open and the return code it received while accessing that file.</p> <p>Action If you purchased a terminal license with your controller and you receive this message, locate the terminal license you received with your controller and follow the directions to reapply the license.</p>



Error Number	Error Message	Solution
12	Supported device count information:	<p>Problem This informational message is generated by the message handler. It is followed by information on how many devices the controller is communicating with or will communicate with. The message handler emits this message every time you start the controller. It also emits the message every time it sends or receives data from a device it has not communicated with before. For example:</p> <pre data-bbox="602 890 1114 961">1994-04-13 21:03:29 7-5-12 Supported device count information: Number of devices allowed is 1.</pre> <pre data-bbox="602 1003 1203 1100">1994-04-15 09:33:46 7-23-12 Supported device count information: Current device count is now 30. Transaction originated from device: rdrpA</pre> <p>Action If the number of devices allowed does not correspond to the number shown on your terminal license, contact your local Intermec representative. Pay attention to the current terminal count to ensure you do not exceed the number of terminals for which you are licensed.</p>
13	Active device count limit reached. Transaction not routed.	<p>Problem This warning message is generated by the message handler informing you that the number of devices that the controller is attempting to communicate with is greater than your device license allows.</p> <p>Action When the message handler emits this message, it has discarded a transaction. To avoid any further loss of data, shut down the controller and take steps to migrate your terminal license to the next level to allow the controller to communicate with more terminals.</p>
16	Error creating DC IPC channel - Message handler exits	<p>Problem A system error occurred while the message handler input IPC channel was being created. This channel is essential to the operation of the controller.</p> <p>Action Check the specific system error for further information. Shut down and reboot the controller. Start data collection.</p>

Model 200 Controller User's Manual

Error Number	Error Message	Solution
17	Error creating DC ACK IPC channel - Message handler exits	<p>Problem A system error occurred while the message handler acknowledgment IPC channel was being created. This channel is essential to the operation of the controller.</p> <p>Action Check the specific system error for further information. Shut down and reboot the controller. Start data collection.</p>
18	Error opening an application or DevCom IPC channel	<p>Problem A system error occurred while an application destination channel, auxiliary channel, DevComm channel, or DevComm ACK channel was being opened. The controller is not able to communicate with the application or DevComm involved.</p> <p>Action Make sure you have started data collection. Check the specific system error code for more information. You may need to shut down and reboot the controller.</p>
22	Invalid number of bytes in transaction read from DCM_ACK IPC channel	<p>Problem A system error occurred while reading the ACK channel.</p> <p>Action Check the specific system error code for more information.</p>
23	Error reading Message handler input IPC channel - DCM_Q	<p>Problem A system error occurred while reading the Receive channel.</p> <p>Action Check the specific system error code for more information.</p>
24	Failure to convert transaction number in transaction from device	<p>Problem An error was returned from an internal conversion routine. A transaction that was routed to an application may have an invalid transaction number.</p> <p>Action Verify data sent to the application has valid transaction numbers in the transaction header. Contact Intermec Technical Support.</p>
28	MsgHandler. Error reading from the application temporary file	<p>Problem A system error occurred while reading from an application temporary file. Data may not have been delivered to the application.</p> <p>Action Shut down the controller and verify that the temporary files are not corrupted. Also, check the specific system error code for more information</p>



Error Number	Error Message	Solution
29	MsgHandler. Error closing or deleting a destination's temporary file	<p>Problem A system error occurred while deleting a Hot Standby file.</p> <p>Action Shut down the controller and verify that the temporary files are not corrupted. Also, check the specific system error code for more information.</p>
30	App id was not found - no response sent to device	<p>Problem A transaction was sent from a device with an invalid transaction ID or the application table does not contain all configured applications. If a transaction was configured to be sent to the device or the bad transaction ID response is in use, then this transaction was not delivered to the device.</p> <p>Action Verify that transactions sent from your devices have valid transaction IDs that are configured for valid applications.</p>
31	Error writing transaction to an application temporary file	<p>Problem A system error occurred while writing to an application's temporary file. Data may be lost.</p> <p>Action Verify the environment variable DCMAPFILES is valid. Check the specific system error code for more information.</p>
32	Error writing transaction to an application temporary IPC channel	<p>Problem A system error occurred while writing a transaction to an application's auxiliary channel (AUX_Q). Data may be lost.</p> <p>Action Check the specific system error code for more information. Run the Status Monitor feature in the controller to determine if transactions are being stored to an application's auxiliary channel. Check the configuration for the maximum number of transactions that was defined for this channel.</p>
33	Error getting device handle - logical or physical information not available	<p>Problem A logical name for a destination device could not be associated with a physical address for that device.</p> <p>Action Verify that the destination ID in the transaction is a valid device configured in the GUI.</p>

Model 200 Controller User's Manual

Error Number	Error Message	Solution
34	Error writing acknowledgment to a DevCom or application ACK IPC channel	<p>Problem An internal system error occurred while writing an internal system timeout transaction to the Receive channel or a response transaction to a DevComm ACK channel. A memory problem may exist. A response from an application to a device may not be delivered to the device. The application is not notified of a problem unless the controller is configured to respond to application and the response is not received by the application in a reasonable period of time.</p> <p>Action Check the specific system error code for more information. If a response transaction is involved, verify whether data was received at the device. Contact Intermec Technical Support.</p>
37	Invalid number of bytes in transaction read from application temporary file	<p>Problem A record was read from an application's temporary file that had less than 96 bytes or more than 1120 bytes. The transaction was not forwarded to the application, but still exists in the application's Hot Standby file (.TMP).</p> <p>Action Internal error. However, the application's temporary file may have been corrupted on the disk. Verify the contents of the file by viewing the Hot Standby file. The file may have to be deleted after the controller is stopped, which could result in loss of data. The Hot Standby file is only used if an application is not interactive with the controller. Contact Intermec Technical Support.</p>
38	Error opening or creating an application temporary file	<p>Problem A system error occurred while opening an application's Hot Standby file.</p> <p>Action Verify that enough disk space is available to create new files and the environment variable DCMAPPPFILES is set. Check the environment variable DCMMAXFH to ensure that enough file handles are available in the system. You can use the following equation to determine the maximum number of file handles required by the message handler:</p> $\text{file handles} = (\# \text{ configured ports})^2 + (\# \text{ total applications} + 1)^2 + 3$ <p>Check the specific system error code for more information.</p>



Error Number	Error Message	Solution
39	Error reading a transaction from an application temporary IPC channel	<p>Problem A system error occurred while the message handler was reading a transaction from one of its internal auxiliary channels (AUX_Q). The message handler maintains an auxiliary channel for each application that it communicates with. It uses the AUX_Q channel to store a transaction for an application that has not acknowledged the last transaction, but has not timed out. When an application times out or when the number of transactions in an AUX_Q channel exceeds the user-defined limit, the message handler writes all the transactions into a Hot Standby file.</p> <p>Action Check the specific system error code for more information. This may be an internal problem. Contact Intermec Technical Support.</p>
40	DCM_Q IPC channel error after ACK interrupt	<p>Problem A system error occurred while querying the Receive channel after an acknowledge was received in the ACK channel.</p> <p>Action Check the number of elements available in the Receive channel using the Trace feature. Check the specific system error code for more information. Since this error occurred on a query, it is likely that the data is preserved. Check the data sent to devices and applications and recover any bad data. Contact Intermec Technical Support if the problem persists.</p>
41	DCM_ACK IPC channel error after ACK interrupt	<p>Problem A system error occurred while querying the ACK channel after an acknowledge.</p> <p>Action Check the number of elements available in the Receive channel using the Trace feature. Check the specific system error code for more information. Since this error occurred on a query, it is likely that the data is preserved. Check the data sent to devices and applications and recover any bad data. Contact Intermec Technical Support if the problem persists.</p>
42	Error writing to DCM_Q	<p>Problem A system error occurred while writing a transaction to the Receive channel.</p> <p>Action This error only occurs when the controller is trying to send the current time to its connected controllers. Data is not lost, but you should try to determine the cause of this error. Check the system specific return code for more information on what may have caused the error.</p>

Model 200 Controller User's Manual

Error Number	Error Message	Solution
44	Failure setting the ACK timeout timer for an application	<p>Problem When a transaction is delivered to an application's channel, a timer is started to make sure the application acknowledges the transaction within the Hot Standby timeout period. If no system error code was returned for this transaction, then the offset in the system application table is invalid. If a system error code was reported, then a system error occurred while setting this timer.</p> <p>Action Check the specific system error code for more information. There may not be enough timer or semaphore handles on your system. If no system error code was given, contact Intermec Technical Support</p>
45	Failure disabling the ACK timeout timer for an application	<p>Problem A system error occurred while disabling a timer for an application ACK timeout. A DosTimerStop instruction was issued.</p> <p>Action In most cases, no action is necessary. If an application is not getting transactions, verify the application is acknowledging data or sending a DcmInter system transaction to the Receive channel during the appropriate time. Check the specific system error code for more information. If the problem persists, shut down and reboot the controller.</p>
47	Error deleting a record from an application temporary file	<p>Problem A system error occurred while removing a record from an application's temporary file. Data stored in the file may not have been properly delivered to an application.</p> <p>Action Verify that the file has not been corrupted. The file has the name of the application channel with a .TMP extension. Check the system error code for more information. This problem should correct itself when a new application's temporary file is created during execution. If the problem persists, delete the file and reboot the controller.</p>
48	Unable to find app id for application acknowledgment in DCM_ACK IPC channel	<p>Problem The ACK channel contains a transaction in which the source application ID field (chSrcApId) in the transaction header was not found in the application table.</p> <p>Action Verify that the source application ID field in the transaction header that was sent from the application is valid and is configured in the GUI.</p>



Error Number	Error Message	Solution
49	Invalid number of bytes in transaction read from DCM_Q IPC channel	<p>Problem A transaction sent to the Receive channel had less than 96 or more than 1120 bytes.</p> <p>Action Do not send transactions through the controller that do not have a proper header of 96 bytes and/or more than 1K (1024 bytes) of data.</p>
50	Error opening a DevCom ACK IPC channel	<p>Problem A system error occurred while opening an internal DevComm ACK channel.</p> <p>Action Check whether the DevComm is running or an invalid DevComm was running when the controller was started. Verify that a message handler is not already running. Check the specific system error for further information. Shut down and reboot the controller.</p>
51	Transaction received by Devcomm was in bad format	<p>Problem The DevComm received a transaction that was not in the proper format.</p> <p>Action Verify that the application that created the transaction formatted it correctly with a 96-byte header and no more than 1024 bytes (1K) of data.</p>
52	The DCMXFERTMP env vbl not found - cannot complete file xfer	<p>Problem The DevComm cannot perform the FileXfer without the DCMXFERTMP environment variable.</p> <p>Action Make sure that the DCMXFERTMP environment variable is set prior to running the controller.</p>
53	Parameter error occurred - could not initialize Devcomm	<p>Problem A call was made to open the communication port, for example COM1, resulting in an error code.</p> <p>Action Verify that no other users or applications have control over the port. Check the system specific return code for more information.</p>
56	The Devcomm name service could not translate the name given.	<p>Problem The DevComm could not interpret either the physical or logical name given.</p> <p>Action Verify the configuration and the setup of your downline devices. If the problem continues, contact Intermec Technical Support.</p>
58	DEV SMA. Transaction received did not have a proper SMA format	<p>Problem The DevComm SMA did not understand the transaction it received.</p> <p>Action Try the operation again. Verify the SMA request format.</p>

Model 200 Controller User's Manual

Error Number	Error Message	Solution
59	DEV SMA. Transaction received was neither a Request or Response msg	Problem The DevComm SMA did not understand the transaction it received. Action Try the operation again. Verify the SMA request format.
60	DEV SMA. The device type specified in the transaction is not recognized	Problem The logical or physical device name given in the DevComm SMA transaction was not recognized. Action Verify the transaction and the configuration and then try the operation again.
61	DEV SMA. Invalid Data for SMA initialization	Problem The DevComm SMA could not initialize. Action Verify that the DevComm is not already running. If the problem persists, contact Intermecc Technical Support.
62	DEV SMA. Device Error	Problem A device error occurred during a DevComm SMA request and the DevComm could not complete the request. Action Determine which device had the error and correct the problem.
63	DEV SMA. Invalid Request	Problem The DevComm SMA did not understand the message received. Action Try the operation again. Verify the SMA request format.
64	DEV SMA. Invalid (request/response) transaction received	Problem The DevComm SMA did not understand the message received. Action Try the operation again. Verify the SMA request format.
65	DEV SMA. Could not match the response data to an issued SMA request	Problem The DevComm SMA did not understand the message received. Action Try the operation again. Verify the SMA request format.
67	DEV SMA. Unable to find Command Table for this device	Problem Internal DevComm SMA error. Action Shut down and reboot the controller. If the error continues, contact Intermecc Technical Support.
68	DEV SMA. Command Set timeout has occurred	Problem The DevComm SMA has timed out a request from the source application specified. The request did not complete successfully. Action Determine cause of failure and then try the operation again.



Error Number	Error Message	Solution
72	DEV SMA. Invalid/Missing data during execution of Request/Response function	<p>Problem The DevComm SMA did not have sufficient data to complete the request.</p> <p>Action Verify the transaction format and data and then try operation again.</p>
73	DEV SMA. "Soft" Protocol response received	<p>Problem The specified error was received from the device, but no data was lost.</p> <p>Action Correct the problem in the device.</p>
74	DEV SMA. "Hard" Protocol response received	<p>Problem The specified error was received from the device and data may have been lost.</p> <p>Action Correct the problem in the device.</p>
81	APPC Error. Allocate Partner Transaction Program Failed	<p>Problem Could not connect to partner computer.</p> <p>Action Refer to the APPC return code for more information.</p>
83	APPC Error. Send Data to Partner Transaction Program Failed	<p>Problem Could not send data to partner transaction program.</p> <p>Action Verify partner transaction program verb flow and check communication between partner computers. Refer to the APPC return code for more information.</p>
84	APPC Error. Data Conversion Error	<p>Problem Could not convert data from ASCII to EBCDIC or EBCDIC to ASCII.</p> <p>Action Check the ACSSVC return codes for more information.</p>
85	APPC Error. Receive Data from Partner Transaction Program Failed	<p>Problem Could not receive data from partner transaction program.</p> <p>Action Verify partner transaction program verb flow and check communication between partner computers. Refer to the APPC return code for more information.</p>
86	APPC Error. Receive Allocate from Partner Transaction Program Failed	<p>Problem Allocation from partner transaction program failed.</p> <p>Action Verify partner transaction program verb flow and check configuration. Refer to the APPC return code for more information.</p>
87	APPC Error. Could not get Send Control From Partner Transaction Program	<p>Problem Could not switch from receive to send state.</p> <p>Action Verify partner transaction program verb flow. Refer to the APPC return code for more information.</p>

Model 200 Controller User's Manual

Error Number	Error Message	Solution
88	APPC Error. Could not Write Acknowledge transaction in DCM_ACK IPC channel	Problem Write to ACK channel failed. The controller may not be running. Action Shut down and reboot the controller.
89	APPC Error. Could not Write DCMINTER to Message handler's DCM_Q IPC channel	Problem Write to Receive channel failed. The controller may not be running. Action Examine return code and then shut down and reboot the controller. Start data collection.
90	APPC Error. Could not Allocate Memory for Temp Data Buffer	Problem Failed to allocate enough memory for proper program operation. Action Shut down and reboot the controller. Contact Intermec Technical Support.
91	APPC Error. Could not Send Error to Partner Transaction Program	Problem Could not send error indicator to partner transaction program. Action Verify partner transaction program verb flow and check communication between partner computers. Refer to the APPC return code for more information.
92	APPC Error. Deallocate Partner Transaction Program Failed	Problem Could not deallocate session correctly. Action Verify partner transaction program verb flow and check communication between partner computers. Refer to the APPC return code for more information.
93	APPC Error. Could not Send Confirmed to Partner Transaction Program	Problem Could not confirm data or allocate. Action Verify partner transaction program verb flow and check communication between partner computers. Refer to the APPC return code for more information.
94	APPC Error. TP_Ended could not complete	Problem Could not end transaction correctly. Action Verify partner transaction program verb flow.
98	APPC Error. Batch File Transfer failed	Problem The batch file transfer NetComm message failed to transfer the file to the partner transaction program. Action Check the rest of the error message and any return codes. It is an error with a BFT file extension. Check other error messages for related problems.



Error Number	Error Message	Solution
108	Error building netcom argument list - configuration argument missing/invalid	<p>Problem Not all arguments were available for a remote application.</p> <p>Action Use Advanced Setup to verify that all arguments are specified for a remote application. The configuration file may be corrupt.</p>
110	Error spawning receive netcom	<p>Problem A system error occurred while creating a detached NetComm process. The message handler is continuing execution.</p> <p>Action Verify that the executable file exists in your directory and check the system error code for more information. Shut down and reboot the controller.</p>
111	Error opening DCMSTOPFILE during Initialization	<p>Problem A system error occurred while opening the start/stop file.</p> <p>Action Verify that DCMSTOP.DAT is a valid text file. Verify the environment variable DCMMAIN is set to a valid path and there is enough disk space available in the location to store the file. Check the specific system error code for more information.</p>
112	Error creating DCMSTOPFILE during DC stop	<p>Problem When the controller is stopped, it saves application program information in the start/stop file DCMSTOP.DAT. A system error occurred while creating this file.</p> <p>Action Verify the environment variable DCMMAIN is set to a valid path and there is enough disk space available in the location to store the file. Check the specific system error code for more information.</p>
113	Error writing to DCMSTOPFILE during DC stop	<p>Problem A system error occurred while writing data to the start/stop file DCMSTOP.DAT.</p> <p>Action Verify there is enough disk space available in the main directory to write to a file. Check the specific system error code for more information.</p>
114	Error closing DCMSTOPFILE during DC stop	<p>Problem A start/stop file DCMSTOP.DAT was created and a system error occurred while closing the file handle. The file may be corrupt or missing. When the controller is rebooted, an application may not receive the last transaction sent.</p> <p>Action Make sure all data was received by the application. The application should transmit a DcmInter transaction upon startup. Check the specific system error code for more information.</p>

Model 200 Controller User's Manual

Error Number	Error Message	Solution
120	Unable to write to a batch-file-transfer file	<p>Problem The message handler process was unable to write to a file that is used to perform a batch file transfer.</p> <p>Action Check the return code for more specific information. Make sure that the disk partition is not full. The BFT file is read by the batch file transfer APPC NetComm after the message handler has transferred the contents of a Hot Standby file to it. The message handler returns the error condition to the requesting APPC NetComm.</p>
121	Unable to close a batch-file-transfer file	<p>Problem The message handler was unable to close a file that is used to perform batch file transfer.</p> <p>Action Check the return code for more specific information. Make sure that the disk partition is not full. The BFT file is read by the batch file transfer APPC NetComm after the message handler has transferred the contents of a Hot Standby file to it. The message handler returns the error condition to the requesting APPC NetComm.</p>
122	Error opening batch-file-transfer file	<p>Problem The message handler could not open/create a file that is used to perform batch file transfer.</p> <p>Action See previous error message. You would not expect this error to occur unless the disk is full or some other process has an existing BFT file open. If you are using the TYPE command to inspect a BFT file when a batch file transfer request comes in, the transfer will fail.</p>
123	Error copying application IPC channel file to batch-file-transfer file	<p>Problem The message handler was unable to copy the contents of a Hot Standby file to a file used for batch file transfer.</p> <p>Action See previous error message. The most likely cause of this error is lack of disk space</p>
131	LAN. Problem reading ACK from named pipe	<p>Problem LAN Send NetComm failed in reading the ACK from the specified named pipe.</p> <p>Action Check the return code for specific information. Restart the remote application.</p>
132	LAN. IPC channel Error	<p>Problem A LAN NetComm had a problem with the specified channel.</p> <p>Action Check the return code for more specific information. Then, shut down and reboot the controller.</p>



Error Number	Error Message	Solution
133	LAN. Semaphore Open Error	<p>Problem A LAN NetComm had a problem opening the specified semaphore.</p> <p>Action Try to restart the remote application. If the problem persists, shut down and reboot the controller. You may also have too many applications running. Check the return code for specific information.</p>
134	LAN. Semaphore Clear Error	<p>Problem A LAN NetComm could not clear the specified semaphore.</p> <p>Action Restart the remote application. If the problem persists, shut down and reboot the controller. Check the return code and other Status Monitor errors for more specific information.</p>
135	LAN. Semaphore Set Error	<p>Problem The Pipe Manager could not set the specified semaphore.</p> <p>Action Restart the remote application. If the problem persists, shut down and reboot the controller. Check the return code and other Status Monitor errors for more information.</p>
136	LAN. Problem writing ACK to DCM_ACK IPC channel	<p>Problem LANSSEND NetComm could not write the ACK message to the ACK channel.</p> <p>Action Check that the controller is running. Shut down and reboot the controller. Check the return code for more specific information.</p>
137	LAN. Could not load LAN application tables.	<p>Problem The Pipe Manager was unable to load the configuration file LAN application tables into memory.</p> <p>Action Check the return code for more information. You may be out of memory—stop other processes and try to shut down reboot the controller. You may be out of file handles. Check your DCMMAXFH environment variable in CONFIG.SYS, increase that value, and then shut down and reboot the controller.</p>
138	LAN. Could not create semaphore arrays.	<p>Problem The Pipe Manager could not create the semaphore arrays to manage the LAN semaphores.</p> <p>Action Check the return code for more information on the problem. Shut down and reboot the controller.</p>

Model 200 Controller User's Manual

Error Number	Error Message	Solution
139	LAN. Could not spawn LAN netcom.	<p>Problem The Pipe Manager could not spawn the specified LAN NetComm.</p> <p>Action Check the return code for specific information. Check that the DCMMAIN environment variable is correct. You may also be out of memory. Shut down and reboot the controller.</p>
140	An unknown app id was found in a transaction sent to the DCM_Q IPC channel	<p>Problem An application sent a transaction with an invalid source or destination ID in the header to the Receive channel. Data in this transaction was not delivered.</p> <p>Action Use the GUI to verify that all applications have been configured properly and the application ID in the transaction header is that of an existing application. If the transaction is a system transaction, no action is taken.</p>
141	A system error occurred disabling an interrupt timeout	<p>Problem A system error occurred while starting a thread that controls shutdown timing. The controller shutdown process may not work properly.</p> <p>Action If the controller shutdown did not operate correctly, stop all controller processes before continuing. Check the specific system error code for more information. This error may be tied to the _beginthread instruction and the use of dynamic link libraries for multithreaded applications.</p>
145	Error spawning a thread	<p>Problem A system error occurred when the message handler attempted to create a thread of execution.</p> <p>Action Check the specific system error code and take the appropriate action.</p>
148	MH message. IPCWait error	<p>Problem The message handler received an error while it was waiting for input on more than one IPC channel.</p> <p>Action Check the system return code and take action based on this information. Contact Intermecc Technical Support.</p>
161	LAN. LAN Server application is already active	<p>Problem The specified remote LAN application tried to connect to the controller, but it is already active.</p> <p>Action Verify that the application is not running on another workstation.</p>



Error Number	Error Message	Solution
163	LAN. Creation of the named pipe failed.	<p>Problem The LAN NetComm could not create the specified named pipe.</p> <p>Action Check the return code for specific information.</p>
164	LAN. Named pipe failed to connect.	<p>Problem The LAN NetComm received a failure when trying to connect the specified named pipe.</p> <p>Action Check the return code for specific information. Restart the remote application.</p>
165	LAN. Named pipe write failure	<p>Problem The LAN NetComm failed when writing to the specified named pipe.</p> <p>Action Check the return code for specific information. Restart the remote application.</p>
166	LAN. Named pipe read failure	<p>Problem The LAN NetComm failed when reading from the specified named pipe.</p> <p>Action Check the return code for specific information. Restart the remote application.</p>
167	LAN. Failed to set the named pipe handle state	<p>Problem The LAN NetComm could not set the state of the named pipe handle. The remote application may have closed the named pipe.</p> <p>Action Check the return code for more specific information. Try restarting the remote application.</p>
168	LAN. Named pipe close failure	<p>Problem The LAN NetComm failed to close the named pipe.</p> <p>Action Check the return code for specific information. This condition is nonfatal as the application is shutting down.</p>
169	LAN. LAN Server application is not currently configured	<p>Problem The remote LAN application specified is not configured in the configuration file currently in use.</p> <p>Action Check that the application is spelled correctly in the GUI. Check that the proper file is being used and is listed in the Status Monitor.</p>
170	LAN. Failed to spawn thread for pipemgr	<p>Problem The controller may be trying to spawn more threads than is allowed by the system.</p> <p>Action The THREADS statement in the CONFIG.SYS file governs the number of concurrent threads that the controller will allow.</p>

Model 200 Controller User's Manual

Error Number	Error Message	Solution
171	APPC. Invalid transaction size received for batch file transfer	<p>Problem The batch file transfer NetComm received a message that was of invalid size.</p> <p>Action Check that the Hot Standby files have not been corrupted.</p>
200	EMCOMM ERROR - Screen description could not be found	<p>Problem The host screen description is not defined in the template for this screen mapping application.</p> <p>Action Check the template and script file and make sure a screen description exists for the specified screen label.</p>
201	EMCOMM ERROR - Field description could not be found	<p>Problem The host screen field description could not be found in the current screen description for this portion of the script.</p> <p>Action Check the template or script file and make sure the current screen's fields are correctly defined.</p>
202	EMCOMM ERROR - Region description could not be found	<p>Problem The region label could not be found in the screen description.</p> <p>Action Check the template or script file and make sure the screen region is correctly defined.</p>
203	EMCOMM ERROR - Field or region description could not be found	<p>Problem The host screen field or region label could not be found in the screen description.</p> <p>Action Check the template or script file and make sure the region or field is correctly defined.</p>
204	EMCOMM ERROR - The tran ID could not be found in the mappings	<p>Problem The transaction ID for the current transaction could not be found in the list of transaction IDs for this application name. An application may have erroneously sent a transaction to this application with a bad transaction ID.</p> <p>Action Check the source of the transaction and correct the problem or use the GUI to add this transaction ID to the configuration file.</p>
205	EMCOMM ERROR - No mapping exists for this tran ID.	<p>Problem The transaction ID for the current transaction does not have any screen mappings configured in the GUI. The script call PUT_MAPPED_TRANS was called with the transaction ID, but no mappings were found.</p> <p>Action Either edit the script so that the PUT_MAPPED_TRANS is not called with this transaction ID, or use the Script Builder to specify a mapping for the transaction.</p>



Error Number	Error Message	Solution
206	EMCOMM WARNING - Data written to the terminal session was truncated	<p>Problem The data transaction written is longer than the field length. The last part of the data field was dropped.</p> <p>Action This error is not fatal. Verify the length of the fields.</p>
207	EMCOMM ERROR - A bad position was specified - cannot write data	<p>Problem The position on the host screen is invalid. The field or region description in the script may not have the correct row and column values.</p> <p>Action Check the host screen and verify the row and column positions of the field or region. Use the Script Builder to correct the script.</p>
208	EMCOMM ERROR - The terminal session is busy - timed out	<p>Problem The EmComm timed out while waiting for the host-busy condition to clear. The timeout value in the script variables may be too short or the host may be hung. If <code>_CRIT_EXIT</code> is included in the script, the EmComm will exit.</p> <p>Action Determine if there is a problem with the host. If you want to increase the timeout period used by the EmComm, use the GUI to edit the configuration.</p>
209	EMCOMM ERROR - The terminal presentation space is not available	<p>Problem The EmComm application cannot find the terminal session indicated by the short session ID. The terminal session is not available.</p> <p>Action Start another session or configure the GUI with a valid screen mapping session ID.</p>
210	EMCOMM ERROR - The data sent to the terminal session was invalid	<p>Problem The data written to the terminal session caused a key lock. The data is probably an invalid type.</p> <p>Action Check the script and make sure that the data was entered in the correct screen. Check the source of the data to ensure that the transactions are formatted correctly.</p>
211	EMCOMM ERROR - The keyboard is locked and could not be cleared	<p>Problem The EmComm has encountered a key lock condition and cannot clear it. This is a fatal error. <code>_CRIT_EXIT</code> will execute if it is in the script.</p> <p>Action The problem is either with the host or with the script. Determine the location of the problem and correct it.</p>

Model 200 Controller User's Manual

Error Number	Error Message	Solution
212	EMCOMM ERROR - The terminal screen is unformatted	Problem The EmComm cannot read from the current cursor position because the host screen is not field- formatted. Action Change the script. You cannot perform a SEND_MESSAGE or FILL_FIELD with CUR_POS specified in a non field-formatted screen.
213	EMCOMM WARNING - A string of length 0 was encountered and was not written	Problem The data field specified to be written was of length 0 and could not be written to the terminal session. This condition is not fatal. Action Use Script Builder to check the script, the mappings, and the source of the transaction.
214	EMCOMM ERROR - The script has a syntax or logical error	Problem The script file is not written correctly and cannot be loaded. Action Run the script checker on the script file to detect syntax errors.
215	EMCOMM ERROR - The template has a syntax error	Problem The template is not written correctly. Action Review the template and make sure screen descriptions are written correctly.
216	EMCOMM ERROR - The call in the script could not be found - syntax error	Problem A call in the script file is not written correctly. Action Review the script file and make sure the script calls are written correctly.
217	EMCOMM ERROR - No script was found in the file	Problem The specified script file does not contain script. Action Review the script file and add script to the file.
218	EMCOMM ERROR - No template was found in the file	Problem The specified template file does not contain a template. Action Verify the template file exists or generate a new template from the menu.
219	EMCOMM ERROR - File error - could not open or read from the file	Problem System error—the file specified could not be opened. Action Check that the file exists and that it is not locked.



Error Number	Error Message	Solution
220	EMCOMM ERROR - The screen description is not correct	Problem A screen description in the script file is not formatted correctly. Action Review the script file and make sure the screen description is correct.
221	EMCOMM ERROR - The region description is not correct	Problem A region description is not formatted correctly in the script file. Action Review the script file and make sure that the regions are described correctly.
222	EMCOMM ERROR - The field description is not correct	Problem A field description is not formatted correctly in the script file. Action Review the script file and make sure that the fields are described correctly.
224	EMCOMM WARNING - The data field from the transaction does not exist	Problem The data field specified in either PUT_MAPPED_TRANS or PUT_TRANS_FIELD does not exist in the current data transaction. This error is not fatal. It may be an error in the mappings, the script call, or in the source of the data transaction. Action Correct the error.
225	EMCOMM ERROR - System error - the terminal session may not be started	Problem A general system error was received from the EHLLAPI. The system may not be available or the terminal session may have terminated. Action Check for errors and correct the problem.
226	EMCOMM ERROR - Terminal Session in MACH CHECK state	Problem The 3270 terminal session is in MACH CHECK state. Action Check with your network administrator to correct the problem.
227	EMCOMM ERROR - Terminal Session - system not available	Problem The host is not available. Action Check with your network administrator to correct the problem.
228	EMCOMM ERROR - Memory Allocation error - not enough memory	Problem There is not enough memory to run the EmComm. Action Check with your network administrator to correct the problem.

Model 200 Controller User's Manual

Error Number	Error Message	Solution
229	EMCOMM ERROR - No match found for script key word - syntax error	Problem A call in the script contains a syntax error. Action Use the script checker to edit the script file to check for misspellings.
230	EMCOMM ERROR - Internal processing error	Problem An unknown error occurred. Action Contact your network administrator.
233	EMCOMM ERROR - A IPC channel error occurred	Problem An error with the specified channel occurred. The system return code is given. Action Determine the problem and correct if necessary.
234	EMCOMM WARNING - The transaction sent has been truncated. It was too long.	Problem A SEND_MESSAGE call had data that was longer than the maximum data transaction size. The data was truncated and sent to the specified destination. Action Correct the problem.
235	EMCOMM ERROR - A parameter on a script call was incorrectly formatted	Problem A parameter on a script call is incorrect and cannot be loaded. Action Run the script checker against the script file to find the syntax error. Correct the parameter.
238	EMCOMM PARAMETER ERROR - Not enough command line parameters	Problem The command to start the EmComm does not have enough parameters. Action Retype the command, making sure you include all the required parameters.
240	Cannot open the trace file for the script file passed	Problem The EmComm is in Trace mode and could not open the trace file for the script file. Action Make sure the file is not locked by another application. Only one trace can be performed on a file at one time.
241	EMCOMM ERROR - There was no mapping for the current screen and tran ID	Problem The current screen description is not in the list of mappings for the transaction ID of the current transaction. The script file or the configuration file may be in error. Action Either use the Script Builder to add mapping for this screen and transaction or check the script file and make sure the correct screen is referenced before the PUT_MAPPED_TRANS call.



Error Number	Error Message	Solution
276	Serio. Port is closed	Problem The given serial port has been closed unexpectedly. Action Shut down and reboot the controller. If the problem persists, contact Intermec Technical Support.
277	Serio. Invalid data bit value	Problem The data bits value for the given serial port is invalid. Action Verify the configuration in the GUI.
278	Serio. Invalid stop bit value	Problem The stop bit value for the given serial port is invalid. Action Verify the configuration in the GUI.
279	Serio. Invalid parity value	Problem The parity value for the given serial port is invalid. Action Verify the configuration in the GUI.
280	Serio. Read serial port timeout.	Problem The DevComm timed out while reading the specified port. The device is not responding to the DevComm within a reasonable amount of time. Action Make sure the device is powered on, connected, and configured correctly. The tuning parameters may need to be adjusted for both receiving and sending data if the device is responding too slowly. Refer to the device's user's manual to change these values.
281	Serio. OS2, Could not set baud rate	Problem The baud rate could not be set for the given serial port. Action Verify the configuration in the GUI.
282	Serio. OS2, line ctrl error	Problem Could not set the line control for the given serial port. Action Verify that the port is a serial port, otherwise contact Intermec Technical Support.
283	Serio. OS2, XON, XOFF error	Problem Could not set XON/XOFF protocol for the given serial port. Action Verify that the port is a serial port, otherwise contact Intermec Technical Support.
284	Serio. OS2, input flush error	Problem Could not set the input flush for the given serial port. Action Verify that the port is a serial port, otherwise contact Intermec Technical Support.

Model 200 Controller User's Manual

Error Number	Error Message	Solution
285	Serio. OS2, output flush error	Problem Could not set the output flush for the given serial port. Action Verify that the port is a serial port, otherwise contact Intermec Technical Support.
289	Serio. Could not write data to serial port	Problem An error occurred writing data to the given serial port. Action Check that no other processes are trying to access that port. Contact Intermec Technical Support.
300	200GUI. No valid configuration file found, start DC terminated	Problem The configuration file for the controller is bad or not found. Action Verify the environment variables are set correctly. Try using another file.
301	200GUI. Status session could not be started, start DC continued	Problem The status session program could not be found or started. Action Verify the environment variables are set correctly and the DCMSTAT.EXE file is in the correct directory.
302	200GUI. .CNF file read failed, DC may not have started properly	Problem An error occurred when the configuration file was read. Action Shut down and reboot the controller. Try starting data collection again. You may have a corrupt configuration file. Restore or recreate the configuration using the GUI.
303	200GUI. Error attempting to reboot controller, try manual shutdown and reboot	Problem An error occurred when you rebooted the controller. Action Shut down the controller and reboot it.
307	200GUI. Mismatch between device and destination tables, start DC terminated	Problem An error occurred when the configuration file was read. Action Corrupt configuration file. You may need to restore or recreate a new configuration file using the GUI.
352	200GUI. Error retrieving remaining free space	Problem Error checking the amount of available disk space. Action Check the environment variables.
353	200GUI. No response to system STATUS transaction	Problem Message handler is not responding to the transaction sent by the controller to get active operational parameters. Action Check if the message handler is running. You may need to stop data collection, shut down, and reboot the controller.



Error Number	Error Message	Solution
354	200GUI. No response to system halt transaction	<p>Problem Message handler is not responding to the transaction sent by the controller to stop data collection.</p> <p>Action Check if the message handler is running. You may need to stop data collection, shut down, and reboot the controller.</p>
355	200GUI. No response to system INTER transaction	<p>Problem Message handler is not responding to the transaction sent by the controller to establish communications.</p> <p>Action Check if the message handler is running. You may need to stop data collection, shut down, and reboot the controller.</p>
356	200GUI. Informational: Starting 200 data collection	No problem. Informational message only.
357	200GUI. Informational: Stopping 200 data collection	No problem. Informational message only.
361	200GUI. Unable to resume interactive communications with Message handler	<p>Problem Message handler is not responding to a transaction sent by the controller to reestablish communications.</p> <p>Action Check if message handler is running. You may need to stop data collection, shut down, and reboot the controller.</p>
364	200GUI. Attempted to create a second CON_IN IPC channel, only one allowed	<p>Problem The controller may already be running since its IPC channel already exists.</p> <p>Action Use the existing IPC channel. Do not create a new one.</p>
401	Invalid # of arguments in current record read from config file.	<p>Problem The configuration file is not properly formatted.</p> <p>Action Do not manually edit the configuration file; use the GUI. If you are using a file that was created by the GUI, contact Intermec Technical Support. You will be asked to send a copy of your configuration file to Intermec.</p>
402	Unable to add structure to config file ram tables.	<p>Problem The configuration file is not properly formatted.</p> <p>Action Do not manually edit the configuration file; use the GUI. If you are using a file that was created by the GUI, contact Intermec Technical Support. You will be asked to send a copy of your configuration file to Intermec.</p>

Model 200 Controller User's Manual

Error Number	Error Message	Solution
450	More data was written to device than allowed - write has failed	<p>Problem The transaction sent to the device exceeds the maximum allowable transaction size.</p> <p>Action Verify the maximum data size that the device you are communicating with can accept and adjust the transaction accordingly.</p>
451	Protocol error occurred	<p>Problem The DevComm received a protocol error while sending or receiving data.</p> <p>Action Verify that the device is on and configured to match the configuration file. If your device is a 9161, try turning on the time append feature. If the problem continues, contact your network administrator or Intermec Technical Support.</p>
452	Could not send data to device - device possibly not active or unavailable	<p>Problem The DevComm could not send data to the device given, but communications are normal.</p> <p>Action There may be a problem with the device such that it cannot receive data. Determine the cause of the problem and correct it. This problem most often occurs when the controller queue for a device address is full.</p>
454	Timeout occurred during data transfer	<p>Problem The DevComm timed out trying to send to or receive data from a device. There may be a problem with the device.</p> <p>Action Determine the source of the problem and correct it. Contact Intermec Technical Support. Tuning parameters may need to be adjusted.</p>
455	More data was received than Devcomm buffer can hold.	<p>Problem More data was received from a device than the DevComm expected.</p> <p>Action Verify that the device is configured correctly and that it is communicating.</p>
489	RC_DIRONLY. Just dir, (not file) input.	<p>Problem DevComm: The given file name was only a directory, not a valid filename.</p> <p>Action Provide a valid filename.</p>
490	RC_BADDIR. Invalid drive / directory path input.	<p>Problem DevComm: The given file path is invalid.</p> <p>Action Provide a valid file path.</p>



Error Number	Error Message	Solution
491	RC_RECORD. Invalid record number.	Problem DevComm: The given record number was invalid. Action Correct the record number reference.
492	RC_NOMORE. No more files from dir search, etc.	Problem DevComm: The directory search is complete and no more files were found. Action Search a different directory.
494	RC_MEM. Out of memory during allocate.	Problem DevComm: Memory allocation errors. Action Shut down the controller and contact your network administrator.
495	RC_INVALID_PARAMETER. Invalid parameter	Problem DevComm: An invalid parameter was given to the DevComm. Action Check the parameter specification and correct the problem.
496	RC_NO_FILES. Cannot open another file - system limits exceeded	Problem The DevComm could not open any more files. The system file handle limit has been exceeded for this DevComm. Action Contact your network administrator. You may have to increase the file handle limit.
497	RC_SYSERROR or RC_SYS Misc system error - check system return code	Problem DevComm: Internal system error. Action Shut down the controller and contact your network administrator.
500	Invalid IPC handle - IPC (50)	Problem DevComm: The IPC handle being used is not valid—the creator of the IPC channel may have closed it. Action Determine why the IPC channel is not available and correct the problem. The creator process may be gone.
501	Invalid IPC name - IPC (51)	Problem DevComm: The IPC name being used to open/create an IPC channel is not valid. Action Verify the IPC name being used is valid. If the IPC name is invalid use a valid name to correct the problem.
503	This IPC channel already exists - cannot recreate - IPC (53)	Problem DevComm: The IPC channel being created already exists. There is probably a DevComm running with this name. Action Shut down the controller. If the other DevComm is still running, contact Intermecc Technical Support.

Model 200 Controller User's Manual

Error Number	Error Message	Solution
504	The IPC channel is full - cannot write more data - IPC (54)	<p>Problem DevComm: The IPC transaction limit has been reached for the IPC channel specified.</p> <p>Action Contact your network administrator. Determine why the IPC channel is overfilling and correct the problem or contact Intermec Technical Support.</p>
505	The IPC channel does not exist - IPC (55)	<p>Problem DevComm: The IPC channel requested does not exist. The creating process is probably not available.</p> <p>Action Determine why the creating process for the specified IPC channel is not creating it.</p>
506	Cannot create the IPC channel - IPC (56)	<p>Problem DevComm: The IPC channel specified could not be created.</p> <p>Action Contact your network administrator. Make sure the IPC channel name is in the service file and system limits have not been exceeded.</p>
511	BAD_FILE_ERROR	<p>Problem DevComm: An internal file I/O error occurred.</p> <p>Action Contact your network administrator and determine source of problem.</p>
512	Cannot create or open the file	<p>Problem DevComm: Cannot create or open the file specified. The file may be locked.</p> <p>Action Determine the file status: if it is locked, unlock it to correct the problem. If the file is unlocked, contact Intermec Technical Support.</p>
513	File access is denied.	<p>Problem DevComm: Access to the specified file has been denied.</p> <p>Action Contact your network administrator and correct the problem.</p>
514	Invalid file handle	Contact Intermec Technical Support to help you solve the problem.
515	The file already exists - cannot recreate	<p>Problem DevComm: The file specified cannot be recreated and will not be overwritten.</p> <p>Action Specify a unique filename. This operation will not overwrite or append to this filename.</p>



Error Number	Error Message	Solution
516	The file does not exist - cannot open	<p>Problem DevComm: The file specified cannot be opened and will not be created.</p> <p>Action Check that the path of the file is correct and that the file exists.</p>
517	Cannot create the file.	<p>Problem DevComm: The filename specified cannot be created.</p> <p>Action Contact your network administrator and determine the source of the problem.</p>
518	Cannot flush the file buffer.	<p>Problem DevComm: System error. Cannot flush the write buffer for the file specified.</p> <p>Action Contact your network administrator to correct the problem.</p>
519	This feature is not supported for this file	<p>Problem DevComm: System error—cannot perform the action on the specified file.</p> <p>Action Contact your network administrator to correct the problem.</p>
520	Invalid file type	<p>Problem DevComm: The file specified has an invalid type.</p> <p>Action Verify the file name and type and correct the problem.</p>
521	Invalid file mode	<p>Problem DevComm: The file specified is in an invalid mode.</p> <p>Action Verify the file name and determine source of problem.</p>
522	Too many files are open - cannot open another	<p>Problem DevComm: Could not open any more files. The system file handle limit has been exceeded for this DevComm.</p> <p>Action Contact your network administrator. You may have to increase the file handle limit.</p>
523	Cannot close file - not open	<p>Problem DevComm: Could not close the specified file.</p> <p>Action Contact your network administrator to determine the source of the problem.</p>
524	File error	<p>Problem DevComm: Undetermined file error occurred on specified file.</p> <p>Action Contact your network administrator to determine the source of the problem.</p>

Model 200 Controller User's Manual

Error Number	Error Message	Solution
677	UPS hardware battery is low. Controller will shutdown immediately.	<p>Problem The UPS battery power is low. It will immediately stop data collection and then shut down the controller.</p> <p>Action Stop sending transactions to the controller. Allow the controller to stop data collection and shut itself down.</p>
710	FileXfer. An error occurred attempting to download a file.	<p>Problem An error occurred trying to download a file to the given device.</p> <p>Action Verify the file content and its location. Correct the problem and try operation again. Look at other messages to determine the source of the problem.</p>
711	FileXfer. Internal error occurred while downloading.	<p>Problem An internal error occurred during a file transfer. This problem may indicate a memory problem or other system level problem.</p> <p>Action Contact your network administrator.</p>
712	FileXfer. Could not initialize the download of a file.	<p>Problem The DevComm could not initialize the file transfer. Possibly the result of an invalid file name or the specified device is already performing another transfer.</p> <p>Action Verify that the file name has a correct full path or relative path. Make sure all other transfers to that device have completed. Try again.</p>
714	The IRL file downloaded did not compile.	<p>Problem IRL file downloaded to the device did not compile correctly.</p> <p>Action Correct the problem and download the file again.</p>
718	A doubly nested CMD file was found. Cannot continue download.	<p>Problem The command file requested for downloading contained a nested command file. You cannot have nested command files.</p> <p>Action Correct the problem.</p>
720	There was an initialization failure for a file transfer.	<p>Problem The DevComm could not initialize the file transfer. Possibly the result of an invalid file name or the specified device is already performing another transfer.</p> <p>Action Verify that the file name has a correct full path or relative path. Make sure all other transfers to that device have completed. Try operation again.</p>



Error Number	Error Message	Solution
722	Internal file transfer error; upload cancelled.	<p>Problem An internal error occurred during a file transfer. This problem may indicate a memory problem or other system level problem.</p> <p>Action Contact your network administrator.</p>
723	FileXfer. Internal file transfer error; download cancelled.	<p>Problem An internal error occurred during a file transfer. This problem may indicate a memory problem or other system level problem.</p> <p>Action Contact your network administrator.</p>

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 controller.

SNA Subsystem Management Helps you troubleshoot the controller by showing you the current status of links, sessions, and transaction programs. You can change the status of many communication processes on the controller and watch the immediate effects of these changes.

Trace Utility Records the information processing through the controller message handler queues during data collection. You can display the trace results and you can save the file.

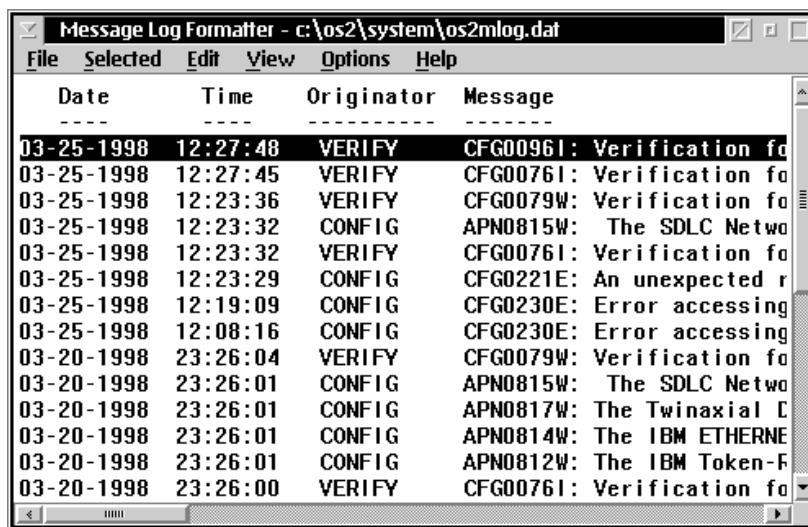
Using the Message Log Formatter

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.



The screenshot shows a window titled "Message Log Formatter - c:\os2\system\os2mlog.dat". The window has a menu bar with "File", "Selected", "Edit", "View", "Options", and "Help". Below the menu bar is a table with four columns: "Date", "Time", "Originator", and "Message". The table contains 15 rows of log entries. The first row is highlighted in black. The entries are as follows:

Date	Time	Originator	Message
03-25-1998	12:27:48	VERIFY	CFG00961: Verification fo
03-25-1998	12:27:45	VERIFY	CFG00761: Verification fo
03-25-1998	12:23:36	VERIFY	CFG0079W: Verification fo
03-25-1998	12:23:32	CONFIG	APN0815W: The SDLC Netwo
03-25-1998	12:23:32	VERIFY	CFG00761: Verification fo
03-25-1998	12:23:29	CONFIG	CFG0221E: An unexpected r
03-25-1998	12:19:09	CONFIG	CFG0230E: Error accessing
03-25-1998	12:08:16	CONFIG	CFG0230E: Error accessing
03-20-1998	23:26:04	VERIFY	CFG0079W: Verification fo
03-20-1998	23:26:01	CONFIG	APN0815W: The SDLC Netwo
03-20-1998	23:26:01	CONFIG	APN0817W: The Twinaxial C
03-20-1998	23:26:01	CONFIG	APN0814W: The IBM ETHERNE
03-20-1998	23:26:01	CONFIG	APN0812W: The IBM Token-F
03-20-1998	23:26:00	VERIFY	CFG00761: Verification fo

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.

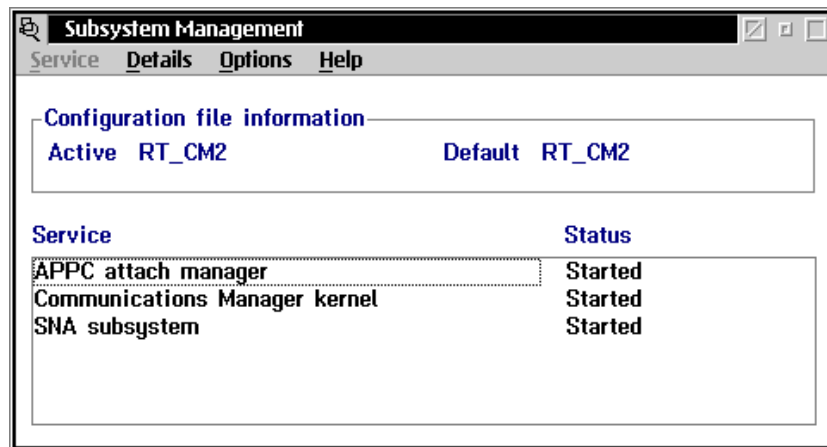


Using SNA Subsystem Management

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 Model 200 Controller.

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

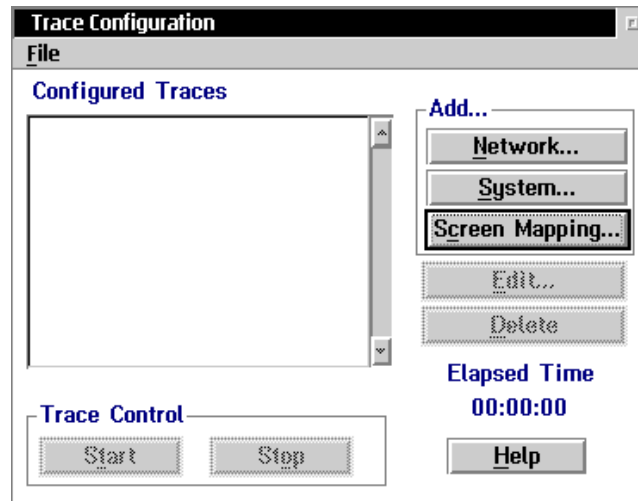
This system diagnostics tool provides you with ways to configure and run traces on the peer-to-peer network connections, downline device communications, and screen mapping sessions. The Trace Utility combines features from IP trace and SNA trace applications that are provided with the IBM PComm product.

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 controller saves all of the traces in the D:\SYSDIAG\TRACEUTL\CURRENT directory.

Note: Each time 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 this window, see the Help menu that is provided by IBM.

To save a trace

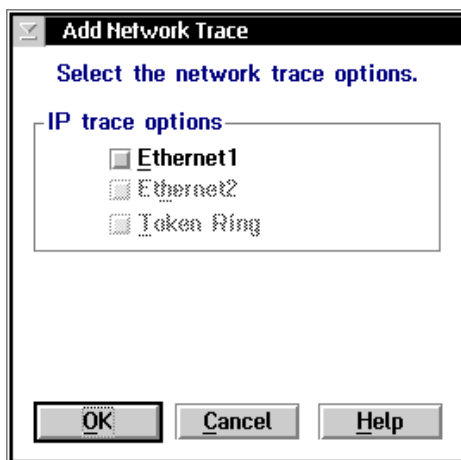
1. From the Trace Configuration dialog box, choose the File menu command.
2. Choose Backup Trace Files. A message box appears instructing you to insert a blank formatted disk in your disk drive.
3. Choose Backup. The trace files are backed up to the disk.

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, enable 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.

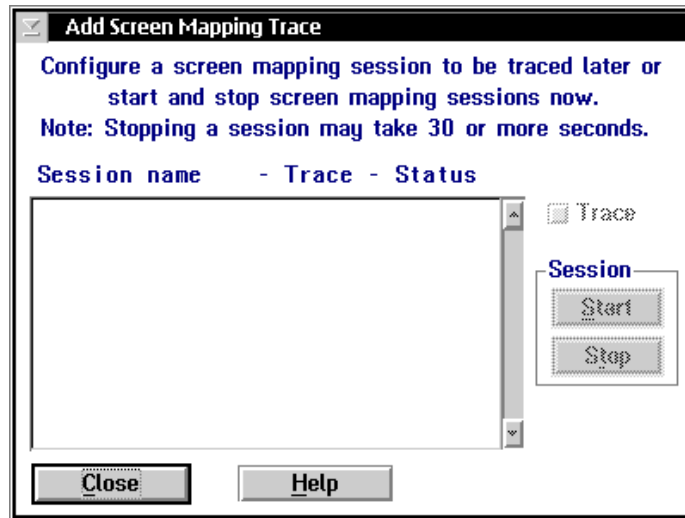


Adding a Screen Mapping Trace

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 OK. The trace appears in the Configured Traces list box.

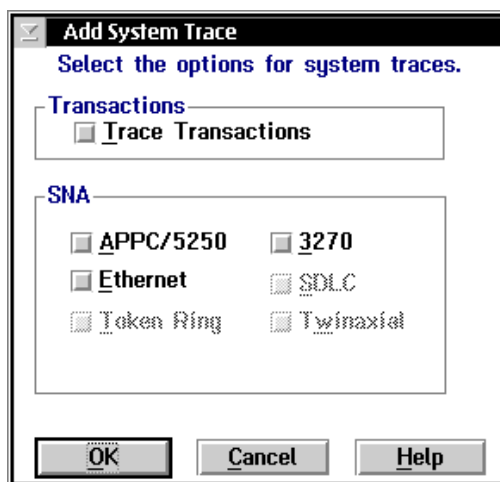
Adding a System Trace

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" in the next section.

The transaction trace file is called TRXTRACE.TXT and it contains up to 10,000 transactions in the order that the controller 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, enable the Trace transactions check box if you want to record transactions.
3. In the SNA box, enable the appropriate SNA traces.
4. Choose OK. The trace appears in the Configured Traces list box.



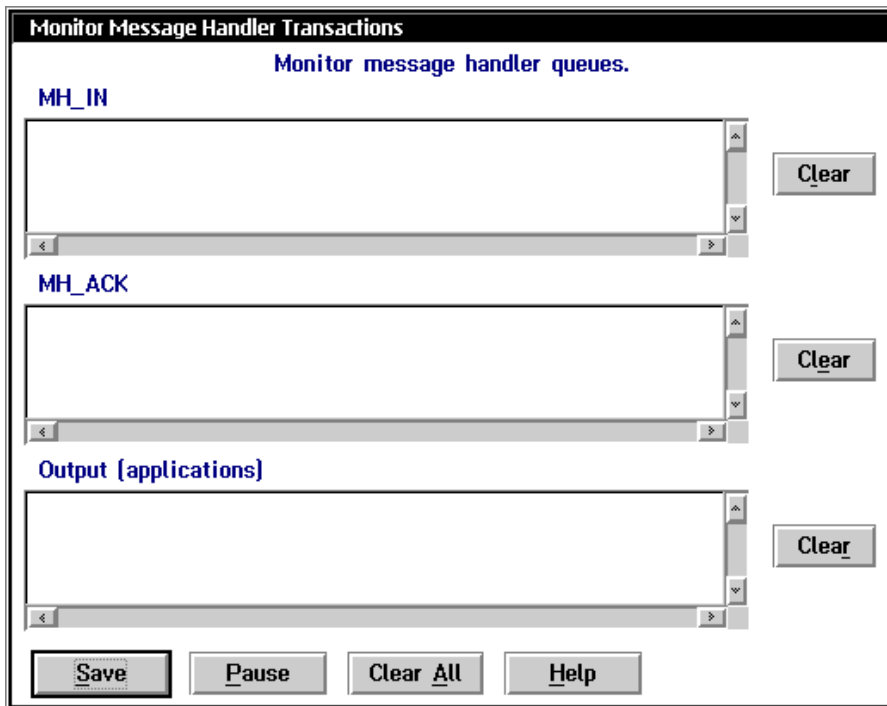
Understanding the Monitor Message Handler Transactions Dialog Box

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. Choose Clear to clear the information in the box.



Model 200 Controller User's Manual

To pause the system trace

- Choose Pause.

To save the system trace

- Choose Save. The results are stored in the D:\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.



Helpful Information

This appendix provides helpful information about system cabling. It also provides procedures for using the controller to verify your network connections, to transfer files, and to configure the TRAKKER Antares terminals.

System Cabling Specifications

This table lists the cables you may use to connect your host and your data collection network with your Model 200 Controller. They also list who supplies the cables and any Intermec part numbers.

From	To	Cable Type	Supplied by	Intermec Part No.
Ethernet card (10 Mbit)	Network	UTP for 10BaseT	Customer	None
		RG-58 coax for 10Base2		
		50-ohm coax for 10Base5		
Ethernet card (100 Mbit)	Network		Customer	None
Token Ring card	Network	RJ-45 to STP	Card vendor	None
Twinaxial card	Network	15 conductor IBM custom	Intermec accessory	589194
Coaxial card	Network	RG-58 coax	Customer	None
SDLC card	Network	25 conductor IBM custom	Customer	None
RF controller card (2-port)	9181 Base Radio Unit	Belden - 1000 ft	Intermec accessory	583326
		cable kit w/clamp	Intermec accessory	055003
RF controller card (4-port)	9181 Base Radio Unit	4-port interface cable	Intermec	063226
		Belden - 1000 ft	Intermec accessory	583326
		cable kit w/clamp	Intermec accessory	055003

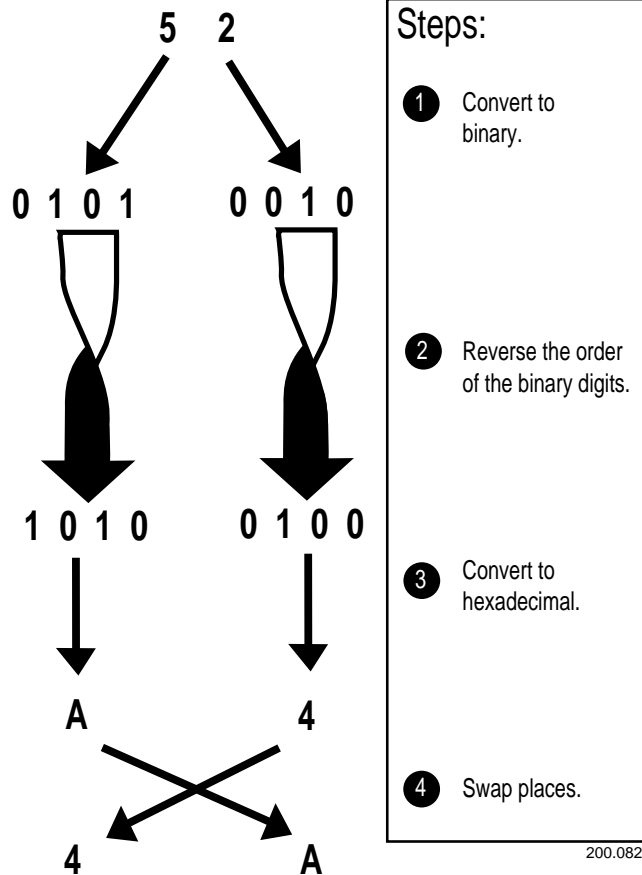
Model 200 Controller User's Manual

System Cabling Specifications (continued)

From	To	Cable Type	Supplied by	Intermec Part No.
Model 200 Controller	External modem	DB-25 to DB-9 modem	Intermec	047287
Model 200 Controller	UPS	STP	Intermec	589157
Model 200 Controller	9180 Network Controller	DB-25 to DB-9 null modem	Intermec accessory	047569
Model 200 Controller	9154 CrossBar Controller	DB-25 to DB-9 null modem	Intermec accessory	047569
Model 200 Controller	9161 Port Concentrator	DB-25 to DB-9 null modem	Intermec accessory	047569

Converting Ethernet Addresses to Token Ring MAC Format

When configuring the AS/400 host on the Model 200 Controller, 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.



Model 200 Controller User's Manual

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 Controller to Verify Your Network Connections

You can use the Model 200 Controller 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 controller to send or receive transactions.

Sending Transactions

Once you configure the Model 200 Controller, you may want to verify that you have a connection between the controller and a data collection device or you may want to verify you have a connection between the controller 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 data collection 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 the Hot Standby Files" in Appendix A.

Send Transaction

Enter a transaction to be sent.

Source ID:

Destination ID:

Transaction ID:

(D)ata or (S)ystem:

Data:

Model 200 Controller User's Manual

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 data collection 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 alphanumeric and special characters	None

To verify your connection

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. Select Send Transaction and then choose Start. The Send Transaction dialog box appears.
5. (Optional) In the Source ID field, enter a name that you want to use as the source of the transaction.
6. If you want to send the transaction to one device, in the Destination ID field enter the logical name of the device that you are using to verify the connection.

Or, if you want to send the transaction to all the devices that are configured to accept it, in the Transaction ID field enter the unique name of the transaction.

7. In the Data or System field, enter D or S. This field defines the transaction to be a data or a system transaction.
8. (Optional) In the Data field, enter any data you want to send with the transaction ID.
9. Choose Send to send the transaction to the device.
10. Choose Close to close the dialog box and return to the System Maintenance dialog box.
11. Choose Close to return to the main menu.

Receiving Transactions

Once you have configured the Model 200 Controller, you may want to test your configuration by sending transactions from a data collection device to an application without starting the application on the host. Or, you may want to send transactions to a data collection device.

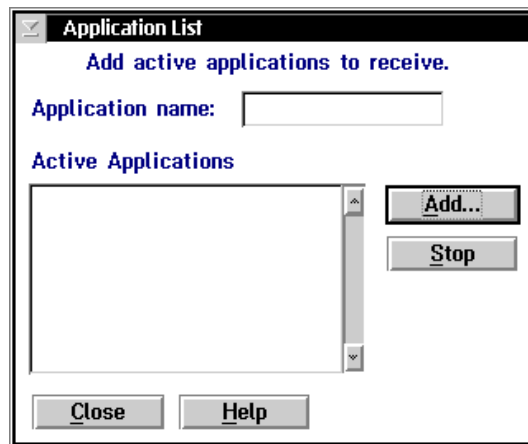
The receive transactions feature can troubleshoot your connection to a destination. It lets the controller emulate the destination, application, or device, without the destination being active. It also displays a list of transactions that the devices or applications sent to the destination.

Note: Any transactions routed to the destination are intercepted by the controller 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.

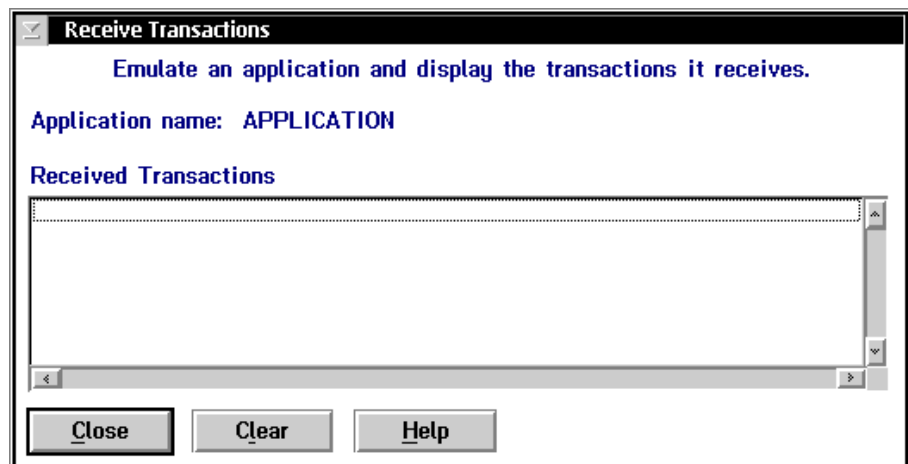
To start the emulator to receive transactions

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.

Model 200 Controller User's Manual



5. In the Application name field, enter the name of a destination. The destination name (application or device) must be defined in the controller.
6. Choose Add. The Receive Transactions dialog box appears and the controller 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.
9. Choose Close to close the dialog box and return to the System Maintenance dialog box.
10. Choose Close to return to the main menu.

Using the Controller to Transfer Files

You can use the Model 200 Controller 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.

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 controller contains the files and data you want to download. You can put files onto the controller 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" in the next section.
4. Start data collection on the controller.
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 chapter.

Limitations when Downloading IRL Programs

Problem When you download an IRL program from the Model 200 Controller, it converts the mnemonic representation of ASCII control characters (0-31) 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 controller converts these characters, the data collection 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 controller will strip off the leading < character and then pass the correct mnemonic representation to the data collection device.

Problem When you download an IRL program from the Model 200 Controller, 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 data collection 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:

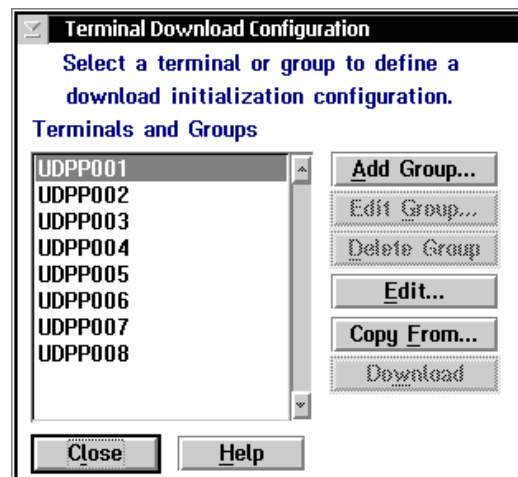
- using PC-IRL to download the IRL program. For help, see the *PC-IRL Reference Manual* (Intermec Part No. 049212).
- using the hex number for the control character. The device translates the hex number after it has parsed all the special characters. Use the previous table to translate the control character 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.

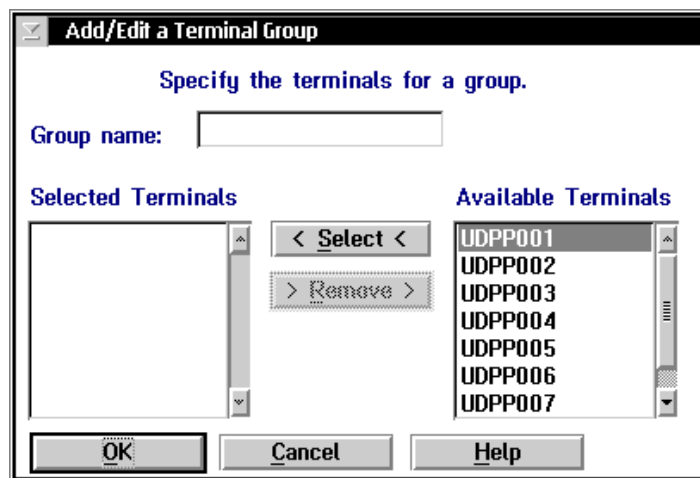
To add a group

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.



Model 200 Controller User's Manual

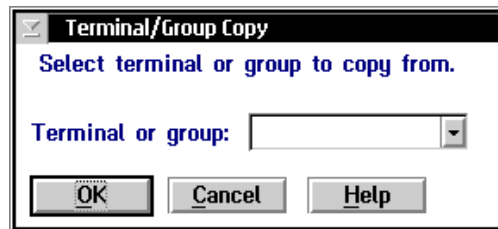
3. Choose Add Group. The Add/Edit a Terminal Group dialog box appears.



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.

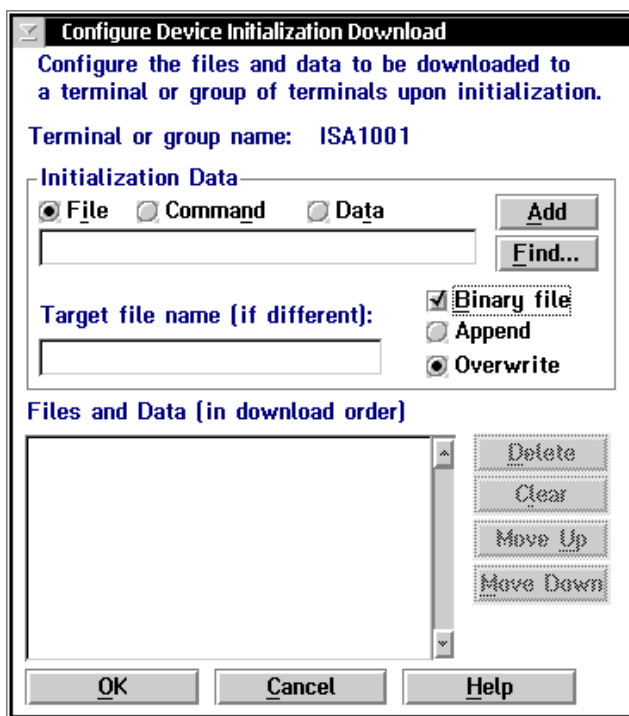


3. In the Terminal or group field, click the down arrow on the right side of the field. A list of terminals or groups that you have configured appears. Select a terminal or group from the list box whose configuration you want to copy.
4. Choose OK to copy the configuration, save your changes, and return 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 controller 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.
9. Choose Close to close the dialog box and return to the System Maintenance dialog box.
10. Choose Close to return to the main menu.

Using Download Server Commands to Transfer Files

This section explains some special commands that you can run on data collection devices or use with the Send Transaction feature on the Model 200 Controller. 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 data collection 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 controller 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 controller sends all the files and data defined for device address pA to pA.
G=group	The controller sends all the files and data defined for the group to all the devices in the group.
F=filename	The controller sends the filename to pA. You can also specify the directory for the file.
D=data	The controller sends the data specified in the command line to pA.
E=errormessage	The controller 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 controller will send the source all files and data that are configured for the source.

7. Choose Send to send the transaction to the controller. The controller performs the download server command.
8. Choose Close to close the dialog box and return to the System Maintenance dialog box.
9. Choose Close to return to the main menu.

Using the Controller to Configure TRAKKER Antares Terminals

You can use the Model 200 Controller 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.

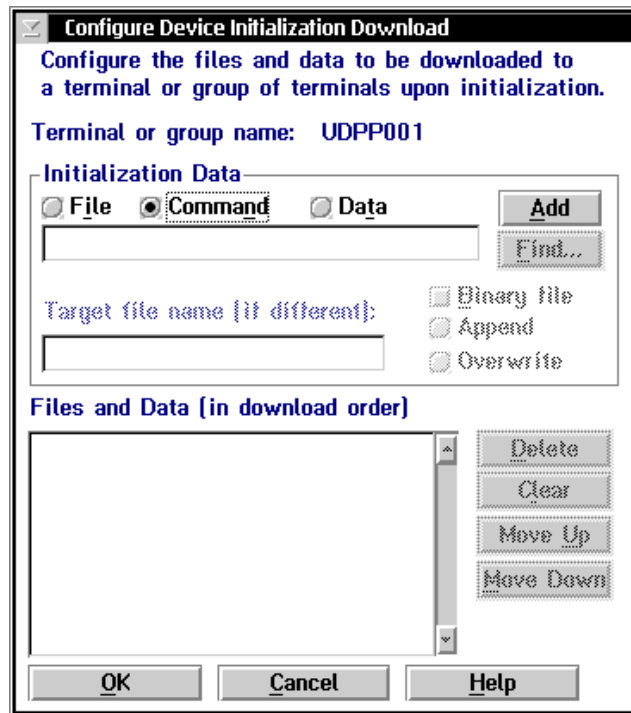
To send configuration commands to a terminal, you need to perform these tasks:

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 chapter.
3. Start data collection on the controller.
4. Download the configuration command to the terminal or group using the download server.

Note: You can continue running an application on the TRAKKER Antares terminal while configuring the terminal from the controller.

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.



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
```

Model 200 Controller User's Manual

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 controller downloads the commands to the terminal or group.
8. Choose Close to close the dialog box and return to the System Maintenance dialog box.
9. Choose Close to return to the main menu.

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.



Using Remote Console



This appendix explains how to use the remote console option on your Model 200 Controller. For help upgrading the controller 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 controller 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 controller to a printer that is connected to the remote PC (OS/2 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 controller. 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 controller. You cannot purchase commercially-available NetOp PC Remote Control software.

Configuring the NetOp Host (Model 200 Controller)

The Model 200 Controller 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.

To configure the NetOp host for TCP/IP or dial-up SLIP

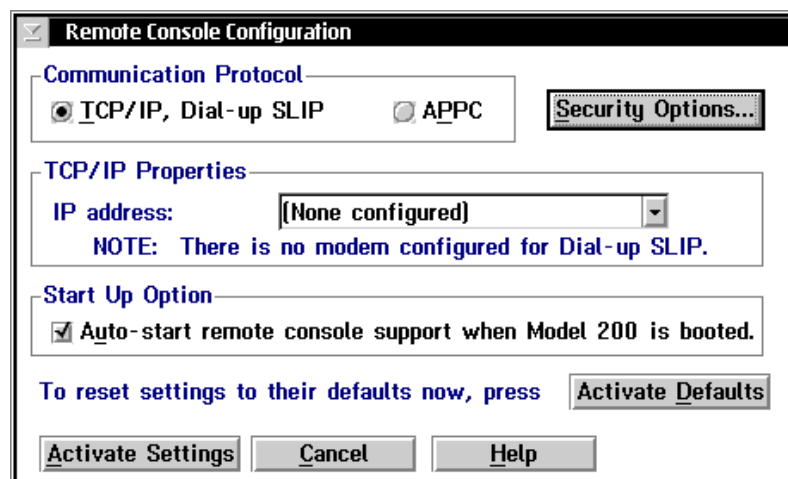
1. From the main menu, choose System Maintenance. The System Maintenance dialog box appears.
2. In the System Maintenance list box, select Remote Console Support and then choose Start. The Remote Console Configuration dialog box appears.
3. In the Communication Protocol box, choose which type of communication protocol you are using to communicate with the NetOp guest software.

For help with TCP/IP or dial-up SLIP, see "Configuring for TCP/IP or Dial-Up SLIP" in the next section.

For help with APPC, see "Configuring for APPC" later in this chapter.

Configuring for TCP/IP or Dial-Up SLIP

If you are using dial-up SLIP, you must connect a modem to the Model 200 Controller. For help, see "Connecting a Modem" in Chapter 2.





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	TCP/IP and Dial-up SLIP
TCP/IP Properties	The IP address field lets you choose which IP address you are using to accept the connection. If you are using dial-up SLIP, choose 222.222.222.10.	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 controller starts the NetOp host software when it is booted.	Check, Clear	Check

To configure for TCP/IP

1. In the TCP/IP Properties box, click the down arrow on the right side of the field. A drop-down list of configured IP addresses appears. Select the IP address of the network adapter card that you want to use to accept the connection.

Or, to accept connections for all available IP addresses, choose All.
2. In the Start-Up Option box, enable or disable the controller from automatically starting remote console when it boots. A check in the check box enables this feature.
3. Configure any security options. For help, see "Configuring Security" later in this chapter.
4. Choose Activate Settings. You can use the new configuration immediately.

To configure for SLIP

1. In the TCP/IP Properties box, click the down arrow on the right side of the field. A drop-down list of configured IP addresses appears. Select 222.222.222.10, which is the SLIP server on the controller.
2. In the Start-Up Option box, enable or disable the controller from automatically starting remote console when it boots. A check in the check box enables this feature.
3. Configure any security options. For help, see "Configuring Security" later in this chapter.
4. Choose Activate Settings. You can use the new configuration immediately.

Configuring for APPC

The screenshot shows a dialog box titled "Remote Console Configuration". It has a checked checkbox in the top-left corner. The dialog is divided into several sections:

- Communication Protocol:** Contains two radio buttons: "TCP/IP, Dial-up SLIP" (unselected) and "APPC" (selected). To the right is a "Security Options..." button.
- APPC Properties:** Contains a text field labeled "Local node name:" with the value "ACCNET" entered.
- Start Up Option:** Contains a checked checkbox labeled "Auto-start remote console support when Model 200 is booted."

At the bottom of the dialog, there is a line of text: "To reset settings to their defaults now, press" followed by an "Activate Defaults" button. Below this are three buttons: "Activate Settings", "Cancel", and "Help".



Field	Description	Value	Default
Communication Protocol	This box lets you specify which communication protocol you are using for remote connections.	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 controller starts the NetOp host software when it is booted.	Check, Clear	Check

To configure the NetOp host for APPC

1. In the APPC Properties box, enter the local node name of the controller.
2. In the Start-Up Option box, enable or disable the controller from automatically starting remote console when it boots. A check in the check box enables this feature.
3. Configure any security options. For help, see "Configuring Security" in the next section.
4. Choose Activate Settings. You can use the new configuration immediately.

Configuring Security

The NetOp host software includes security features to prevent unauthorized access to the Model 200 Controller. You can also use the security options to limit the actions that the remote PC can perform.

The screenshot shows a dialog box titled "Remote Console Security Options" with a checked checkbox in the top-left corner. The dialog contains the following sections:

- Set the security options for remote guests. Access to all these options can be password-protected**
- Allow Remote Client to...**
 - Use keyboard and mouse
 - Chat
 - Send files to controller
 - Receive files from controller
 - Lock controller keyboard and mouse
 - Blank controller screen
- Enable...**
 - Inactivity timeout after: minutes (1-999).
 - Remote guest password:
 - Maximum attempts allowed before hangup: (1-999)
- Access to these Security Options**
 - Requires password:
 - Retype to confirm:

At the bottom of the dialog are three buttons: "OK", "Cancel", and "Help".



Field	Description	Value	Default
Use keyboard and mouse	This check box determines if the remote PC user can control the controller keyboard and mouse. If this check box is clear, the remote PC user can only look at the screen on the controller.	Check, Clear	Check
Chat	This check box determines if the remote PC user can start a chat with the controller user.	Check, Clear	Check
Send files to controller	This check box determines if the remote PC user can transfer files from the remote PC to the controller.	Check, Clear	Check
Receive files from controller	This check box determines if the remote PC user can transfer files from the controller to the remote PC.	Check, Clear	Check
Lock controller keyboard and mouse	This check box determines if the remote PC user can lock the controller keyboard and mouse during a session.	Check, Clear	Clear
Blank controller screen	This check box determines if the remote PC user can blank the controller 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 controller.	Check, Clear	Clear
...minutes	This field specifies how long the controller waits before it ends the NetOp connection if there is no activity between the remote PC and the server.	1 to 999	10

Model 200 Controller User's Manual

Field	Description	Value	Default
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

To configure security

1. In the Remote Console Configuration dialog box, choose Security Options. The Remote Console Security Options dialog box appears.
2. Enable or disable the Use keyboard and mouse check box. A check in the check box indicates that the remote PC user can use the keyboard and mouse to access the controller.
3. Enable or disable the chat feature. A check in the check box indicates that the remote PC user can start a chat session with a controller user.
4. Enable or disable the Send files to controller check box. A check in the check box indicates that the remote PC user can send files to the controller.
5. Enable or disable Receive files from controller check box. A check in the check box indicates that the remote PC user can receive files from the controller.



6. Enable or disable the Lock controller keyboard and mouse check box. A check in the check box indicates that the keyboard and the mouse of the controller are locked when a connection is made. Intermec recommends that you enable this feature.
7. Enable or disable the Blank controller screen check box. A check in the check box indicates that controller screen goes blank when a connection is made.

Note: Screen update is considered an activity.

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 controller.

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 controller.
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.

Model 200 Controller User's Manual

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 controller 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 controller 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 controller.
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 controller.
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 controller 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.

Model 200 Controller User's Manual

Tips for using APPC

1. Use Communication Manager Setup to create a configuration file that defines the partner LU, such as the controller, 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.



Upgrading the Controller and Devices



This appendix provides you with instructions on how to upgrade the Model 200 Controller and how to use the controller to upgrade the TRAKKER Antares terminals.

Upgrading Your Licenses

When you purchased your Model 200 Controller, you selected a license that let 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 128 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 controller.

Level	Network Size (Number of Terminals)
1	1-8
2	1-24
3	1-64
4	1-128

The controller maintains an internal count of the number of devices that connect to it. Every time a new device is sent data, the controller increments its count. If the count reaches the maximum network size, the controller 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 controller, 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.
5. Choose Close to return to the main menu.

Upgrading to Screen Mapping

You can purchase screen mapping with remote console (Part No. 067190) or without remote console (Part No. 066370). Intermec has designed an automated Script Builder Tool that lets you create custom screens and script files for your JANUS devices or TRAKKER Antares terminals. Remote console lets you manage the controller 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.
5. Choose Close to return to the main menu.



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 controller remotely. To run remote console, you also need to purchase the Intermec version of Danware's NetOp® PC Remote Control guest software:

- Remote control software for Windows™ 95 and NT (Intermec Part No. 590480)
- Remote control software for OS/2 (Intermec Part No. 590478)

Note: This guest software contains special software that works with the Model 200 Controller. 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 Support 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.
5. Choose Close to return to the main menu.

Using the Controller to Upgrade TRAKKER Antares Terminals

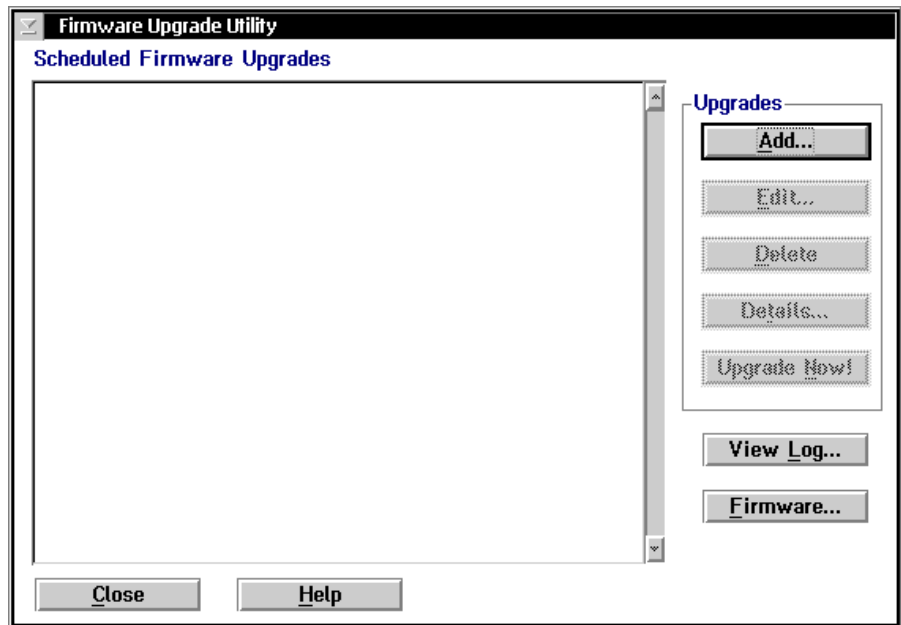
The Firmware Upgrade Utility lets you simultaneously upgrade the firmware on all the TRAKKER Antares terminals that the Model 200 Controller can communicate with. It detects which firmware each terminal is running and performs the correct upgrade procedure for that version. This utility also lets you 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 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 need to determine if the firmware or application is already on the controller or is on a floppy disk that contains the new firmware or application. To see what firmware and applications are on your controller, 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.	Pending

Model 200 Controller User's Manual

Column	Description	Example
3 (cont.)	<p>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 controller at the scheduled time of the upgrade event.</p> <p>Complete The utility successfully performed the upgrade.</p> <p>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.</p>	
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

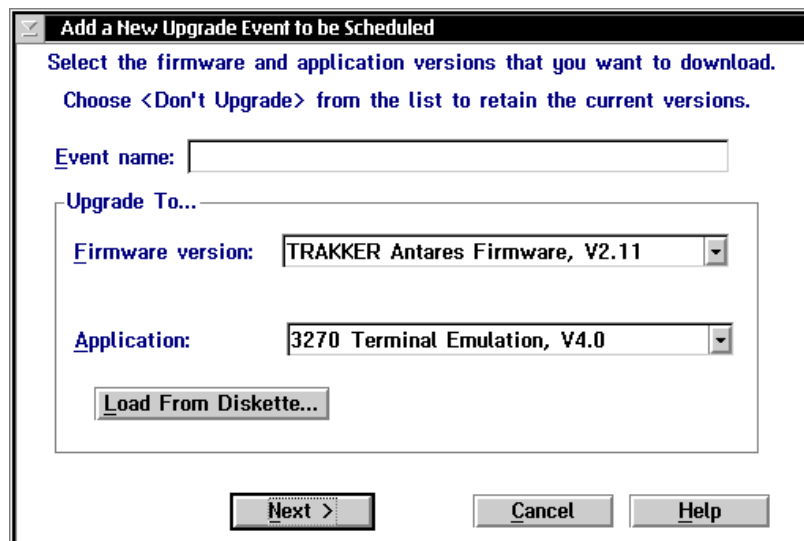
The Firmware Upgrade Utility lets you schedule the upgrade events or you can start the upgrade event immediately.

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 Intermecc representative or a VAR. For help, see “Loading Firmware and Applications From a Disk” later in this appendix.

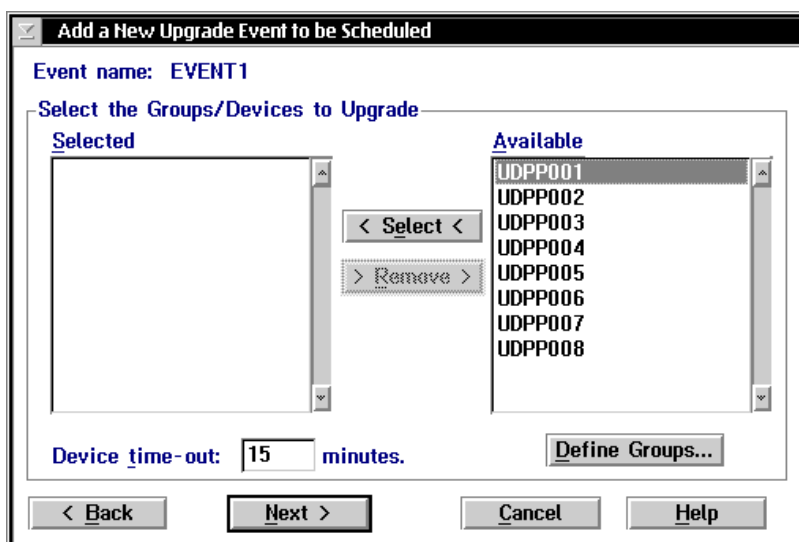
Or, choose <Don’t Upgrade> if you want to keep the current firmware version on your devices.
4. In the Application field, click the down arrow on the right side of the field. A list of applications that you can download appears. Choose one.

Model 200 Controller User's Manual

Or, load the application from a disk that was supplied to you by your local Intermecc 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.



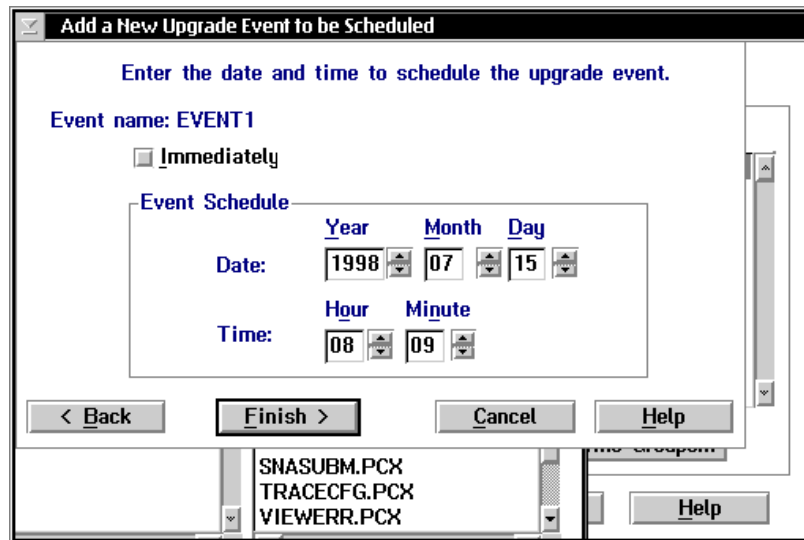
6. Define logical groups of devices. All group names have a G on the right side of the name. For help, see "Defining a Group" later in this appendix.
7. Select the groups and devices that you want to upgrade.

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 Groups/Devices 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 Groups/Devices 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) 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 controller.

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 Model 200 Controller. 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 controller

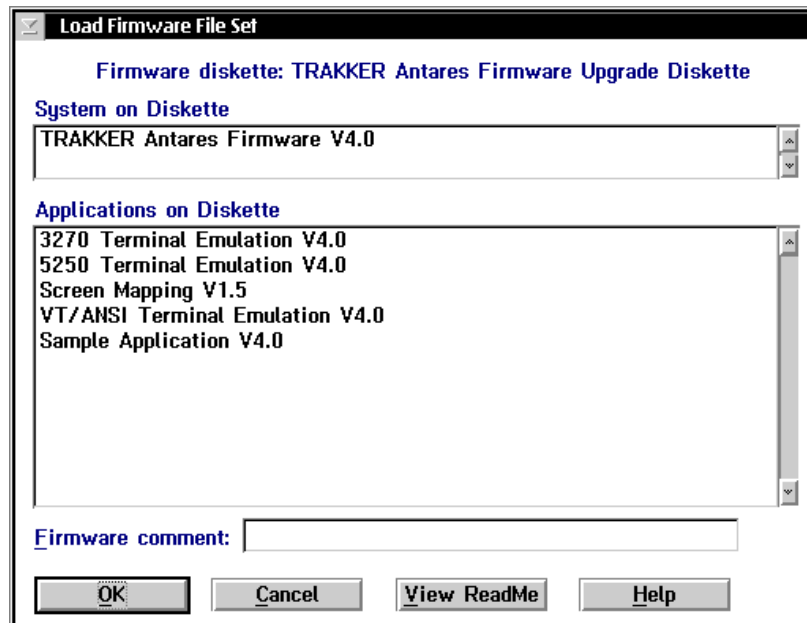
1. From the Firmware Upgrade Utility window, choose Add. The Add a New Upgrade Event to be Scheduled dialog box appears.
2. Choose Load From Diskette. This message box appears.



3. Insert the Firmware Upgrade disk in the disk drive of the controller.
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.



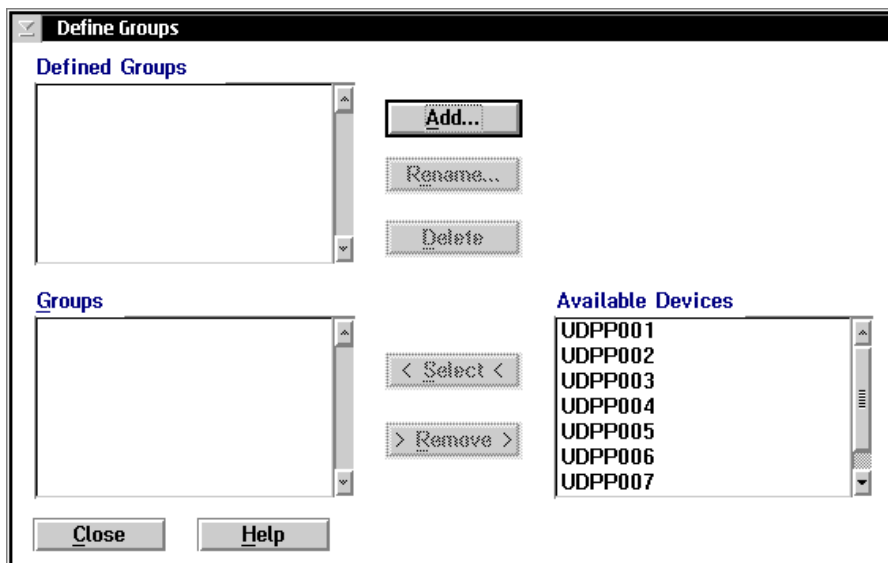
5. In the Firmware comment field, enter any comments you want to be stored with the firmware or application. These comments appear in the Firmware File Set Details message box. You can enter up to 40 alphanumeric characters, special characters, or spaces.
6. Choose View ReadMe if you want to read the 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 controller. Several message boxes appear to show you the status of the loading process.
8. When the utility has copied the files to the controller, a message box appears.
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 controller 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

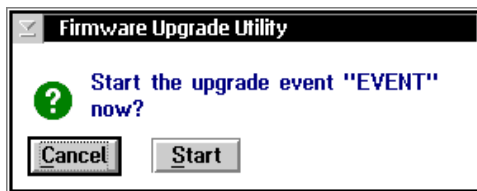
1. From the second Add a New Upgrade Event to be Scheduled dialog box, choose Define Groups. The Define Groups dialog box appears.
2. In the Defined Groups list box, select the group that you want to rename.
3. Choose Rename. The Group Name dialog box appears.
4. In the Group name field, enter the new 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, start data collection on the controller.

- 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 dialog box appears:



Choose Start to start the upgrade event.



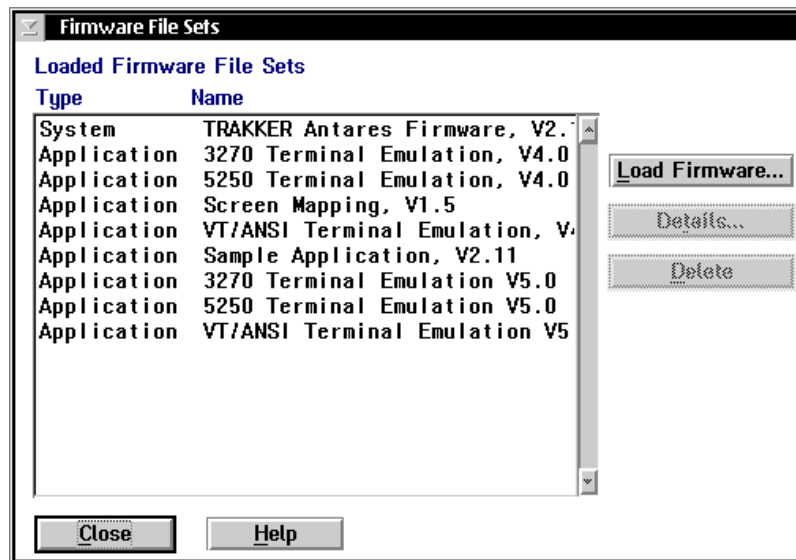
Managing System Firmware and Applications

You can view the firmware and applications that are loaded on your Model 200 Controller. From the Firmware File Sets 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 controller.
- delete firmware or applications that are loaded on the controller.

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.

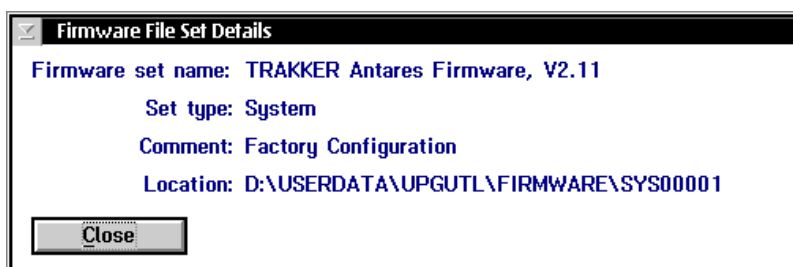


To load firmware or an application from a disk

- 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 dialog box.

To delete firmware and applications from the controller

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 controller.

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.

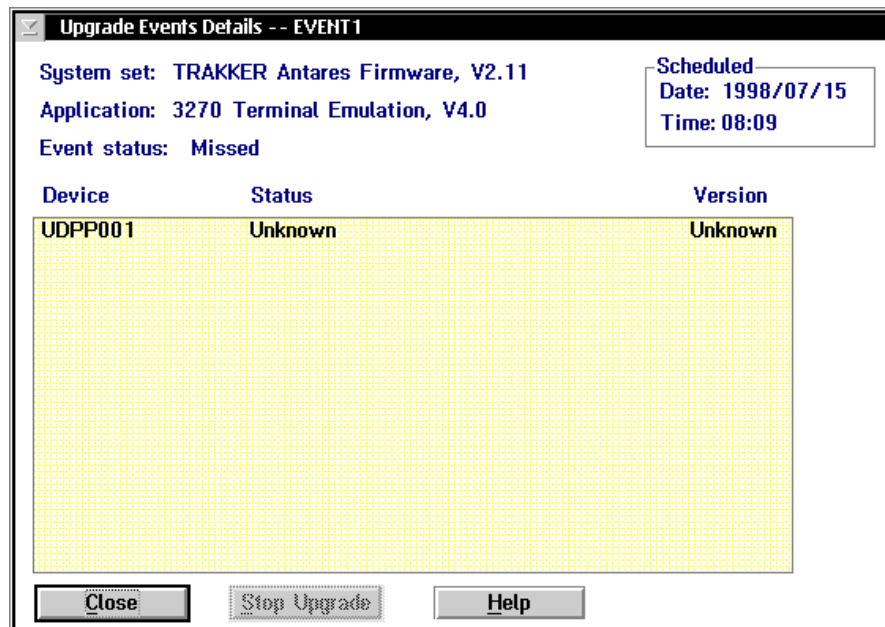
Stop Upgrade button If the status of upgrade on a terminal is Upgrading, you can stop the Model 200 Controller thread that is handling/monitoring the upgrade. For example, if your terminal battery is too low, you can stop the upgrade, change the battery, and restart the upgrade of the terminal.



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.



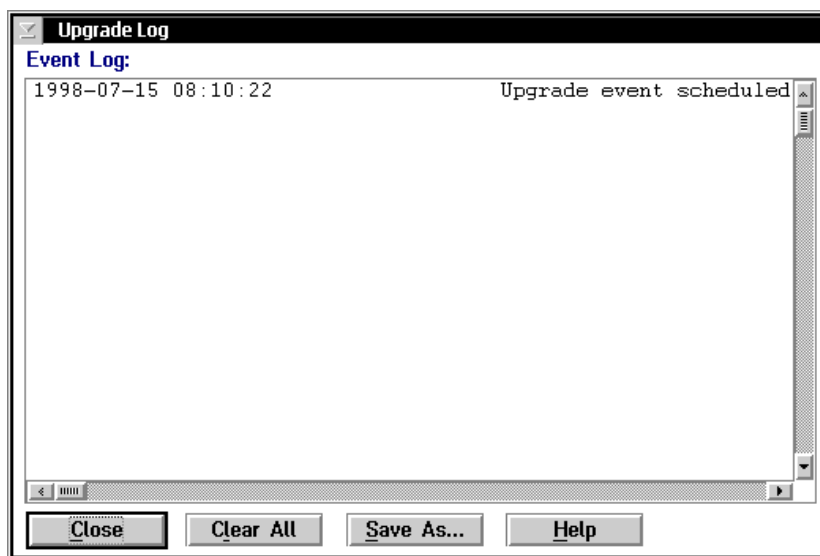
3. If necessary, you can select a device and choose Stop Upgrade to stop the upgrade of that device.
4. Choose Close to close the screen and return to the Firmware Upgrade Utility window.

Viewing the Event Log

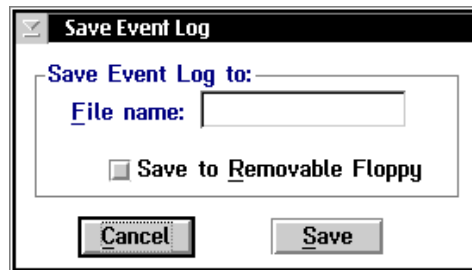
The event log contains the history of all upgrade events. The log is sorted by date and time, with the most recent event listed first.

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.



- 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 controller 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.



Worksheets

This appendix provides worksheets that you need to complete before using Fast Setup to configure your Model 200 Controller. You may need help from your network administrator to obtain this information.

Start Here

Question	Answer	Worksheet Page No.(s)
1. What downline network adapter cards does the controller have?	Ethernet RF controller card 1 RF controller card 2	see Question 5 E-4 E-4
2. Are you using Intermec's UDP Plus network?	Yes No	E-5, E-6 none
3. Are you connecting to a 9180 controller?	Yes No	E-7, E-8 none
4. Are you connecting to Intermec's CrossBar network?	Yes No	E-7, E-9 none
5. What upline network adapter cards does the controller have?	Ethernet Token Ring Coaxial Twinaxial SDLC	E-10 E-10 none E-10 E-10
6. What kind of host communications are you using?	Telnet Terminal Emulation 5250 Terminal Emulation 3270 Terminal Emulation Peer-to-Peer Applications VT/ANSI Screen Mapping 5250 Screen Mapping 3270 Screen Mapping	E-11 E-12, E-13 E-14 - E-17 E-18, E-19 E-20 E-21 - E-23 E-24 - E-26

Model 200 Controller to RF Card Worksheet

Question	Answer
How many 9181 BRUs are you going to connect to the Model 200 Controller (1-8)?	
How many RF controller cards do you need (1-2)?	
What type of RF controller cards do you need (2-port/4-port)?	

RF Controller Card	RFNC address (0-63)	Network ID (1-254)	RF Channel (0-6)	Number of RF Devices to Enable
1 (1-4 BRUs)				
2 (1-4 BRUs)				

Model 200 Controller to TRAKKER Antares Terminals Worksheet

Question	Answer
How many TRAKKER Antares terminals are going to communicate through the Model 200 Controller (1-128)?	
Are you going to use a DNS server to track the IP addresses?	Yes / No

TRAKKER Antares Terminal Logical Name	IP Address (xxx.xxx.xxx.xxx)

Model 200 Controller to JANUS Devices for the 2.4 GHz RF Network Worksheet

Question	Answer
How many JANUS devices for the 2.4 GHz RF network are you going to communicate through the Model 200 Controller (1-128)?	

The controller treats each JANUS device for the 2.4 GHz RF network as a node. Therefore, you need to assign a peer-to-peer destination name to each JANUS device.

JANUS Device for 2.4 GHz RF Network Destination Name

Model 200 Controller to 9180 and CrossBar Worksheet

Device	Question	Answer
9180	Will you be connecting the Model 200 Controller to a 9180 Network Controller? If yes, how many 9180 controllers do you have (1-3)?	Yes / No
9154	Will you be connecting the Model 200 Controller to a 9154 CrossBar controller? If yes, how many 9154 controllers do you have (1-3)? How many data collection devices are connected to each 9154?	Yes / No
9161-01	Will you be connecting the Model 200 Controller to a 9161-01 Port Concentrator? If yes, how many 9161-01s do you have (1-3)? How many data collection devices are connected to each 9161-01?	Yes / No
9161-02	Will you be connecting the Model 200 Controller to a 9161-02 Port Concentrator? If yes, how many 9161-02s do you have (1-3)? How many data collection devices are connected to each 9161-02?	Yes / No

Model 200 Controller to 9180 Worksheet

Using the results from the worksheet on page A-7, choose the COM port that you want to connect to each 9180 Network Controller.

Note: You obtain COM3 by purchasing an optional serial I/O board (Intermec P/N 589167).

9180 v1.x	COM1	COM2	COM3	Number of RF Data Collection Devices to Enable
1				
2				
3				
9180 v2.x	COM1	COM2	COM3	Number of RF Data Collection Devices to Enable
1				
2				
3				

Model 200 Controller to CrossBar Worksheet

Using the results from the worksheet on page A-7, choose the COM port that you want to connect to each external Intermecc controller.

Note: You obtain COM3 by purchasing an optional serial I/O board (Intermec P/N 589167).

9154	COM1	COM2	COM3	Number of Multi-Drop Data Collection Devices to Enable
1				
2				
3				
9161-01	COM1	COM2	COM3	Number of Point-to-Point Data Collection Devices to Enable
1				
2				
3				
9161-02	COM1	COM2	COM3	Number of Multi-Drop or Point-to-Point Devices to Enable
1				
2				
3				

Network Adapter Cards Worksheet

Note: The default setting for the Ethernet card is 10BaseT. Contact your local Intermec representative or VAR if you cannot connect to your Ethernet network because you are using 10Base2 or 10Base5.

Note: No configuration is necessary for a coaxial card.

Ethernet Card (Local Host)	Cable Type (10Base2, 10Base5, 10BaseT)	Host Name (Ethernet Card)	IP Address (xxx.xxx.xxx.xxx)	Subnet Mask (xxx.xxx.xxx.xxx)
1				
2				

Twinaxial Card	Address (0-6)
1	

SDLC Card	Local Station (01-FE)
1	

Telnet Terminal Emulation Worksheet

Host Name	Host IP Address (xxx.xxx.xxx.xxx)

Use the table below if you are explicitly linking terminals to hosts.

Host Name	Terminal Logical Name

5250 Terminal Emulation (Ethernet/Token Ring) Worksheet

Host Name	Network ID	Host LU	Local PU	Address

Use the table below if you are explicitly linking terminals to hosts.

Host Name	Terminal Logical Name

A user ID and a password may be required for logging into the host

User ID	Password

5250 Terminal Emulation (Twinaxial) Worksheet

Host Name	Network ID	Host LU

Use the table below if you are explicitly linking terminals to hosts.

Host Name	Terminal Logical Name

A user ID and a password may be required for logging into the host.

User ID	Password

3270 Terminal Emulation (Ethernet/Token Ring) Worksheet

Host Name	Local PU	Address	Node ID

Host Name	NAU Pool (001-254)

3270 Terminal Emulation (SDLC) Worksheet

Host Name	Network ID	Host LU	Node ID

Host Name	NAU Pool (001-254)



Peer-to-Peer Applications Worksheet (continued)

Transaction ID	Field Number	Field Name

VT/ANSI Terminal Sessions Worksheet

Host Name	Host IP Address (xxx.xxx.xxx.xxx)

Session Name	Terminal Mode	Number of Sessions (1-228)	Host Name (same as above table)	Port Number

5250 Terminal Sessions (Ethernet/Token Ring) Worksheet

Host Name	Network ID	Host LU	Local PU	Address

Session Name	Number of Sessions (1-15)	Host Name (same as above table)	AS/400*	S/36	Mode

*A user ID and a password may be required for logging into the AS/400.

User ID	Password

5250 Terminal Sessions (Twinaxial/SDLC) Worksheet

Host Name	Network ID	Host LU

Session Name	Number of Sessions (1-15)	Host Name (same as above table)	AS/400*	S/36	Mode

*A user ID and a password may be required for logging into the AS/400.

User ID	Password

5250 Terminal Sessions (Coaxial) Worksheet

Host Name

Session Name	Number of Sessions (1-15)	Host Name (same as above table)	AS/400*	S/36	Mode

*A user ID and a password may be required for logging into the AS/400.

User ID	Password

3270 Terminal Sessions (Ethernet/Token Ring) Worksheet

Host Name	Local PU	Address	Node ID

Session Name	Number of Sessions (1-26)	Host Name (same as above table)	NAU Address (1-254)



3270 Terminal Sessions (SDLC) Worksheet

Host Name	Network ID	Host LU	Node ID

Session Name	Number of Sessions (1-26)	Host Name (same as above table)	NAU Address (1-254)

3270 Terminal Sessions (Coaxial) Worksheet

Session Name	Number of Sessions (1-5)	Host Name	NAU Address (1-254)



Glossary

This glossary contains definitions for terms specific to this manual and networking.

10BaseT, 10Base2, or 10Base5

An implementation of Ethernet IEEE standard to describe the primary characteristics of the cabling system. The 10 signifies 10 Mbit/s. Base indicates that the type of signaling used is baseband. The T at the end means that twisted-pair cable is used. The number (2, 5, or 10) at the end indicates the maximum cable length in hundreds of meters.

3270 or 5250 terminal emulation

An application that allows Intermec data collection devices to look like an IBM 3270 or 5250 terminal.

access point

A bridge that allows RF packets to go from the Intermec RF network to an Ethernet or token ring network.

Advanced Setup

The GUI that runs on the Model 200 Controller and allows you to configure the controller. See also Fast Setup.

ANSI terminal emulation

An application that allows Intermec data collection devices to look like an ANSI terminal.

APPC

APPC applications use APPC/LU 6.2 to communicate between the Model 200 Controller and any other machine on an SNA network. APPC applications use APPC/LU 6.2 verbs to communicate with the controller.

bandwidth

The size in hertz of the frequency range that a signal transmission occupies. Typical narrow band signals occupy a 25 KHz bandwidth. The 2.4 GHz radio frequency signal occupies a 1 MHz bandwidth.

Model 200 Controller User's Manual

baseband

A network in which the entire bandwidth of the transmission medium is used by a single digital signal. No modulation techniques are used.

bindery emulation

NetWare 4.0 feature that lets you emulate the bindery database system that was available in all previous versions.

BOOTP (Bootstrap Protocol) server

A device that assigns an IP address in response to a query from an IP node. In this query, the IP node supplies its physical address. The BOOTP server then checks its tables to determine the corresponding IP address.

bridge

An internetworking device that incorporates the first two layers of the OSI model and allows connection of networks or subnetworks with similar architectures.

broadcast

A type of transmission in which a message sent from the host is received by many devices on the system.

BRU (Base Radio Unit)

An Intermec 900 MHz RF device that receives messages from the controller and broadcasts them to Intermec 900 MHz RF data collection devices. The BRU also receives messages sent from devices over the radio waves and sends them to the controller.

channel

The path for transmitting data from a device to the host computer. In RF networks, it is the frequency hopping sequence the card follows. The 2.4 GHz bandwidth can be divided into 15 different channels.

coaxial

A type of cable used to connect the controller directly to an IBM host. Coaxial cable consists of an outer layer of insulation, an outer conductor, another insulating layer, and a central conductor.

CrossBar

Intermec proprietary data collection network consisting of a 9161 port concentrator or a 9154 controller, data collection devices, printers, and input devices.

CSMA/CD (Carrier Sense Multiple Access/Collision Detection)

An Ethernet device using CSMA/CD senses whether or not a channel is in use before attempting to transmit information. If it detects no other carrier, it transmits. If a collision is detected, the device stops transmitting, waits a random length of time, and begins transmitting again.

current screen

The current screen in screen mapping refers to the host screen you are currently defining. You must select a current screen before you can define host screen fields, regions, and messages.

current transaction

The current transaction in screen mapping refers to the transaction for which you are currently defining script. The current transaction may send data to different host screens. You must select a current transaction before you can define host screens, host screen fields, regions, and messages.

data collection device

A device used with a scanner that collects data by scanning bar codes and sending this data to a host computer.

data transmission

An event in which a block of data is transmitted from one device to another.

DevComm (Device Communications Processes)

DevComms are the interface between data collection devices and the controller message handler. DevComms implement all protocols that are required to communicate with the devices.

device

Any physical item that is attached to a computer. A terminal, a printer, a reader, and a controller are all devices.

Model 200 Controller User's Manual

device address

A type of address that is used by the host to identify a particular data collection device. This address can also refer to the device's physical address.

direct sequencing

A radio frequency spread spectrum technique by which the transmitted signal is spread over a particular frequency range.

domain

The area within a LAN that defines a region administered by a controller or server. The domain is also called a subnetwork.

downline

A device that is at the terminal end of a connection to the computer is referred to as being downline. When devices are connected to a computer, they are connected in a "line." Downline is a direction relative to the computer. Contrast with "upline."

If more than one computer is connected in a line, the upline computers usually handle data processing and the downline computers usually handle data collection and sometimes some data "preprocessing."

EmComm (Emulator Communications)

EmComms allow transaction data from a data collection device to be mapped to host applications running in a 3270 or 5250 terminal emulator.

Ethernet

A type of LAN that allows the transmission of computer data, audio data, and video data at 10 Mbit/s across a linear bus topology. Ethernet uses the access method known as Carrier Sense Multiple Access with Collision Detection (CSMA/CD). See IEEE 802.3 standard for the specifications.

Fast Setup

A quick configuration program that runs on the controller GUI. Generally, Fast Setup is used to demonstrate the controller, but you can also use it to configure your network, if it is a simple one.

***field***

An area of a host window to which data can be written.

field-formatted screen

A window on a host such as an AS/400 in which input is restricted to specific areas.

frequency hopping

A spread spectrum technique by which the band is divided into a number of channels and the transmissions hop from channel to channel in a prespecified sequence.

host application

An application running remotely on a host.

host busy

The condition in which the host computer is processing a request and has not responded, or has not updated the screen. On a 3270 terminal, the OIA shows X-SYSTEM, X-CLOCK, or X-[]]. On a 5250 terminal, the OIA shows "II" (Input Inhibited).

host computer

If several computers are connected together on a network, the controlling computer is the host computer. A host computer can be a desktop, laptop, or notebook PC.

HOSTS file

A database that contains a list of remote hosts' IP addresses and their logical names (aliases) that any device on the network can reach.

Hot Standby mode

The mode an application is considered to be in by the Model 200 Controller when the controller sends a transaction to an application, and it does not respond within the time set in the Hot Standby timeout. Whenever a device tries to send this application a transaction, the controller can send the device a Hot Standby message. Until the application becomes active again, any transactions destined for that application are written to a Hot Standby file. When the application becomes active, the controller sends it all the transactions in its Hot Standby file.

Model 200 Controller User's Manual

IP (Internet Protocol)

This is the protocol for the network layer in TCP/IP protocol. It acts as a router for frames and is also responsible for frame addressing. It verifies it has all the frames to pass to the TCP layer and that they are in the correct order.

IP address

An internal TCP/IP protocol stack variable. This address is a network layer address that is assigned to each device in a TCP/IP network.

IPX (Internet Packet eXchange)

This is the protocol for the network layer in SPX/IPX protocol. It provides a way for packets to be exchanged on a network. It acts as a router for messages to other computers, it directs incoming data to the correct local process, and is also in charge of addressing.

Julian format

This date format specifies the date as the elapsed day of the year. For example, January 2 is 002.

LAN (Local Area Network)

A group of intelligent workstations that are hooked together to allow them to share data, printers, and other devices. LANs are usually used over a small geographic area.

link station

A link station exists at the end point of a logical connection. It can send to and receive data from other link stations.

logical unit (LU)

LUs define the name by which devices are known throughout the SNA network. An LU is SNA software that accepts APPC verbs and acts on those verbs. A single LU can provide services for multiple transaction programs. Multiple LUs can be active in a node simultaneously. Intermec uses LU type 6.2 that supports communication between a host application and the controller terminal session manager.

LRC (Logitudinal Redundancy Check)

LRC provides horizontal error checking of data blocks received and transmitted by the controller. LRC performs an exclusive OR of the data bits, excluding the SOM, but including the received or transmitted EOM characters.

LSL (Link Support Layer)

This layer serves as an intermediary between ODI and the link driver that supplies an interface between the network card and the rest of the operating system.

main host screen

The main host screen in screen mapping is the host screen that your startup keystroke sequence brings you to and where all data collection for the script starts. This screen is always the first screen to receive data from a transaction.

NAU (Network Addressable Unit)

A network address that allows a device to communicate with IBM hosts in a 3270 network.

NetComm (Network Communications Processes)

Applications communicate with the controller through network communications processes called NetComms. NetComms are responsible for safely routing data from remote applications across a network to the controller and back.

network

A collection of devices that can store and manipulate electronic data, interconnected in such a way that their users can store, retrieve, and share information with each other.

network administrator

The person who is responsible for the installation, management, and control of a network.

network ID

A number used by a device during channel search to locate the controller's RFNC address.

Model 200 Controller User's Manual

network interface card (NIC)

An adapter card that is installed in the controller that allows it to connect to a network (for example, Ethernet, Token Ring, Twinaxial). The card contains both the hardware to accommodate the cables and the software to use the network's protocols. The NIC is also called a network adapter card.

network node

An end point in a network to which or from which data can be routed. Usually this is a workstation or host computer.

Novell user name

This parameter identifies the user to the Novell software running on a remote host.

operator information area (OIA)

A line on a 3270 or 5250 emulator screen that contains status information (for example, input inhibited, keylock, system available) for a terminal session.

OSI model

Open Systems Interconnection reference model. A framework developed by the International Standards Organization (ISO) to provide worldwide standards for computer communications.

packet

The unit of information that the network uses to communicate. A packet includes a single network message with its associated header, addressing information, data, and optional trailer. A packet can also be called a frame or datagram.

peer-to-peer network

A type of LAN whose workstations are capable of being both clients and servers.

port

The physical place where devices connect to each other for communications purposes.

preferred tree

The tree you specify that you first want to connect to in a NetWare 4.X network if you have multiple trees. If this tree has a server with a free connection, the NetWare DOS Requester attaches to it.

presentation space

The physical space being displayed by the terminal emulator session.

protocol stack

A group of drivers that work together to span the layers in the network protocol hierarchy.

RARP (Reverse Address Resolution Protocol) server

A device that assigns a physical address in response to a query from an IP node. In this query, the IP node supplies its IP address. The RARP server then checks its tables to determine the corresponding physical address.

region

In screen mapping, a particular area on a screen that can be used to display messages and error conditions. Also referred to as the “significant region.”

region message

In screen mapping, a user-defined string that is sent to the source of the transaction when the region is not detected.

repeater

The repeater extends coverage of the RFDC system by functioning as a store-and-forward device for messages.

RFDC system

Radio frequency data collection system, which refers to a data collection system in which the individual components communicate with each other by radio signals.

RFNC address

The radio frequency network controller’s address that is used by the devices to communicate with the BRUs attached to the controller.

Model 200 Controller User's Manual

router

A software and hardware connection between two or more subnetworks that permits traffic to be routed from one network to another on the basis of the intended destinations of that traffic.

screen event

In screen mapping, the operation that is performed on the host screen when data collection starts. There are three types of screen events: mapping data (from a transaction field or a static string) onto a host field, taking actions when a region is detected or not detected, and sending a message to the source of the transaction.

screen mapping

An application that allows you to map data fields from a smaller reader screen to larger 3270 or 5250 screens. This image can be stored in the host, in the controller, or on the local device.

screen message

In screen mapping, a user-defined string that is sent to the source of the transaction after certain screen events.

script file

A file that provides instructions for navigating around host application screens. It also provides instructions for mapping transaction fields from the reader to the host application screens.

serial

A communications scheme in which the bits of a byte are transferred one at a time. Often serial transmission is used to link host computers to terminals and PCs to printers.

server

A computer that is configured to provide services to the network.

session

A single runtime copy of a 3270 or 5250 terminal emulator, through which a host application can be accessed.

session pooling

The controller establishes one 3270 or 5250 terminal session upline to an IBM host. Then, multiple 3270 or 5250 devices downline from the controller can log in to the controller and send data asynchronously to the host. Each device does not need to establish a separate terminal session.

shell out feature

This feature allows you to go to the DOS command line without exiting the installation utility.

SNA (System Network Architecture)

The IBM architecture for supporting computer communications between dissimilar systems.

SNMP (Simple Network Management Protocol)

This protocol was used to manage network activity before the OSI model was approved. This application runs on top of the TCP/IP protocol. It uses management programs called “agents” to monitor network traffic. It stores the information it collects in the Management Information Base (MIB). Your network administrator can use management software interacting with the MIB to obtain information about network activity.

spread spectrum

A radio data transmission modulation technique by which the transmitted signal is spread over a bandwidth wider than the information bandwidth.

SPX (Sequenced Packet eXchange)

This is the protocol for the transport layer in the SPX/IPX protocol. It provides a method for reliable data transfer. SPX makes sure that packets from higher layers are received in order and without error before sending them to IPX for transmission.

store and forward

A method where messages are temporarily stored in the controller before they are transmitted to their destination. It is used when the upline network or host application is temporarily stopped.

Model 200 Controller User's Manual

subnet mask

An internal TCP/IP protocol stack variable. This mask is used in the IP protocol to separate the subnet address from the local IP address. The IP protocol performs a bit-wise AND on the IP address and the subnet mask. Each address segment represents one byte, where 255 converts to FF hex.

For example, if the IP address is 192.009.150.184 and the subnet mask is 255.255.255.0, the subnet address is 192.009.150.

TCP (Transmission Control Protocol)

This is the protocol for the transport layer in the TCP/IP protocol. It provides a method for reliable, error-free, full-duplex communications between sender and receiver nodes. TCP takes long messages from higher layers and breaks them up before passing them to IP for transmission. It makes sure that the messages are in sequence when it receives them and it retries failed transmissions.

template

A file that contains a menu of screens for data collection devices. The template is downloaded to the devices from the Model 200 Controller or the devices can use the reader program to request the template.

terminal emulation (TE)

A data collection device that is running terminal emulation looks like the terminal. For example, the device uses no CPU, no RAM, and no hard disk. Two general classifications are devices running in Character mode and those running in Block mode. Character mode devices emulate VT terminals where a character travels all the way from the host to a device and back. Block mode devices emulate 3270 or 5250 terminals where entire screens are sent to a device, the user fills in all the data fields on the device, and sends the entire screen back to the host.

terminal license

A license that you can purchase from Intermec that determines how many devices you can simultaneously use to communicate with the Model 200 Controller.

terminal session

A terminal session is an active communication link between a device and the host. See also *session pooling*.

terminal template application

An application that runs on the data collection device that requests and runs the templates for 3270 or 5250 screen mapping.

token ring

A type of LAN that transfers data at either 4 or 16 Mbits/s. It is a network transport technology in which a token is passed around a ring topology.

transaction

A transaction is made up of a header and a group of fields. For example, a work order transaction might have a transaction type and three fields consisting of a work order number, part number, and due date.

twinaxial

A type of cable used to connect the controller directly to an IBM host. Twinaxial cables consist of an outer layer of insulation, an outer conductor, another insulating layer, and two side-by-side center conductors.

UDP (User Datagram Protocol)

This protocol is an alternative to TCP. This protocol is the Internet standard for wireless devices. You can use UDP when you do not need a guaranteed delivery. You can also use UDP when you do not require all the services of TCP.

UDP Plus

This Intermec-designed protocol is based on UDP. UDP Plus improves the performance of devices in a mobile wireless environment. Intermec uses this protocol to communicate between the controller and TRAKKER Antares terminals.

UNIX user name

This parameter is a variable in the DOS environment. The UNIX user name identifies the user to the Novell software running on a remote host.

upline

A device that is at the computer end of a connection between a computer and a device is referred to as being upline. When devices are connected to a computer, they are connected in a "line." Upline is a direction relative to the device, in contrast to "downline."

Model 200 Controller User's Manual

If more than one computer is connected in a line, the upline computers usually handle data processing and the downline computers usually handle data collection and sometimes some data "preprocessing."

VT terminal emulation

An application that allows Intermec data collection devices to look like a VT100, VT220, or VT320 terminal.



Index

Symbols and Numbers

- #ACCNET mode, 8-18, 9-5
- #INTER mode, 8-18
- \$IPT transaction ID, 9-23, 9-26
- 10BaseT, 10Base2, or 10Base5, definition, G-3
- 3270 NAU Pool dialog box, 8-28
 - New NAU field, 8-28
 - Unlinked NAUs pool, 8-28
- 3270 screen mapping, Data response timeout field, 11-25
- 3270 SNA terminal emulation, 1-4, 8-6
 - definition, G-3
 - hot key for JANUS devices, 8-35
 - setting host parameters, 8-22
 - setting up, 8-22
- 3270 Terminal Emulation Configuration dialog box, 8-23
 - Available Terminals list box, 8-23
 - Host Name - Linked Terminal - NAU list box, 8-23
 - Host Name list box, 8-23
- 3270 terminal emulation worksheet, E-14, E-16
- 3270 terminal session
 - adding, 10-21
 - setting Ethernet host parameters, 10-5
 - setting SDLC host parameters, 10-6
 - setting up, 10-6
- 3270 terminal sessions worksheet, E-24, E-25, E-26
- 3270 terminals, mapping keyboard to controller keyboard, 10-30
- 5250 screen mapping, Data response timeout field, 11-25
- 5250 SNA terminal emulation, 1-4, 8-6
 - definition, G-3
 - hot key for JANUS devices, 8-35
 - setting host parameters, 8-12
 - setting up, 8-12
- 5250 Terminal Emulation Configuration dialog box, 8-13
 - Available Terminals list box, 8-13
 - Host Name - Linked Terminals list box, 8-13
 - Host Name list box, 8-13
 - Use device names check box, 8-12, 8-13
- 5250 Terminal Emulation Mode dialog box, 8-19
 - #ACCNET mode, 8-18
 - IBM mode, 8-18
- 5250 Terminal Emulation Security dialog box, 8-20
 - Host user ID field, 8-20
 - Password field, 8-20
- 5250 terminal emulation worksheet, E-12, E-13
- 5250 terminal session
 - adding, 10-15
 - setting SDLC host parameters, 10-5
 - setting up, 10-6
- 5250 terminal sessions worksheet, E-21, E-22, E-23
- 5250 terminals, mapping keyboard to controller keyboard, 10-29
- 900 MHz RF network, 1-4
 - configuring JANUS devices, 8-30, 11-109
 - connecting to, 3-4
 - figure, 3-5
- 9154 controller, adding, 4-7
- 9161 controller
 - adding, 4-10
 - configuring, 4-18
 - using internal DIP switches, 4-18
- 9180 and CrossBar to Model 200 Controller worksheet, E-7
- 9180 controller, 1-4
 - adding, 4-13
 - connecting to, 3-4, 4-3
- 9180 to Model 200 Controller worksheet, E-8

A

- Able to receive data check box, 3-17, 3-34, 4-21
- abnormal logoff sequence, 11-26
 - creating, 11-31
- Abnormal Logoff Sequence dialog box, 11-32
 - Captured Keystrokes box, 11-32
 - Start button, 11-32
 - Stop button, 11-32
- AC in, 1-10, 2-4, 2-9
- AC out, 1-10
- access points
 - communicating with JANUS devices, 3-19

Model 200 Controller User's Manual

- access points (*continued*)
 - communicating with TRAKKER Antares terminals, 3-19
 - communicating with UDP Plus terminals, 3-19
 - definition, G-3
- accessing a command prompt, 2-26
- accessing the TE Configuration menu, 8-43
 - on JANUS devices, 8-35
- accessories
 - modem, 2-11
 - monitor, 2-7
 - uninterruptable power supply, 2-8
- ACK channel, 1-15, 9-22
- ACK transaction, 1-15, 9-18, 9-20
- ACK_MESSAGE command, 11-103
- Acknowledgment Delay box
 - Lower limit field, 3-23
 - Upper limit field, 3-23
- Acknowledgment delay field, 3-9
- Activate button, 2-24
- Activate Configuration message box, 8-29, 9-15, 10-25
- Activate Defaults button, C-3
- activating your run-time configuration, 8-29, 9-15, 10-25, 11-83, 11-103
- active application, 1-31
- active configuration, 2-17
- Active Recovery mode, 1-33
- adapter card
 - coaxial, 6-5
 - Ethernet, 5-6, 5-16
 - SDLC, 7-5
 - token ring, 5-6, 5-16
 - twinaxial, 6-6
- Adapter card field, 8-16, 8-26, 10-18, 10-24
- Add a Downline Connection Point dialog box
 - Downline Connections list box, 3-22
- Add a Downline Connection Point dialog box, 3-7, 3-22, 4-5
 - Downline Connections list box, 3-7
- Add a New Upgrade Event to be Scheduled dialog box, D-9
 - Application field, D-9
 - Available Groups/Devices list box, D-10
 - Define Groups button, D-14, D-16
 - Device time-out field, D-11
 - Event name field, D-9
 - Event Schedule box, D-11
 - Firmware version field, D-9
 - Immediately check box, D-11, D-16
 - Load From Diskette button, D-12
 - Selected Groups/Devices list box, D-11
- Add After button, 11-68
- Add button, 1-14
- Add Network Trace dialog box, A-64
 - IP Trace Options box, A-64
- Add Screen Mapping dialog box, A-65
- Add Screen Mapping Trace dialog box
 - Session box, A-65
 - Session Name - Trace - Status list box, A-65
 - Trace check box, A-65
- Add System Trace dialog box, A-66
 - SNA box, A-66
 - Transactions box, A-66
- Add/Edit a Terminal Group dialog box, B-14
 - Available Terminals list box, B-14
 - Group name field, B-14
 - Selected Terminals list box, B-14
- adding a 3270 terminal session, 10-21
- adding a 5250 terminal session, 10-15
- adding a controller, 4-5, 4-7, 4-10, 4-13
- adding a destination, 9-8
- adding a group in the download server, B-13
- adding a host screen, 11-63
- adding a host screen field, 11-40
- adding a menu, 11-101
- adding a message, 11-55
- adding a network trace, A-64
- adding a region, 11-44
- adding a screen mapping field placement entry, 11-82
- adding a screen mapping session, 11-77
- adding a screen mapping trace, A-65
- adding a system trace, A-66
- adding a TCP/IP host, 8-10, 10-10
- adding a terminal field, 11-89
- adding a terminal screen, 11-87
- adding a transaction, 9-13
- adding a transaction field, 9-14

- adding a user block, 11-68
- adding a VT/ANSI terminal session, 10-8
- adding an IBM SNA host, 10-18, 10-23
- adding an SNA host, 8-15, 8-25
- adding upgrade events, D-8
- address family, 9-17
- Address field, 8-16, 8-26, 10-19, 10-24
- Advanced Protocol Configuration dialog box, 5-7, 5-16
 - Ring speed option buttons, 5-8, 5-17
- Advanced SDLC Adapter Protocol
 - Configuration dialog box, 7-6
 - Line mode option buttons, 7-6
 - Line type option buttons, 7-6
 - Link station role field, 7-6
 - Max I-field size field, 7-7
 - NRZI option buttons, 7-6
 - Send XID response immediately check box, 7-7
- Advanced Setup, 1-4, 1-12
 - definition, G-3
- ANSI terminal emulation, definition, G-3
- ANSI terminals, mapping keyboard to controller keyboard, 10-28
- Any string within option button, 11-46
- API, figure, 9-21
- APPC
 - using with remote console, C-6
- APPC applications
 - batch, 9-29
 - interactive, 9-29
 - linking to controller NetComm, 9-30
 - LU name, 9-5
 - MAC address, 9-5
 - mode name, 9-5
 - network ID, 9-5
 - receive, 9-28
 - Receive transaction program, 9-5
 - send, 9-28
 - Send transaction program, 9-5
 - setting host parameters, 9-5
- APPC Properties box, C-7
- APPC verbs, 9-29
- APPC, definition, G-3
- Append box, Append enabled check box, 3-29
- Append enabled check box, 3-13, 3-29, 4-17
- append parameters, 3-11, 3-28, 4-16
- Append Parameters box
 - Append enabled check box, 3-13, 4-17
 - Delimiter field, 3-13, 3-30
 - Include Day check box, 3-13, 3-30
 - Include Month check box, 3-13, 3-30
 - Include Seconds check box, 3-13, 3-30, 4-17
 - Include Year check box, 3-13, 3-29
 - Interval field, 4-17
 - Julian date check box, 3-13, 3-30
 - Record day rollover check box, 4-17
- Application field, D-9
 - Don't Upgrade option, D-10
- Application List dialog box, B-9
- application status, 1-30
 - active, 1-31
 - controller shutdown, 1-30
- applications
 - IMS, 9-30
 - nonactive, 1-31
 - peer-to-peer, 9-4
 - programming interface figure, 9-21
 - routing transactions, 1-18
 - sending unsolicited data, 9-20
 - status, 1-30
 - understanding TCP/IP, 9-16
- Applications on Diskette box, D-12
- AS/400, performing a double pass-through, 8-21
- ASCII files, using the controller to send, B-11
- Attribute field, 11-92
- AUDIT command, 11-103
- Audit Options box, 11-23
- Auto Calc button, 5-16, 5-18
- Auto send check box, 11-88
- Auto-insert from device field, 3-18, 3-34, 4-22
- auto-login
 - using on JANUS devices, 8-37, 8-38
 - using on TRAKKER Antares terminals, 8-45
- Auto-Start box, 2-15
- AUX_Q, 1-29, 9-22
- auxiliary channel, *See* AUX_Q
- Available Devices list box, D-15

Model 200 Controller User's Manual

- Available Files list box, 2-22
- Available Groups/Devices list box, D-10
- Available list box, 9-9, 11-34, 11-78
- Available Ports list box, 2-9, 2-12
- Available Screens list box, 11-62
- Available Terminals list box, 8-8, 8-13, 8-23, B-14
- Available Transactions list box, 11-20

B

- backing up runtime configuration, 2-18
- backing up system files, 2-18
- backing up the controller, 2-18
- backing up user files, 2-19
- Backup Files button, 2-18, 2-20
- backup power, *See* uninterruptable power supply
- Backup System Files message box, 2-18
- Backup System Files option, 2-18
- Backup User Files dialog box, 2-19
 - Backup Files button, 2-20
 - root directory list box, 2-19
 - Selected Files list box, 2-20
- Backup User Files option, 2-19
- Bad ID response field, 1-32, 2-15
- bandwidth, definition, G-3
- Base logical name field, 3-26
- base radio unit, *See* BRU
- baseband, definition, G-4
- batch applications, 9-29
- batch flag, 1-33
- Baud rate field, 4-7, 4-10, 4-13
- binary files, using the controller to send, B-11
- bindery emulation, definition, G-4
- Blank controller screen check box, C-9
- BOOTP server, definition, G-4
- bootstrap protocol server, *See* BOOTP server
- bridge, definition, G-4
- Broadcast enabled check box, 3-12, 3-29, 4-17
- broadcast parameters, 3-11, 3-28, 4-15
- Broadcast Parameters box
 - Broadcast enabled check box, 3-12, 3-29, 4-17
 - Include Date check box, 3-12, 4-17
 - Include Seconds check box, 3-12, 4-17
 - Interval field, 3-13, 3-29, 4-17

- Postamble box, 3-13
- Postamble field, 4-17
- Preamble field, 3-13, 4-17
- Time format option buttons, 3-13, 4-17

broadcast, definition, G-4

BRU

- adding to controller, 3-7
- connecting to the controller, 3-4
- definition, G-4
- using with JANUS devices, 3-14

BRU Parameters box, 3-6

- BRU Status check box, 3-9
- Channel - Frequency field, 3-9
- Repeat count field, 3-9

BRU Status check box, 3-9

Build Menu List dialog box, 11-100

Build Screen List dialog box, 11-86, 11-96

building menus, 11-100

buttons

- Add, 1-14
- Cancel, 1-14
- Close, 1-14
- Delete, 1-14
- description, 1-14
- dialog box, 1-14
- Edit, 1-14
- Help, 1-14
- Hide at Boot Time, 1-11
- OK, 1-14
- Show at Boot Time, 1-11
- using, 1-13

C

- cabling, B-3
- Cancel button, 1-14
- Cancel processing screen events option button, 11-47
- Capture button, 11-48, 11-50
- Capture Keystrokes dialog box, 11-50
 - Start button, 11-50
 - Stop button, 11-50
- CAPTURE_POS command, 11-103
- captured keystrokes
 - editing, 11-33

- Captured Keystrokes box, 11-28, 11-30, 11-32, 11-37, 11-51
- capturing keystrokes, 11-26, 11-50
- Card number field, 3-8
- carrier sense multiple access/collision avoidance, *See* CSMA/CD
- Change Name button, 11-20
- changing the order of screen events, 11-59
- changing the security for the TE Configuration menu, 8-48
- Channel - Frequency field, 3-9
- channel, definition, G-4
- chapter checklist, 1-3, 2-3, 3-3, 4-3, 5-3, 6-3, 7-3, 8-3, 9-3, 10-3, 11-3, 11-4
- Chat check box, C-9
- checking a script file, 11-70
- Clear All button, A-8
- Clear button, A-8, A-67
- clearing the Hot Standby files, A-7
- clearing the IP address and subnet mask, 5-12
- Close button, 1-14
- coaxial
 - cable, 6-4
 - configuring network adapter card, 6-5
 - definition, G-4
 - installing the controller, 6-4
- Collapse All button, 11-70
- Column field, 11-40, 11-46, 11-63, 11-91
- COM ports, 1-10, 2-9, 2-11
- command prompt
 - accessing, 2-26
 - password, 2-26
- Command Prompt Password dialog box, 2-26
 - Password field, 2-26
- communicating with APPC applications, 9-28
- communicating with TCP/IP applications, 9-16
- Communication Parameters box, 3-6, 4-6
 - Acknowledgment delay field, 3-9
 - Baud rate field, 4-7, 4-10, 4-13
 - Card number field, 3-8
 - Data bits option buttons, 4-7, 4-10, 4-13
 - LRC enabled check box, 4-7, 4-10, 4-13
 - Network ID field, 3-8
 - Parity option buttons, 4-7, 4-10, 4-13
 - Retry count field, 3-9
 - RFNC address field, 3-8
 - Serial port field, 4-7, 4-10, 4-13
 - Stop bits option buttons, 4-8, 4-11, 4-14
- Communication Protocol box, C-5, C-7
- communications parameters, configuring for terminal sessions, 10-6
- Concatenation char field, 11-23
- configuration, *See* run-time configuration
- configuration files
 - active, 2-17
 - current, 2-17
 - default, 2-17
 - restoring default, 2-17
- Configure Device Initialization Download dialog box, 8-33, 8-43, 11-111, 11-120, B-16, B-21
- Configure Route dialog box, 5-14
 - Metric count field, 5-14
 - Route destination field, 5-14
 - Route type field, 5-14
 - Router field, 5-14
- Configure Time Parameters dialog box, 3-12, 3-28, 3-29, 4-16
 - Append enabled check box, 3-13, 3-29, 4-17
 - append parameters, 3-11, 3-28, 4-16
 - Broadcast enabled check box, 3-12, 3-29, 4-17
 - broadcast parameters, 3-11, 3-28, 4-15
 - Delimiter field, 3-13, 3-30
 - Include Date check box, 3-12, 4-17
 - Include Day check box, 3-13, 3-30
 - Include Month check box, 3-13, 3-30
 - Include Seconds check box, 3-12, 3-13, 3-30, 4-17
 - Include Year check box, 3-13, 3-29
 - Interval field, 3-13, 3-29, 4-17
 - Julian date check box, 3-13, 3-30
 - Postamble field, 3-13, 4-17
 - Preamble field, 3-13, 4-17
 - Record day rollover check box, 4-17
 - Time format option buttons, 3-13, 4-17
- configuring a next host screen, 11-37, 11-51
- configuring advanced SDLC parameters, 7-6
- configuring download information, B-16
- configuring RF controller cards, 3-6
- configuring routing tables, 5-14
- configuring security, C-8

Model 200 Controller User's Manual

- configuring the controller SNA node, 10-20
- configuring the IEEE 802.2 protocol, 5-16
- configuring the local SNA node, 8-17, 10-20
- configuring the NetOp guest, C-11
- configuring the NetOp host, C-3
- configuring the UDP Plus network, 3-21
- configuring TRAKKER Antares terminals, using the download server, B-20
- Connection field, 3-16, 3-32, 4-20
- Connection Point List dialog box, 3-7, 3-21, 4-5
- Continue processing screen events option button, 11-47
- controller
 - acknowledging transactions, 1-25
 - adding an RF controller card, 3-7
 - adding the UDP Plus network, 3-22
 - architecture, 1-15
 - communicating with TCP/IP applications, 9-18
 - configuring for token ring, 5-5
 - connecting to coaxial, 6-4
 - connecting to Ethernet, 5-4
 - connecting to SDLC, 7-4
 - connecting to the 2.4 GHz RF network, 3-19
 - connecting to the 900 MHz RF network, 3-4
 - connecting to twinaxial, 6-4
 - DevComm, 1-15
 - EmComm, 1-16
 - features, 1-4
 - front panel, 1-9
 - identifying data collection devices, 8-7, 8-12, 8-22
 - maintaining, 2-18
 - message handler, 1-15
 - NetComms, 1-16
 - package contents, 1-7
 - rear panel, 1-10
 - receiving unsolicited data, 9-20
 - setting application status, 1-30
 - TSM, 1-16
 - using as an IP bridge, 3-19
 - using to configure TRAKKER Antares terminals, B-20
 - using to upgrade TRAKKER Antares terminals, D-6
 - See also* external Intermec controllers
- Controller address field, 6-6
- Controller Command Prompt option, 2-26
- controller parameters, 4-6
- controller SNA node, configuring, 10-20
- Controls option buttons, 10-13
- copying a script file, 11-19
- copying a terminal screen, 11-99
- copying download information, B-15
- creating a download server command, B-18
- creating a logon sequence, 11-27
- creating a new script file, 11-17
- creating a normal logoff sequence, 11-29
- creating a region message, 11-53
- creating a screen for data collection devices, 11-83
- creating a screen message, 11-53
- creating an abnormal logoff sequence, 11-31
- creating menus, 11-100
- creating script files, 11-7
- CrossBar and 9180 to Model 200 Controller worksheet, E-7
- CrossBar devices
 - configuring, 4-19
 - editing, 4-21
- CrossBar network, 1-4
 - definition, G-5
 - figure, 4-4
- CrossBar to Model 200 Controller worksheet, E-9
- CSMA/CD, definition, G-5
- Current button, 11-35
- current configuration, 2-17
- Current cursor position option button, 11-56
- current host screen, 11-36
- Current NAU field, 8-29
- Current region check box, 11-56
- Current row option button, 11-56
- current screen, definition, G-5
- current transaction, 11-34
 - definition, G-5
 - selecting host screens, 11-36
- CURRENT_SCREEN command, 11-105
- Cursor keys option buttons, 10-13

D

- Data bits option buttons, 4-7, 4-10, 4-13
- data collection
 - starting, 2-24
 - stopping, 2-25
- data collection devices
 - creating screens, 11-83
 - definition, G-5
 - explicitly linking to hosts, 8-7, 8-12, 8-22
 - identifying, 4-19
 - routing transactions, 1-21
- data collection network
 - connecting to, 3-4
 - connecting to 900 MHz, 3-5
 - connecting to CrossBar network, 4-4
 - connecting to UDP Plus network, 3-20
 - figure, 1-6
- Data field, B-8
- data integrity, 1-18, 1-25
 - with controllers, 1-28
- data integrity modes, 1-28
 - Faster mode, 1-28
 - Safer mode, 1-28
- Data or system field, B-8
- Data response timeout field, 11-23, 11-25
- data transactions, 1-17
- data transmission, definition, G-5
- Data type field, 11-92
- date fields, 11-90
- DcmRsmTran system transaction, 1-30
- default configuration, 2-17
 - restoring, 2-17
- Define button, 11-48
- Define Groups button, D-14, D-16
- Define Groups dialog box, D-14, D-16
 - Available Devices list box, D-15
 - Defined Groups list box, D-15
 - Groups list box, D-15
 - Rename button, D-16
- Define Message dialog box, 11-55
 - Current cursor position option button, 11-56
 - Current region check box, 11-56
 - Current row option button, 11-56
 - Name field, 11-56
 - None option button, 11-56
 - Region option button, 11-56
 - Text field, 11-56
 - Type option buttons, 11-56
- Defined Groups list box, D-15
- defining a group, D-14
- defining a next screen sequence, 11-97
- defining user blocks, 11-65
- Delete Address button, 5-12
- Delete button, 1-14
- Delete Files button, 2-23
- Delete Script dialog box, 11-21
 - Script name field, 11-21
- Delete User Files dialog box, 2-23
 - Delete Files button, 2-23
 - root directory list box, 2-23
 - Selected Files list box, 2-23
- Delete User Files option, 2-23
- deleting a script file, 11-21
- deleting objects, xxi
- deleting user files, 2-23
- Delimiter field, 3-13, 3-30, 9-13
- delivery response, 1-19, 1-25
- Delivery Responses box, 3-19, 3-35
- Description box, 11-17, 11-19
- Description field, 11-63
- Description text box, 11-17
- destination field, 1-18
- Destination ID field, B-8
- Destination name field, 9-9
- destinations, adding a name, 9-8
- Details button, D-18, D-19
- DevComms, 1-15, 1-17
 - definition, G-5
- Device Address dialog box, 3-36, 3-37
 - Domain field, 3-36
 - IP address field, 3-37
 - Resolve button, 3-36
- device address, definition, G-6
- device communications process, *See* DevComms
- device license, *See* terminal license
- Device List dialog box, 3-16, 3-31, 4-20
 - Connection field, 3-16, 3-32, 4-20
 - Disable All button, 3-16, 3-32, 4-20
 - Enable All button, 3-16, 3-32, 4-20

Model 200 Controller User's Manual

- Device List dialog box (*continued*)
 - Enabled check box, 3-16, 3-32, 4-20
 - Device Parameters dialog box, 3-17, 3-33, 4-21
 - Able to receive data check box, 3-17, 3-34, 4-21
 - Auto-insert from device field, 3-18, 3-34, 4-22
 - Device type field, 3-17, 3-34, 4-22
 - Hot standby field, 3-18, 3-34, 4-22
 - Interactive response field, 3-18, 3-34, 4-22
 - Logical name field, 3-17, 3-34, 4-21
 - Physical address field, 4-22
 - To be routed to device field, 3-18, 3-34, 4-22
 - Device time-out field, D-11
 - Device type field, 3-17, 3-34, 4-22
 - device, definition, G-5
 - devices
 - editing, 3-17
 - identifying, 3-15
 - DHCP server, using to provide TCP/IP configurations, 5-6
 - dialog boxes
 - buttons, 1-14
 - moving around, 1-13
 - navigating, 1-13
 - dial-up SLIP, using with remote console, C-4
 - direct sequencing, definition, G-6
 - direct TCP/IP socket interface, 1-4
 - comparing to the NetComm API, 9-25
 - figure, 9-24
 - host application requirements, 9-26
 - using, 9-23
 - using international text pass-through, 9-27
 - using the \$IPT transaction ID, 9-23, 9-26
 - Disable All button, 3-16, 3-32, 4-20
 - disabling the security for the TE Configuration menu, 8-49
 - displaying international characters
 - on JANUS devices, 8-39
 - on TRAKKER Antares terminals, 8-45
 - DNS
 - using, 5-10
 - DNS button, 5-10
 - DNS Configuration dialog box, 5-10
 - Domain Names box, 5-11
 - Name Server Addresses box, 5-11
 - DNS server
 - determining an IP address, 3-25, 3-36
 - using, 3-25
 - Domain field, 3-26, 3-36
 - domain name systems, *See* DNS
 - Domain Names box, 5-11
 - domain, definition, G-6
 - Don't Upgrade option, D-9, D-10
 - double pass-through, performing, 8-21
 - Down button, 11-60
 - Downline Connections list box, 3-7, 3-22
 - downline, definition, G-6
 - download server
 - adding a group, B-13
 - copying information, B-15
 - downloading JANUS TE software, 8-32, 8-33
 - transferring files, B-16
 - using to download the template, 11-114, 11-119
 - using to download the terminal template application, 11-111
 - using to download TRAKKER Antares TE software, 8-42
 - download server commands, using to transfer files, B-18
 - downloading files
 - using download server commands, B-18
 - using the download server, B-16
 - downloading JANUS TE software, 8-31, 8-33, 8-34, 11-113, 11-114
 - downloading the terminal template application, 11-111, 11-113
 - using Interlnk, 11-112
 - downloading TRAKKER Antares TE software, 8-41
- ## **E**
- Edit button, 1-14
 - Edit NAU Address dialog box, 8-29
 - Current NAU field, 8-29
 - editing a CrossBar device, 4-21
 - editing a device's IP address, 3-37
 - editing a link, 8-29
 - editing an RF device, 3-17
 - editing objects, xxi

- editing the captured keystrokes, 11-33
 - EHLLAPI mnemonic field, 11-23
 - electronic software distribution, D-6
 - EmComms, 1-16
 - definition, G-6
 - Emulator Communications, *See* EmComms
 - Enable All button, 3-16, 3-32, 4-20
 - Enabled check box, 3-16, 3-32, 4-20
 - ending terminal emulation, on JANUS devices, 8-37
 - error log file, A-5
 - error messages, A-26
 - viewing, A-28
 - error messages, A-26
 - message boxes, A-9
 - understanding, A-29
 - viewing, A-26
 - Error retries option buttons, 11-23
 - Ethernet
 - configuring network adapter card for IEEE 802.2, 5-16
 - configuring network adapter card for TCP/IP, 5-6
 - configuring routing tables, 5-14
 - converting IP addresses to token ring, B-5
 - definition, G-6
 - enabling routing daemon, 5-12
 - installing the controller, 5-4
 - manually configuring TCP/IP, 5-6
 - routing tables, 5-6
 - setting up a 3270 terminal session, 10-5
 - using DHCP for TCP/IP configurations, 5-6
 - Ethernet driver support field, 5-18
 - event log
 - saving to disk, D-20
 - viewing, D-20
 - Event name field, D-9
 - Event Schedule box, D-11
 - events, *See* screen events
 - exiting the TE Configuration menu
 - on JANUS devices, 8-36
 - on TRAKKER Antares terminals, 8-44
 - explicit links
 - between devices and hosts, 8-7, 8-12, 8-22
 - editing NAUs, 8-29
 - external Intermecc controllers, 1-4, 1-28, 4-4
 - adding, 4-5
 - adding a 9154 controller, 4-7
 - adding a 9161 controller, 4-10
 - adding a 9180 controller, 4-13
 - Communication Parameters box, 4-6
 - Hot Standby Timeout box, 4-6
 - Integrity Mode box, 4-6
 - Multi-Drop Enabled box, 4-6
 - parameters, 4-6
 - setting the time parameters, 4-15
 - Time Parameters button, 4-15
- F**
- fan, 1-10
 - Fast Setup, 1-4, 1-12
 - definition, G-6
 - Faster mode, 1-28
 - features, 1-4
 - Field label field, 11-40
 - Field name field, 9-14, 11-91
 - field, definition, G-7
 - field-formatted screen, definition, G-7
 - File Handling dialog box
 - Backup User Files option, 2-19
 - Delete User Files option, 2-23
 - Restore User Files option, 2-21
 - File option button, 11-94
 - File Transfer Time box, 2-15
 - FILL_FIELD command, 11-103
 - filling the NAU pool, 8-28
 - Firmware button, D-17
 - Firmware comment field, D-13
 - Firmware File Sets dialog box, D-17
 - Delete button, D-18
 - Details button, D-18
 - Load Firmware button, D-17
 - Firmware Upgrade Utility, 1-5, 8-41, D-6
 - Add a New Upgrade Event to be Scheduled dialog box, D-9
 - adding upgrade events, D-8
 - defining a group, D-14
 - deleting applications, D-18
 - deleting firmware, D-18
 - Details button, D-19

Model 200 Controller User's Manual

Firmware Upgrade Utility (*continued*)

- Firmware button, D-6, D-17
 - loading files from a disk, D-12, D-17
 - performing the upgrade, D-16
 - renaming a group, D-16
 - Scheduled Firmware Upgrades box, D-7
 - scheduling upgrade events, D-6
 - Upgrade Now! button, D-16
 - View Log button, D-20
 - viewing details of a firmware file, D-18
 - viewing details of an application, D-18
 - viewing firmware and applications, D-17
 - viewing the event log, D-20
 - viewing upgrade event details, D-18
- Firmware version field, D-9
- Don't Upgrade option, D-9
- fixed fields, 11-90
- floppy disk access indicator, 1-9
- floppy disk drive, 1-9
- fNetACK flag, 9-20
- frequency hopping, definition, G-7
- From field, 11-94
- front panel
- description, 1-9
 - figure, 1-9, 1-10
 - floppy disk access indicator, 1-9
 - floppy disk drive, 1-9
 - hard disk access indicator, 1-9
 - power indicator, 1-9
 - power switch, 1-9
 - reset switch, 1-9
- FTP
- using to download JANUS TE software, 8-34, 11-113, 11-114
 - using to download the terminal template application, 11-113
- fully interactive system, 1-26

G

- Generate Template dialog box, 11-102
 - Menu name field, 11-102
 - Template file name field, 11-102
- generating templates, 11-102
- Get Field button, 11-18
 - using to get host screen field attributes, 11-42

- using to get screen identifier, 11-64
- Get Region button, using to get region attributes, 11-49
- Go to next screen option button, 11-47
- group
 - defining for Firmware Upgrade Utility, D-14
 - renaming in the Firmware Upgrade Utility, D-16
- Group Name dialog box, D-15
 - Group name field, D-15
- Group name field, B-14, D-15
- Groups list box, D-15
- guest software, configuring C-11
- GUI, learning about, 1-11

H

- handshake, 1-18, 1-26
- hard disk access indicator, 1-9
- header
 - batch flag, 1-33
 - destination field, 1-18
 - system message flag, 1-18
 - transaction, 1-17
- Help button, 1-14
- help, using, 1-12
- Hide at Boot Time button, 1-11
- host
 - adding, 8-10, 8-15, 8-25, 10-10, 10-18, 10-23
 - explicitly linking to devices, 8-7, 8-12, 8-22
 - performing a double pass-through, 8-21
 - removing a user ID, 8-19
 - requirements for terminal emulation, 8-6
 - setting a user ID, 8-19
 - setting security, 8-19
- host access sequences
 - capturing, 11-26
 - creating a logon sequence, 11-27
 - creating a normal logoff sequence, 11-29
 - creating an abnormal logoff sequence, 11-31
- host application, requirements for direct TCP/IP socket interface, 9-26
- host application, definition, G-7
- host busy, definition, G-7
- host computer, definition, G-7

- Host Connection Configuration dialog box, 8-15, 8-26, 10-18, 10-19, 10-24
 - Adapter card field, 8-16, 8-26, 10-18, 10-24
 - Address field, 8-16, 8-26, 10-19, 10-24
 - Host LU field, 8-16, 10-19
 - Host name field, 8-16, 8-26, 10-18, 10-24
 - Local PU field, 8-15, 8-16, 8-25, 8-26, 10-19, 10-24
 - Network ID field, 8-16, 10-19
 - Node ID field, 8-26, 10-24
- host connectivity table, 8-6, 10-5
- Host LU field, 8-16, 10-19
- Host Name - Linked Terminal - NAU list box, 8-23
- Host Name - Linked Terminals list box, 8-8, 8-13
- Host Name box, 10-8, 10-16, 10-22
- Host name field, 8-10, 8-16, 8-26, 10-10, 10-18, 10-24
- Host Name list box, 8-8, 8-13, 8-23
- host parameters
 - 3270 SNA terminal emulation, 8-22
 - 3270 terminal session on Ethernet, 10-5
 - 3270 terminal session on SDLC, 10-6
 - 5250 SNA terminal emulation, 8-12
 - 5250 terminal session on SDLC, 10-5
 - APPC applications, 9-5
 - peer-to-peer applications, 9-5
 - TCP/IP applications, 9-5
 - terminal sessions, 10-5
 - VT/ANSI terminal emulation, 8-7
- host screen, 11-26
 - selecting regions, 11-43
- Host Screen Definition dialog box, 11-63
 - Cancel processing screen events option button, 11-47
 - Column field, 11-63
 - Description field, 11-63
 - Row field, 11-63
 - Screen ID field, 11-63
 - Screen label field, 11-63
- Host Screen Field Definition dialog box, 11-40
 - Column field, 11-40
 - Field label field, 11-40
 - Keystroke to exit field, 11-41
 - Length field, 11-40
 - Row field, 11-40
 - Static string option button, 11-41
 - Transaction field number option button, 11-41
- Host Screen Field List dialog box, 11-39
- host screen fields
 - adding, 11-40
 - identifying, 11-10
 - selecting, 11-39
 - using the Get Field button, 11-42
- Host Screen Region Definition dialog box, 11-45
 - Any string within option button, 11-46
 - Capture button, 11-48, 11-50
 - Column field, 11-46
 - Continue processing screen events option button, 11-47
 - Define button, 11-48
 - Go to next screen option button, 11-47
 - Keystrokes to clear check box, 11-46
 - Region group check box, 11-46
 - Region label field, 11-46
 - Row field, 11-46
 - Send message check box, 11-46, 11-47
 - Specific string option button, 11-46
- Host Screen Region List dialog box, 11-44
- host screens
 - adding, 11-63
 - current, 11-36
 - defining a main host screen, 11-27
 - maintaining, 11-61
 - selecting for current transaction, 11-36
 - selecting host screen fields, 11-39
- Host Session button, 11-89
- Host session field, 10-26
- host session, starting, 10-26
- Host Terminal Session box, 11-78
- Host user ID field, 8-20, 10-16
- host window, 11-84
 - getting a terminal field attributes from, 11-96
 - getting host screen field attributes, 11-42
 - getting terminal field attributes from, 11-95
 - getting the screen identifier, 11-64
- HOSTS file, definition, G-7
- hot key, TE Configuration menu 8-35

Model 200 Controller User's Manual

Hot standby field, 3-18, 3-34, 4-22, 9-9
Hot Standby files, 1-25, 1-26, 1-27, 1-29, 1-33, 9-22
 clearing, A-7
 using with batch applications, 9-29
 viewing, A-7
Hot Standby message, 1-26, 1-32
Hot Standby message field, 9-13
Hot Standby mode
 changing to active mode, 1-33
 definition, G-7
 fully interactive system, 1-26
 noninteractive system, 1-27
 partially interactive system, 1-27
Hot Standby timeout, 1-29, 1-30, 9-22
Hot Standby Timeout box, 3-6, 3-9, 3-23, 4-6, 4-8, 4-11, 4-14
Hot Standby timeout field, 9-9, 11-78

I

IBM mode, selecting, 8-18
ID delimiter field, 2-15
identifying CrossBar devices, 4-19
identifying RF devices, 3-15
identifying UDP Plus terminals, 3-31
IEEE 802.2 Adapter Protocol Configuration
 dialog box, 5-16, 5-17
 Auto Calc button, 5-16, 5-18
 Ethernet driver support field, 5-18
 IEEE 802.2 card field, 5-18
 Maximum link stations field, 5-18
 Network adapter address field, 5-18
IEEE 802.2 card field, 5-18
IEEE 802.2 protocol, configuring, 5-16
IF_ command, 11-103
IF_BATCH command, 11-103
IF_SEARCH command, 11-103
Immediately check box, D-11, D-16
IMS application, 9-30
Inactivity timeout after field, C-9
Inactivity timer field, 3-23
Include Date check box, 3-12, 4-17
Include Day check box, 3-13, 3-30
Include Month check box, 3-13, 3-30
Include Seconds check box, 3-12, 3-13, 3-30, 4-17

Include Year check box, 3-13, 3-29
input fields, 11-89
Install Accessories dialog box, 2-9, 2-12
 Available Ports list box, 2-9, 2-12
installing the controller
 coaxial, 6-4
 Ethernet, 5-4
 SDLC, 7-4
 token ring, 5-5
 twinaxial, 6-4
Integrity Mode box, 4-6, 4-8, 4-11, 4-14
Inter system transaction, 9-18
interactive applications, 9-29
Interactive response, 4-22
Interactive response field, 3-18, 3-34, 9-9
interactivity
 full, 1-26
 noninteractive, 1-27
 partial, 1-27
 with devices, 1-25
Interlnk, using to download the terminal
 template application, 11-112
international characters
 displaying on JANUS devices, 8-39
 displaying on TRAKKER Antares terminals, 8-45
international text pass-through, 9-11, 9-27
International text pass-through check box, 9-9
Internet packet exchange, *See* IPX
Internet protocol, *See* IP
Interprocess Communication channels
 ACK channel, 1-15
 Receive channel, 1-15
Interval field, 3-13, 3-29, 4-17
IP, 9-16
 definition, G-8
IP address
 clearing, 5-12
 definition, G-8
 determining using DNS, 3-25, 3-36
 editing, 3-37
 TCP/IP applications, 9-5
IP address field, 3-37, 8-10, 10-10
IP bridge, using the controller, 3-19
IP Trace Options box, A-64

IPC channel, 9-18
 IPX, definition, G-8
 IRL programs, limitations when downloading,
 B-12

J

JANUS devices
 communicating with access points, 3-19
 configuring for 900 MHz RF network, 11-109
 configuring for screen mapping, 11-109
 configuring for terminal emulation, 8-30,
 8-35
 configuring for UDP Plus communications,
 8-31
 configuring for UDP Plus network, 11-109
 displaying international characters, 8-39
 downloading the template, 11-113
 downloading the terminal template
 application, 11-110
 ending terminal emulation, 8-37
 identifying to controller, 8-7, 8-12, 8-22
 loading validation files, 11-116
 running screen mapping, 11-117
 running terminal emulation, 8-37
 setting security, 8-46
 starting terminal emulation, 8-36
 terminal emulation software, 8-6
 TE hot key, 8-35
 using terminal emulation, 8-6
 using the auto-login feature, 8-38
 using the direct TCP/IP socket interface, 9-23
 JANUS devices for the 2.4 GHz RF network to
 Model 200 Controller worksheet, E-6
 JANUS TE software, downloading, 8-31, 8-32
 Julian date check box, 3-13, 3-30
 Julian format, definition, G-8

K

keyboard port, 1-10, 2-5
 keyboard, plugging in, 2-5
 keyboards, mapping to controller, 10-27
 Keypad option buttons, 10-13
 keystroke sequences, *See* keystrokes
 Keystroke to exit field, 11-41

keystrokes
 capturing, 11-26, 11-50
 supported mnemonics for terminal sessions,
 11-108

Keystrokes to clear check box, 11-46

L

LAN Workplace for DOS, 3-20
 LAN, definition, G-8
 language support, localized, 1-5
 Length field, 11-40, 11-92
 limitations
 VT/ANSI screen mapping, 11-105
 limitations of Script Builder Tool, 11-103
 Line mode option buttons, 7-6
 Line type option buttons, 7-6
 Line wrap enabled check box, 10-13
 Link station role field, 7-6
 link station, definition, G-8
 link support layer, *See* LSL
 linked screens, *See* next screen sequences
 Load Firmware button, D-17
 Load Firmware File Set dialog box, D-13
 Applications on Diskette box, D-12
 Firmware comment field, D-13
 System on Diskette box, D-12
 View ReadMe button, D-13
 Load From Diskette button, D-12
 loading firmware and applications, D-12
 loading TRAKKER Antares applications, D-17
 loading TRAKKER Antares firmware, D-17
 local area network, *See* LAN
 Local field, 3-23
 Local host name field, 5-8
 Local IP address field, 5-8
 local network adapter, 1-4
 Local PU field, 8-15, 8-16, 8-25, 8-26, 10-19,
 10-24
 local SNA node, configuring, 8-17, 10-20
 Local station field, 7-5
 localized language support, 1-5
 Lock controller keyboard and mouse check box,
 C-9
 LOG_ERROR command, 11-103
 Logical name field, 3-17, 3-34, 4-21

Model 200 Controller User's Manual

- logical unit, *See* LU
- logitudinal redundancy check, *See* LRC
- Logoff Sequence dialog box
 - Captured Keystrokes box, 11-30
 - Start button, 11-30
- logon sequence, 11-26, 11-27
 - example, 11-28
- Logon Sequence dialog box, 11-28, 11-61
 - Captured Keystrokes box, 11-28
 - Main screen field, 11-28
 - Start button, 11-50
 - Stop button, 11-28
- Lower limit field, 3-23
- LPT1, 1-10
- LRC enabled check box, 4-7, 4-10, 4-13
- LRC, definition, G-9
- LSL, definition, G-9
- LU 6.2 verbs, 9-29
- LU name, for APPC applications, 9-5
- LU, definition, G-8

M

- MAC address
 - converting IP addresses, B-5
 - for APPC applications, 9-5
- main host screen, 11-27
 - definition, G-9
 - identifying, 11-10
- main menu
 - figure, 1-11
 - sidebar buttons, 1-12
 - title bar, 1-12
 - toolbar buttons, 1-12
- Main screen field, 11-28
- Maintain Screen List dialog box, 11-61
 - Available Screens list box, 11-62
 - Selected Screens list box, 11-62
- maintaining the controller, 2-18
- maintaining the host screens, 11-61
- managing TRAKKE Antares firmware, D-17
- managing TRAKKER Antares applications, D-17
- manuals, related, xxii

- mapping
 - VT keyboard and controller keyboard, 11-106
 - VT keyboard and script keystroke names, 11-106
- mapping a transaction field, 11-80
- mapping terminal keyboards, 10-27
- Max connections field, 9-16
- Max I-field size field, 6-6, 7-7
- Maximum # messages displayed field, A-27
- Maximum attempts allowed before hangup field, C-10
- Maximum connections field, 2-15
- Maximum link stations field, 5-18
- memory, retaining transactions, 1-29
- Menu Items dialog box, 11-101
- Menu name field, 11-102
- Menu title field, 11-87
- menus
 - adding, 11-101
 - building, 11-100
 - generating into templates, 11-102
- message boxes, A-5
 - troubleshooting error messages, A-9
- message handler, 1-15, 1-17, 9-20
 - active applications, 1-31
 - application status, 1-30
- message log formatter, A-59, A-60
- Message Log Formatter window, A-60
- messages
 - adding, 11-55
 - status, 11-55
 - status vs. transaction, 11-57
 - transaction, 11-55
- messages, creating, 11-53
- Metric count field, 5-14
- MH_ACK box, A-67
- MH_IN box, A-67
- mnemonic keys, supported for terminal sessions, 11-108
- mode
 - Active Recovery, 1-33
 - data integrity, 1-28
- mode name, 8-18
- Mode name field, 10-16
- mode name, for APPC applications, 9-5

Model 200 Controller Status Monitor dialog box, A-26
 Maximum # messages displayed field, A-27
 Model 200 Controller to 9180 and CrossBar worksheet, E-7
 Model 200 Controller to 9180 worksheet, E-8
 Model 200 Controller to CrossBar worksheet, E-9
 Model 200 Controller to JANUS Devices for the 2.4 GHz RF Network worksheet, E-6
 Model 200 Controller to RF card worksheet, E-4
 Model 200 Controller to TRAKKER Antares terminals worksheet, E-5
 Model 200 Controller View Error Log dialog box, A-28
 modem
 connecting, 2-11
 part number, 2-11
 monitor
 connecting, 2-7
 part number, 2-7
 Monitor Message Handler Transactions dialog box, A-67
 Clear button, A-67
 closing, A-68
 MH_ACK box, A-67
 MH_IN box, A-67
 Output box, A-67
 Pause button, A-68
 saving the trace, A-68
 mouse port, 1-10, 2-6
 mouse, plugging in, 2-6
 Multi-Drop Enabled box, 4-6, 4-8, 4-11

N

Name field, 10-16, 10-22, 11-56, 11-78, 11-87
 Name Server Addresses box, 5-11
 NAU address field, 10-22
 NAU address, definition, G-9
 NAU pool, filling, 8-28
 NetACK, 9-20
 NetComms, 1-16, 9-16
 comparing to the direct TCP/IP socket interface, 9-25
 definition, G-9
 figure, 9-18
 linking to APPC application, 9-30
 receive port for TCP/IP applications, 9-5
 send port for TCP/IP applications, 9-5
 using, 9-18
 NetOp guest
 configuring the software, C-11
 using with OS/2, C-13
 using with Windows, C-11
 NetOp host
 configuring, C-3
 configuring for APPC, C-6
 configuring for dial-up SLIP, C-4
 configuring for TCP/IP, C-4
 NetWare Client for DOS, 3-20
 Network adapter address field, 5-18
 network adapter card
 coaxial, 6-5
 Ethernet, 5-6, 5-16
 SDLC, 7-5
 token ring, 5-6, 5-16
 twinaxial, 6-6
 network adapter cards, *See* local network adapter
 network adapter cards worksheet, E-10
 network address, 9-17
 network addressable unit address, *See* NAU address
 network administrator, definition, G-9
 network communications process, *See* NetComms
 network connection parameters, peer-to-peer 2-14
 network connections, verifying, B-7
 Network field, 3-23
 network ID
 definition, G-9
 for APPC applications, 9-5
 Network ID field, 3-8, 8-16, 8-17, 10-19, 10-20
 network interface card, definition, G-10
 network node, definition, G-10
 network trace, A-64
 network, definition, G-9
 New button, 11-38, 11-52
 New NAU field, 8-28

Model 200 Controller User's Manual

New/Open Script dialog box, 11-17
 Description box, 11-17
 Description text box, 11-17
 Script name field, 11-17
 Session ID field, 11-17, 11-18
 Start Session button, 11-18
Next field, 11-98
Next Host Screen dialog box, 11-38, 11-52
 Captured Keystrokes box, 11-37, 11-51
 New button, 11-38, 11-52
 Start button, 11-37, 11-51
 Stop button, 11-37, 11-51
Next Screen dialog box, 11-97
 Next field, 11-98
 Operator field, 11-98
 Screen field, 11-98
 Value field, 11-98
next screen sequences
 defining, 11-97
 defining for host screens, 11-37
 defining for region appearing, 11-51
NGERLOG1.BAK file, A-28
NGERLOG2.BAK file, A-28
NGERROR.LOG file, A-28
NIC, *See* network interface card
Node ID field, 8-17, 8-26, 10-20, 10-24
Node name field, 8-17, 10-20
nonactive application, 1-31
 sending Hot Standby messages, 1-32
None option button, 11-56, 11-94
noninteractive system, 1-27
normal logoff sequence, 11-26
 creating, 11-29
 example, 11-30
Normal Logoff Sequence dialog box, 11-30
 Stop button, 11-30
Novell user name, definition, G-10
NRZI option buttons, 7-6
Number field, 9-14
Number of sessions field, 10-9, 10-16, 10-22
Number of terminals to enable field, 3-26

O

OIA, *See* operator information area
OK button, 1-14

Old Transaction Name - New Transaction Name
 list box, 11-20
online help, *See* help
opening an existing script file, 11-18
Operator field, 11-98
operator information area, definition, G-10
OSI model, definition, G-10
Output box, A-67
output fields, 11-89

P

packet, definition, G-10
parallel port, 1-10
Parity option buttons, 4-7, 4-10, 4-13
partially interactive system, 1-27
Password field, 2-26, 8-20, 10-16
Pause button, A-68
PAUSE command, 11-103
peer-to-peer applications
 creating, 9-4
 setting host parameters, 9-5
peer-to-peer applications worksheet, E-18
peer-to-peer communications, 1-4
Peer-to-Peer Destination List dialog box, 9-7
Peer-to-Peer Destination Parameters dialog box,
 9-8
 Available list box, 9-9
 Destination name field, 9-9
 Hot standby field, 9-9
 Hot Standby Timeout field, 9-9
 Interactive response field, 9-9
 International text pass-through check box,
 9-9
 Selected list box, 9-9
 Transactions held in volatile memory field,
 1-29, 9-9
peer-to-peer links, setting up, 9-6
peer-to-peer network connection parameters,
 2-14
peer-to-peer network, definition, G-10
performing a double pass-through, 8-21
performing the upgrade, D-16
Physical address field, 4-22
Picture field, 11-92
picture fields, 11-90

- port number, 9-17
 - Port number field, 10-9
 - port, definition, G-10
 - Postamble field, 3-13, 4-17
 - power cord
 - part numbers, 2-4
 - plugging in, 2-4
 - using a surge protector, 2-4
 - using a UPS, 2-4
 - power indicator, 1-9
 - power switch, 1-9
 - Preamble field, 3-13, 4-17
 - preferred tree, definition, G-11
 - Prefix option button, 11-94
 - presentation space, definition, G-11
 - procedures
 - deleting an object, xxi
 - editing an object, xxi
 - Process batch transactions check box, 11-23
 - programming interface, figure, 9-21
 - protocol stack, definition, G-11
 - PUT_MAPPED_TRANS command, 11-103
 - PUT_TRANS_FIELD command, 11-104, 11-105
- R**
- Range option button, 11-94
 - RARP server, definition, G-11
 - RDRPGM.EXE, 11-5
 - downloading to JANUS devices, 11-110
 - rear panel
 - AC in, 1-10
 - AC out, 1-10
 - COM ports, 1-10
 - description, 1-10
 - fan, 1-10
 - keyboard port, 1-10
 - LPT1, 1-10
 - mouse port, 1-10
 - parallel port, 1-10
 - serial ports, 1-10
 - video port, 1-10
 - voltage select, 1-10
 - receive applications, 9-28
 - Receive channel, 1-15, 9-18, 9-22
 - Receive files from controller check box, C-9
 - receive NetComm, 9-18, 9-20
 - Receive transaction program, for APPC applications, 9-5
 - Receive Transactions dialog box, B-10
 - Receive Transactions option, B-9
 - receiving transactions, B-9
 - Record day rollover check box, 4-17
 - Region group check box, 11-46
 - Region label field, 11-46
 - region messages
 - creating, 11-53
 - definition, G-11
 - Region option button, 11-56
 - regions
 - adding, 11-44
 - definition, G-11
 - selecting for current host screen, 11-43
 - regions, using the Get Region button, 11-49
 - remote console, C-3
 - configuring NetOp guest for OS/2, C-13
 - configuring NetOp guest for Windows, C-11
 - configuring security, C-8
 - configuring the host, C-3
 - upgrading, D-5
 - Remote Console Configuration dialog box, C-4
 - Activate Defaults button, C-3
 - APPC Properties box, C-7
 - Communication Protocol box, C-5, C-7
 - Security Options button, C-10
 - Start Up Option box, C-5, C-7
 - TCP/IP Properties box, C-5
 - Remote Console Security Options dialog box, C-10
 - Blank controller screen check box, C-9
 - Chat check box, C-9
 - Inactivity timeout after field, C-9
 - Lock controller keyboard and mouse check box, C-9
 - Maximum attempts allowed before hangup field, C-10
 - Receive files from controller check box, C-9
 - Remote guest password field, C-10
 - Requires password field, C-10
 - Retype to confirm field, C-10

Model 200 Controller User's Manual

Remote Console Security Options dialog box

(continued)

Send files to controller check box, C-9

Use keyboard and mouse check box, C-9

Remote guest password field, C-10

Rename button, D-16

renaming a group, D-16

Repeat count field, 3-9

repeater, definition, G-11

Replace Old Name button, 11-20

requesting the template from the controller,

11-115, 11-121

requesting the validation file, 11-123

Required check box, 11-92

Requires password field, C-10

Reset on timeout check box, 11-22

reset switch, 1-9

Reset to Factory Defaults option, 2-17

resetting default configuration, 2-17

Resolve button, 3-36, 8-11, 10-11

Response timeout field, 11-22

Restore Files button, 2-20, 2-22

Restore Old Name button, 11-20

Restore System Files message box, 2-20

Restore System Files option, 2-20

Restore User Files dialog box, 2-22

Available Files list box, 2-22

Restore Files button, 2-22

Selected Files list box, 2-22

Restore User Files option, 2-21

restoring default configuration, 2-17

restoring runtime configuration, 2-20

restoring system files, 2-20

restoring the controller configuration, 2-20

restoring user files, 2-21

Retries field, 3-23

Retry count field, 3-9

Retype to confirm field, C-10

reverse address resolution protocol, *See* RARP
server

RF card to Model 200 Controller worksheet, E-4

RF controller cards, 1-4

2-port, 3-4

4-port, 3-4

adding, 3-7

cables, 3-4

Communication Parameters box, 3-6

configuring, 3-6

Hot Standby Timeout box, 3-6

Time Parameters button, 3-11

Transactions Routed to This Card box, 3-6

RF devices

editing, 3-17

identifying, 3-15

RFDC system, definition, G-11

RFNC address field, 3-8

RFNC address, definition, G-11

Ring speed option buttons, 5-8, 5-17

root directory list box, 2-19, 2-23

Route destination field, 5-14

Route type field, 5-14

Router field, 5-14

router, definition, G-12

Routing button, 5-12

routing daemon

disabling, 5-12

enabling, 5-12

Routing Table Entries Configuration dialog box,
5-13

routing tables, 5-6

configuring, 5-14

routing transactions, 1-18, 9-6

Row field, 11-40, 11-46, 11-63, 11-91

Run View button, A-6

running screen mapping, 11-117, 11-123

running terminal emulation

on JANUS devices, 8-37

on TRAKKER Antares terminals, 8-45

run-time configuration

activating, 8-29, 9-15, 10-25, 11-83, 11-103

backing up, 2-18

saving, 8-29, 9-15, 10-25, 11-83, 11-103

viewing, A-5

runtime configuration, restoring, 2-20

Runtime Configuration dialog box, A-6

Save to Disk button, A-7

run-time options, setting for the script file, 11-22

Runtime Script Options dialog box, 11-22

Audit Options box, 11-23

Concatenation char field, 11-23

Runtime Script Options dialog box (*continued*)

- Data response timeout field, 11-23
- EHLAPI mnemonic field, 11-23
- Error retries option buttons, 11-23
- Process batch transactions check box, 11-23
- Reset on timeout check box, 11-22
- Response timeout field, 11-22
- Send to source when batch transaction received check box, 11-23

S

- Safer mode, 1-28
- Save and activate changes check box, 2-25
- Save and Activate sidebar button, 2-17, 2-24
- Save as new defaults check box, 10-13
- Save As Script With Different Transaction Names dialog box
 - Available Transactions list box, 11-20
 - Change Name button, 11-20
 - Old Transaction Name - New Transaction Name list box, 11-20
 - Replace Old Name button, 11-20
 - Restore Old Name button, 11-20
 - Transaction name field, 11-20
- Save Configuration sidebar button, 2-17
- Save Event Log dialog box, D-20
- Save Script As dialog box
 - Description box, 11-19
 - Script name field, 11-19
 - Use different transactions check box, 11-20
- Save to Disk button, A-7
- saving a script file, 11-18
- saving your run-time configuration, 8-29, 9-15, 10-25, 11-83, 11-103
- Screen Field Validation dialog box
 - Valid if option buttons, 11-94
- Screen Event Ordering dialog box, 11-53, 11-59, 11-60
 - Down button, 11-60
 - Up button, 11-60
- screen events
 - changing the order, 11-59
 - definition, G-12
 - handling regions, 11-59
 - mapping fields, 11-59
 - sending screen messages, 11-53, 11-59
- Screen field, 11-98
- Screen Field Parameters dialog box, 11-91, 11-92
 - Attribute field, 11-92
 - Column field, 11-91
 - Data type field, 11-92
 - Field name field, 11-91
 - Length field, 11-92
 - Picture field, 11-92
 - Required check box, 11-92
 - Row field, 11-91
 - Type field, 11-91
 - Value field, 11-92
- Screen Field Validation dialog box
 - File option button, 11-94
 - From field, 11-94
 - None option button, 11-94
 - Prefix option button, 11-94
 - Range option button, 11-94
 - To field, 11-94
- screen fields, *See* terminal fields
- Screen ID field, 11-63
- screen identifier
 - using the Get Field button, 11-64
- Screen label field, 11-63
- screen mapping, 11-5
 - about the Script Builder Tool, 11-5
 - configuring JANUS devices, 11-109
 - configuring sessions, 11-76
 - configuring TRAKKER Antares terminals, 11-118
 - entering data, 11-117
 - figure, 11-6
 - running on JANUS devices, 11-117
 - running on TRAKKER Antares terminals, 11-123
 - upgrading, D-4
 - using the host window, 11-84
 - using the terminal display, 11-84
- Screen Mapping button, 11-89
- Screen Mapping Field List dialog box, 11-80
- Screen Mapping Field Placement dialog box, 11-82
- screen mapping field placement entry, adding, 11-82

Model 200 Controller User's Manual

- Screen Mapping License Upgrade message box, D-4, D-5
- Screen Mapping Session Definition dialog box, 11-77
 - Available list box, 11-78
 - Host Terminal Session box, 11-78
 - Hot Standby timeout field, 11-78
 - Name field, 11-78
 - Script File box, 11-78
 - Selected list box, 11-78
 - Start session at data collection start check box, 11-78
 - Visible when data collection started? check box, 11-78
- Screen Mapping Session List dialog box, 11-76
- screen mapping sessions, adding, 11-77
- screen mapping trace, A-65
- Screen Mapping Transaction IDs dialog box, 11-34
 - Available list box, 11-34
 - Current button, 11-35
 - Selected list box, 11-34
- screen mapping, definition, G-12
- Screen Message List dialog box, 11-54
 - Send message as current screen event check box, 11-54
- screen message, definition, G-12
- screen messages, creating, 11-53
- screen sequences
 - defining for host screens, 11-37
 - defining for region appearing, 11-51
 - defining for terminal screens, 11-97
- screens, validating terminal fields, 11-93
 - See also* terminal screens
 - See also* host screens
- script
 - symbols, 11-69
 - viewing, 11-69
- Script Builder, 1-4
 - FILL_FIELD, 11-103
- Script Builder Tool, 11-5
 - ACK_MESSAGE, 11-103
 - AUDIT, 11-103
 - CAPTURE_POS, 11-103
 - commands not generated, 11-103
 - CURRENT_SCREEN, 11-105
 - flow chart, 11-15
 - IF_, 11-103
 - IF_BATCH, 11-103
 - IF_SEARCH, 11-103
 - limitations, 11-103
 - LOG_ERROR, 11-103
 - PAUSE, 11-103
 - preparing to use, 11-7
 - PUT_MAPPED_TRANS, 11-103
 - PUT_TRANS_FIELD, 11-104, 11-105
 - SEARCH_SCREEN, 11-103
 - SEND_MESSAGE, 11-104
 - toolbar, 11-16
 - understanding, 11-14
 - USER_INPUT, 11-103
 - using, 11-16
 - WAIT_FOR, 11-103, 11-105
 - WAIT_FOR_LABEL_POS, 11-103
 - WAIT_FOR_POS, 11-103
- script checker, 11-70
- Script File box, 11-78
- script files
 - before you begin, 11-7
 - checking, 11-70
 - copying, 11-19
 - creating, 11-7
 - creating new, 11-17
 - definition, G-12
 - deleting, 11-21
 - identifying key elements, 11-10
 - manually creating, 11-7
 - multiple transaction, 11-8
 - multiple transaction example, 11-12
 - opening an existing, 11-18
 - saving, 11-18
 - saving under a new name, 11-18
 - single transaction, 11-8
 - single transaction example, 11-10
 - verifying the logic, 11-71
- Script name field, 11-17, 11-19, 11-21
- SDLC
 - cable, 7-4
 - configuring advanced parameters, 7-6
 - configuring network adapter card, 7-5

- SDLC (*continued*)
 - installing the controller, 7-4
 - setting up a 3270 terminal session, 10-6
 - setting up a 5250 terminal session, 10-5
- SDLC Adapter Configuration dialog box, 7-5
 - Local station field, 7-5
- SEARCH_SCREEN command, 11-103
- security
 - changing for the TE Configuration menu, 8-48
 - configuring for remote console, C-8
 - defining for 5250 host, 8-19
 - disabling for the TE Configuration menu, 8-49
 - setting for the TE Configuration menu, 8-46
 - verifying on TE Configuration menu, 8-49
- Security Options button, C-10
- Selected Files list box, 2-20, 2-22, 2-23
- Selected Groups/Devices list box, D-11
- Selected list box, 9-9, 11-34, 11-78
- Selected Screens list box, 11-62
- Selected Terminals list box, B-14
- selecting host screen fields, 11-39
- selecting transactions for the script, 11-34
- send applications, 9-28
- Send files to controller check box, C-9
- Send message as current screen event check box, 11-53, 11-54
- Send message check box, 11-46, 11-47
- send NetComm, 9-18, 9-20
- Send to source when batch transaction received check box, 11-23
- Send Transaction dialog box, B-7, B-18
 - Data field, B-8
 - Data or System field, B-8
 - Destination ID field, B-8
 - Source ID field, B-8
 - Transaction ID field, B-8
- Send transaction program, for APPC applications, 9-5
- Send XID response immediately check box, 7-7
- SEND_MESSAGE command, 11-104
- sending a transaction, B-7
- sending download server commands, B-19
- sequenced packet exchange, *See* SPX
- serial controllers, *See* external Intermec controllers
- Serial port field, 4-7, 4-10, 4-13
- serial ports, 1-10
- serial, definition, G-12
- server, definition, G-12
- Session box, A-65
- Session ID field, 11-17, 11-18
- Session Name - Trace - Status list box, A-65
- Session name field, 10-8
- session pooling, definition, G-13
- session, definition, G-12
- setting script run-time options, 11-22
- setting security for the TE Configuration menu, 8-46
- setting system parameters, 2-14
- setting time parameters, 3-11, 3-28, 4-15
- setting up 3270 SNA terminal emulation, 8-22
- setting up 5250 SNA terminal emulation, 8-12
- setting up a screen mapping session, 11-76
- setting up peer-to-peer links, 9-6
- setting up Telnet terminal emulation, 8-7
- setting up terminal sessions, 10-4
- setting up the UDP Plus devices, 3-25
- setting up VT terminals, 10-12
- Setup for Controller dialog box, 4-7, 4-10, 4-13
 - Baud rate field, 4-7, 4-10, 4-13
 - BRU Parameters box, 3-6
 - Communication Parameters box, 3-6, 4-6
 - Data bits option buttons, 4-7, 4-10, 4-13
 - Hot Standby Timeout box, 3-6, 4-6, 4-8, 4-11, 4-14
 - Integrity Mode box, 4-6, 4-8, 4-11, 4-14
 - LRC enabled check box, 4-7, 4-10, 4-13
 - Multi-Drop Enabled box, 4-6, 4-8, 4-11
 - Parity option buttons, 4-7, 4-10, 4-13
 - Serial port field, 4-7, 4-10, 4-13
 - Stop bits option buttons, 4-8, 4-11, 4-14
 - Time Parameters button, 3-11, 4-9, 4-12, 4-15
 - Transactions held in volatile memory field, 4-8, 4-11, 4-14
 - Transactions Routed to This Card box, 3-6
- Setup for Controller RF card dialog box, 3-8
 - Acknowledgment delay field, 3-9
 - BRU Status check box, 3-9

Model 200 Controller User's Manual

Setup for Controller RF card dialog box

(continued)

- Card number field, 3-8
 - Channel - Frequency field, 3-9
 - Hot Standby Timeout box, 3-9
 - Network ID field, 3-8
 - Repeat count field, 3-9
 - Retry count field, 3-9
 - RFNC address field, 3-8
 - Transactions held in volatile memory field, 3-9
- Setup for UDP Plus Terminals dialog box, 3-25
- Base logical name field, 3-26
 - Domain field, 3-26
 - Number of terminals to enable field, 3-26
 - Starting IP address field, 3-26
 - Subnet mask field, 3-26
 - Use DNS check box, 3-26
- shell out feature, definition, G-13
- Short session ID field, 10-16, 10-22
- Show at Boot Time button, 1-11
- Show check box, 10-16
- Shutdown button, 2-25
- Shutdown Controller sidebar button, 2-25
- shutting down the controller, 2-25
- sidebar buttons, 1-12
- Save and Activate, 2-17, 2-24
 - Save Configuration, 2-17
 - Shutdown Controller, 2-25
 - Start Data Collection, 2-24
 - Stop Data Collection, 2-25
 - System Maintenance, 2-9, 2-11
- simple network management protocol, *See* SNMP
- Size field, 11-87
- SNA box, A-66
- SNA host, adding, 8-15, 8-25
- SNA Local Node Information dialog box, 10-20
- SNA Local Node Information dialog box, 8-17
- Network ID field, 8-17, 10-20
 - Node ID field, 8-17, 10-20
 - Node name field, 8-17, 10-20
- SNA node, configuring, 8-17

- SNA subsystem management, A-59, A-61
- SNA, definition, G-13
- SNMP, definition, G-13
- source application ID field, 9-28
- Source ID field, B-8
- Specific string option button, 11-46
- spread spectrum, definition, G-13
- SPX, definition, G-13
- Start button, 2-24, 10-26, 11-30, 11-32, 11-37, 11-50, 11-51
- Start Data Collection sidebar button, 2-24
- Start Host Session command, 10-26
- Start Host Session dialog box, 10-26
 - Host session field, 10-26
 - Start button, 10-26
- Start session at data collection start check box, 11-77, 11-78
- Start Session button, 11-18
- Start Up Option box, C-5, C-7
- starting a host session, 10-26
- starting a terminal session, 10-26
- Starting IP address field, 3-26
- starting terminal emulation, on JANUS devices, 8-36
- starting the controller, 2-24
- Static string option button, 11-41
- status message, 11-55
- status monitor, A-26
- status, application, 1-30
- Stop bits option buttons, 4-8, 4-11, 4-14
- Stop button, 2-25, 11-28, 11-30, 11-32, 11-37, 11-50, 11-51
- Stop Data Collection sidebar button, 2-25
- Stop Upgrade button, D-18
- store and forward, definition, G-13
- Strip pad field, 2-15
- subnet mask
 - clearing, 5-12
 - definition, G-14
- Subnet mask field, 3-26, 5-8
- Subsystem Management window, A-61
- surge protector, 2-4, 2-9
- system cabling specifications, B-3
- System Diagnostics sidebar button, A-59

- system files
 - backing up, 2-18
 - restoring, 2-20
 - System Maintenance dialog box
 - Backup System Files option, 2-18
 - Controller Command Prompt option, 2-26
 - Firmware Upgrade Utility, D-6
 - Receive Transactions option, B-9
 - Remote Console Support, C-4
 - Reset to Factory Defaults option, 2-17
 - Restore System Files option, 2-20
 - Send Transaction option, B-7
 - Start Host Session command, 10-26
 - System Maintenance sidebar button, 2-9, 2-11
 - system message flag, 1-18
 - system network architecture, *See* SNA
 - System on Diskette box, D-12
 - System Parameters dialog box, 2-14
 - Auto-Start box, 2-15
 - Bad ID response field, 1-32, 2-15
 - File Transfer Time box, 2-15
 - ID delimiter field, 2-15
 - Max connections field, 9-16
 - Maximum connections field, 2-15
 - network connection parameters, 2-14
 - peer-to-peer network connection parameters, 2-14
 - Terminal Emulation Setup Screens check boxes, 2-15
 - time synchronization, 2-14
 - Time Synchronization box, 2-15
 - transaction parameters, 2-14
 - System Reporting sidebar button, A-5
 - system trace, A-66
 - system transactions, 1-17
 - DcmRsmTran, 1-30
 - Inter, 9-18
 - setting application status, 1-30
- T**
- TCP, 9-16
 - definition, G-14
 - sockets, 9-22
 - TCP/IP, 5-6
 - configuring routing tables, 5-14
 - enabling routing daemon, 5-12
 - routing tables, 5-6
 - using with remote console, C-4
 - TCP/IP applications
 - communicating with, 9-16, 9-18
 - IP address, 9-5
 - NetComm receive port, 9-5
 - NetComm send port, 9-5
 - setting host parameters, 9-5
 - TCP/IP card field, 5-8
 - TCP/IP Host Connection dialog box, 8-10, 10-10
 - Host name field, 8-10, 10-10
 - IP address field, 8-10, 10-10
 - Resolve button, 8-11, 10-11
 - Use DNS check box, 8-10, 10-10
 - TCP/IP host, adding, 8-10, 10-10
 - TCP/IP Properties box, C-5
 - TCP/IP protocol
 - address family, 9-17
 - network address, 9-17
 - port number, 9-17
 - TCP/IP Protocol Configuration dialog box, 5-8
 - Delete Address button, 5-12
 - DNS button, 5-10
 - Local host name field, 5-8
 - Local IP address field, 5-8
 - Routing button, 5-12
 - Subnet mask field, 5-8
 - TCP/IP card field, 5-8
 - Use DHCP check box, 5-8
 - TCP/IP sockets
 - communicating with, 9-16
 - typical server/client configuration, 9-16
 - using for transaction routing, 9-20
 - using the direct socket interface, 9-23
 - TE Configuration menu
 - accessing on JANUS devices, 8-35
 - accessing on TRAKKER Antares terminals, 8-43
 - changing security, 8-48
 - disabling security, 8-49
 - exiting on JANUS devices, 8-36
 - exiting on TRAKKER Antares terminals, 8-44
 - setting security, 8-46
 - verifying that security is set, 8-49

Model 200 Controller User's Manual

- Telnet terminal emulation, 1-4
 - setting up, 8-7
- Telnet Terminal Emulation Configuration dialog box, 8-8
 - Available Terminals list box, 8-8
 - Host Name - Linked Terminals list box, 8-8
 - Host Name list box, 8-8
- Telnet terminal emulation worksheet, E-11
- template, *See* terminal template
 - definition, G-14
 - downloading to JANUS devices, 11-113
 - downloading to TRAKKER Antares terminals, 11-119
 - requesting from the controller, 11-115
 - using the download server to download, 11-114, 11-119
- Template file name field, 11-102
- templates, generating, 11-102
- terminal display, 11-84
- Terminal Download Configuration dialog box, 8-33, 8-42, 11-111, 11-119, 11-122, B-14
- terminal emulation, 1-4
 - about, 8-5
 - configuring JANUS devices, 8-30, 8-35
 - configuring TRAKKER Antares terminals, 8-40, 8-43
 - definition, G-14
 - ending on JANUS devices, 8-37
 - host connectivity table, 8-6
 - running on JANUS devices, 8-37
 - running on TRAKKER Antares terminals, 8-45
 - starting on JANUS devices, 8-36
- Terminal Emulation Setup Screens check boxes, 2-15
- terminal emulation software
 - downloading, 8-31, 8-41
 - for JANUS devices, 8-6
 - on TRAKKER Antares terminals, 8-7
- terminal fields
 - adding, 11-89
 - date pictures, 11-90
 - fixed, 11-90
 - input, 11-89
 - output, 11-89
 - picture, 11-90
 - time pictures, 11-90
 - using the Get Field button, 11-96
 - using the Host Session button, 11-95
 - validating, 11-93
- terminal keyboards, mapping to the controller keyboard, 10-27
- terminal license, 3-15, 3-31, 4-19, 8-6
 - definition, G-14
 - upgrading, D-3
- Terminal License Upgrade message box, D-4
- Terminal mode field, 10-8
- Terminal Password Configuration dialog box, 8-47
- Terminal Screen and Fields dialog box
 - Auto send check box, 11-88
 - Menu title field, 11-87
 - Size field, 11-87
 - Transaction field, 11-88
 - Wait for Response check box, 11-88
- Terminal Screen and Fields dialog box, 11-87
 - Host Session button, 11-89
 - Name field, 11-87
 - Screen Mapping button, 11-89
 - View button, 11-89
- Terminal Screen Field Validation dialog box, 11-93
- terminal screens
 - adding, 11-87
 - copying, 11-99
 - creating, 11-83
 - creating for data collection devices, 11-83
 - validating fields, 11-93
- Terminal Session Definition dialog box, 10-8, 10-15, 10-21
 - Host Name box, 10-8, 10-16, 10-22
 - Host user ID field, 10-16
 - Mode name field, 10-16
 - Name field, 10-16, 10-22
 - NAU address, 10-22
 - Number of sessions field, 10-9, 10-16, 10-22
 - Password field, 10-16
 - Port number field, 10-9
 - Session name field, 10-8

- Terminal Session Definition dialog box
 - (continued)
 - Short session ID field, 10-16, 10-22
 - Show check box, 10-16
 - Terminal mode field, 10-8
- Terminal Session List dialog box, 10-7
- terminal session manager, *See* TSM
- terminal sessions
 - adding a host, 10-18, 10-23
 - configuring communications parameters, 10-6
 - definition, G-14
 - setting host parameters, 10-5
 - setting up, 10-4, 10-6
 - starting, 10-26
 - supported keystroke mnemonics, 11-108
- terminal template application, 11-5, G-15
 - downloading to JANUS devices, 11-110
- Terminal/Group Copy dialog box, B-15
- Text field, 11-56
- text files, navigating in, 1-13
- time fields, 11-90
- Time format option buttons, 3-13, 4-17
- Time Parameters button, 3-11, 3-28, 4-9, 4-12, 4-15
- time parameters, setting, 3-11, 3-28, 4-15
- time synchronization, 2-14
- Time Synchronization box, 2-15
- title bar, 1-12
- TN3270 terminal emulation, 1-4, 8-6
 - setting up, 8-7
- TN5250 terminal emulation, 1-4, 8-6
 - setting up, 8-7
- To be routed to device field, 3-18, 3-34, 4-22
- To field, 11-94
- token ring
 - cable, 5-5
 - configuring network adapter card for IEEE 802.2, 5-16
 - configuring network adapter card for TCP/IP, 5-6
 - configuring routing tables, 5-14
 - converting IP addresses, B-5
 - definition, G-15
 - enabling routing daemon, 5-12
 - installing the controller, 5-5
 - manually configuring TCP/IP, 5-6
 - ring speed, 5-5
 - routing tables, 5-6
 - using DHCP for TCP/IP configurations, 5-6
- toolbar buttons, 1-12
- Trace check box, A-65
- Trace Configuration dialog box, A-62
 - Trace Control box, A-63
- Trace Control box, A-63
- Trace utility, A-59, A-62
 - adding a network trace, A-64
 - adding a screen mapping trace, A-65
 - adding a system trace, A-66
 - MH_ACK box, A-67
 - MH_IN box, A-67
 - Monitor Message Handler Transactions
 - dialog box, A-67
 - Output box, A-67
 - saving a trace, A-64
 - viewing a trace, A-63
- TRAKKER Antares TE software, downloading, 8-41
- TRAKKER Antares terminals
 - communicating with access points, 3-19
 - configuring for screen mapping, 11-118
 - configuring for terminal emulation, 8-40, 8-43
 - configuring for UDP Plus communications, 8-40
 - configuring using the download server, B-20
 - displaying international characters, 8-45
 - downloading the template, 11-119
 - identifying to controller, 8-7, 8-12, 8-22
 - loading applications from a disk, D-12, D-17
 - loading firmware from a disk, D-12, D-17
 - loading validation files, 11-122
 - managing firmware and applications, D-17
 - requesting the template, 11-121
 - running screen mapping, 11-123
 - running terminal emulation, 8-45
 - setting security, 8-46
 - terminal emulation software, 8-7
 - upgrading, D-6
 - using terminal emulation, 8-6

Model 200 Controller User's Manual

- TRAKKER Antares terminals (*continued*)
 - using the auto-login feature, 8-45
 - using the direct TCP/IP socket interface, 9-23
 - TRAKKER Antares terminals to Model 200
 - Controller worksheet, E-5
 - Transaction field, 11-88
 - Transaction field number option button, 11-41
 - Transaction Field Parameters dialog box, 9-14
 - Field name field, 9-14
 - Number field, 9-14
 - transaction fields
 - adding, 9-14
 - mapping, 11-80
 - transaction header, source application ID field, 9-28
 - Transaction ID box
 - Auto-insert from device field, 3-18, 3-34
 - Auto-inserted from device field, 4-22
 - To be routed to device field, 3-18, 3-34, 4-22
 - Transaction ID field, 9-13, B-8
 - transaction message, 11-55
 - example, 11-58
 - Transaction name field, 11-20
 - transaction parameters, 2-14
 - Transaction Parameters dialog box, 9-13
 - Delimiter field, 9-13
 - Hot Standby message field, 9-13
 - Transaction ID field, 9-13
 - transactions
 - acknowledging, 1-25
 - adding, 9-13
 - adding a field, 9-14
 - current, 11-34
 - data, 1-17
 - definition, G-15
 - header, 1-17
 - identifying, 11-10
 - retaining in memory, 1-29
 - routing, 1-15, 1-18, 9-6
 - routing from applications, 1-18
 - routing from devices, 1-21
 - selecting for the script, 11-34
 - system, 1-17
 - understanding, 1-17
 - understanding routing, 9-20
 - using in script files, 11-8
 - using the receive transactions feature, B-9
 - using the send transactions feature, B-7
 - Transactions box, A-66
 - Transactions held in volatile memory field, 1-29, 3-9, 3-23, 4-8, 4-11, 4-14, 9-9, 9-22
 - Transactions Routed to This Card box, 3-6
 - transferring files
 - using download server commands, B-18
 - using the download server, B-16
 - transmission control protocol, *See* TCP
 - troubleshooting
 - error log error messages, A-26
 - error log file, A-5
 - general, A-3
 - message box error messages, A-9
 - message boxes, A-5
 - message log formatter, A-59
 - SNA subsystem management, A-59
 - Trace utility, A-59
 - viewing Hot Standby files, A-5
 - viewing run-time configuration, A-5
 - viewing the status monitor, A-5
 - TSM, 1-16
 - twinaxial
 - cable, 6-4
 - configuring network adapter, 6-6
 - definition, G-15
 - installing the controller, 6-4
 - Twinaxial Protocol Configuration dialog box, 6-6
 - Controller address field, 6-6
 - Max I-field size field, 6-6
 - Type field, 11-91
 - Type option buttons, 11-56
- ## **U**
- UDP Plus network
 - adding, 3-22
 - configuring, 3-21
 - configuring JANUS devices, 8-31, 11-109
 - configuring TRAKKER Antares terminals, 8-40, 11-118
 - connecting to, 3-19
 - figure, 3-20

- UDP Plus Network Parameters dialog box, 3-22
 - Hot Standby Timeout box, 3-23
 - Inactivity timer field, 3-23
 - Local field, 3-23
 - Lower limit field, 3-23
 - Network field, 3-23
 - Retries field, 3-23
 - Time Parameters button, 3-28
 - Transactions held in volatile memory field, 3-23
 - Upper limit field, 3-23
- UDP Plus terminals
 - communicating with access points, 3-19
 - identifying, 3-31
 - setting up, 3-25
- UDP Plus, definition, G-15
- UDP, definition, G-15
- understanding the error messages, A-29
- understanding the Monitor Message Handler Transactions dialog box, A-67
- understanding the Script Builder Tool, 11-14
- understanding transaction routing, 9-20
- understanding transactions, 1-17
- uninterruptable power supply
 - connecting, 2-8
 - messages, 2-8
 - part number, 2-8
- UNIX user name, definition, G-15
- Unlinked NAUs pool, 8-28
- unsolicited data, sending to controller, 9-20
- Up button, 11-60
- Update button, A-8
- Upgrade Event Details dialog box, Stop Upgrade button, D-18
- upgrade events
 - adding, D-8
 - scheduling, D-6
 - viewing details, D-18
- Upgrade Events Details dialog box, D-19
- Upgrade Log dialog box, D-20
- Upgrade Now! button, D-16
- upgrading to remote console, D-5
- upgrading to screen mapping, D-4
- upgrading TRAKKER Antares terminals, D-6
- upgrading your terminal license, D-3
- upline network
 - configuring for token ring, 5-5
 - connecting to coaxial, 6-4
 - connecting to Ethernet, 5-4
 - connecting to SDLC, 7-4
 - connecting to twinaxial, 6-4
- upline, definition, G-15
- Upper limit field, 3-23
- UPS, *See* uninterruptable power supply
- Use device names check box, 8-12, 8-13
- Use DHCP check box, 5-8
- Use different transactions check box, 11-20
- Use DNS check box, 3-26, 8-10, 10-10
- Use keyboard and mouse check box, C-9
- User Block List dialog box, 11-66
 - Add After button, 11-68
- User Block Text dialog box, 11-68
- user blocks
 - adding, 11-68
 - defining, 11-65
 - using, 11-103
- User Datagram protocol, *See* UDP
- user files
 - backing up, 2-19
 - deleting, 2-23
 - restoring, 2-21
- USER_INPUT command, 11-103
- User-Defined Key option buttons, 10-13
- using DNS, 5-10
- using international text pass-through, 9-11, 9-27
- using peer-to-peer applications, 9-4
- using SNA subsystem management, A-61
- using the controller, 2-24
- using the direct TCP/IP socket interface, 9-23
 - comparing to the NetComm API, 9-25
 - figure, 9-24
 - using the \$IPT transaction ID, 9-23, 9-26
- using the download server to configure a terminal, B-21
- using the message log formatter, A-60
- using the Script Builder Tool, 11-16
- using the status monitor, A-26
- using the Trace utility, A-62

Model 200 Controller User's Manual

V

- Valid if option buttons, 11-94
- validating a terminal field, 11-93
- validation files
 - loading on JANUS devices, 11-116
 - loading on TRAKKER Antares terminals, 11-122
 - requesting from controller, 11-123
- Value field, 11-92, 11-98
- verifying that security is set, 8-49
- verifying the script file logic, 11-71
- verifying your network connections, B-7
- video port, 1-10, 2-7
- View button, 11-89, A-8
- View Hot Standby Files dialog box, A-8
 - Clear All button, A-8
 - Clear button, A-8
 - Update button, A-8
 - View button, A-8
- View Log button, D-20
- View ReadMe button, D-13
- View Results window, 11-70
- View Runtime Configuration Options dialog box, A-5
 - Run View button, A-6
- View Script Structure dialog box, 11-69
 - Collapse All button, 11-70
- viewing error messages, A-26
- viewing Hot Standby files, A-5
- viewing the error log file, A-28
- viewing the Hot Standby files, A-7
- viewing the run-time configuration, A-5
- viewing the script, 11-69
- viewing the status monitor, A-5
- Visible when data collection started? check box, 11-77, 11-78
- voltage select, 1-10
- voltage select switch, 2-4
- VT keyboard mapping, 11-106
- VT Setup dialog box, 10-12
 - Controls option buttons, 10-13
 - Cursor keys option buttons, 10-13
 - Keypad option buttons, 10-13
 - Line wrap enabled check box, 10-13

- Save as new defaults check box, 10-13
- User-Defined Key option buttons, 10-13
- VT terminal emulation, definition, G-16
- VT terminals
 - mapping keyboard to controller keyboard, 10-28
 - setting up, 10-12
- VT/ANSI screen mapping
 - limitations, 11-105
- VT/ANSI screen mapping, Data response timeout field, 11-25
- VT/ANSI terminal emulation, 1-4, 8-6
 - hot key for JANUS devices, 8-35
 - setting host parameters, 8-7
 - setting up, 8-7
 - See also* terminal emulation
- VT/ANSI terminal sessions worksheet, E-20
- VT/ANSI terminal sessions, adding, 10-8

W

- Wait for response check box, 11-55, 11-88
- WAIT_FOR command, 11-103, 11-105
- WAIT_FOR_LABEL_POS command, 11-103
- WAIT_FOR_POS command, 11-103
- worksheets
 - 3270 terminal emulation (Ethernet/token ring), E-14
 - 3270 terminal emulation (SDLC), E-16
 - 3270 terminal sessions (coaxial), E-26
 - 3270 terminal sessions (Ethernet/token ring), E-24
 - 3270 terminal sessions (SDLC), E-25
 - 5250 terminal emulation (Ethernet/token ring), E-12
 - 5250 terminal emulation (twinaxial), E-13
 - 5250 terminal sessions (coaxial), E-23
 - 5250 terminal sessions (Ethernet/token ring), E-21
 - 5250 terminal sessions (twinaxial/SDLC), E-22
 - Model 200 Controller to 9180, E-8
 - Model 200 Controller to 9180 and CrossBar, E-7
 - Model 200 Controller to CrossBar, E-9

Model 200 Controller to JANUS devices for
the 2.4 GHz RF network, E-6
Model 200 Controller to RF card, E-4
Model 200 Controller to TRAKKER Antares
terminals, E-5
network adapter cards, E-10
peer-to-peer applications, E-18
Telnet terminal emulation, E-11
VT/ANSI terminal sessions, E-20

