



**IOJ2020**  
**MULTIPLE PROTOCOL  
MEDIATION INTERFACE  
FOR SAM CONCENTRATORS  
USER'S MANUAL**



**IOJ2020 Release: 13.x**

**102 SW Orange Blossom  
Lake City, Florida  
32025-1613  
phone: 386-754-5700  
email: [sales@trdcusa.com](mailto:sales@trdcusa.com)  
<http://www.trdcusa.com>**

<b>1</b>	<b>IMPORTANT SAFETY INSTRUCTIONS .....</b>	<b>5</b>
<b>2</b>	<b>INTRODUCTION .....</b>	<b>6</b>
2.1	CLOSED USER GROUPS .....	6
2.2	HUNT GROUPS .....	7
2.3	DNS FEATURES.....	7
2.4	TACACS+ RADIUS LOGIN SUPPORT .....	7
2.5	ALARM RELAY UNIT ALARM GRID INTERFACE.....	7
2.6	X.25 MEDIATION FEATURES .....	7
<b>3</b>	<b>PHYSICAL DESCRIPTION .....</b>	<b>9</b>
3.1	POWER INTERFACES.....	9
3.2	ALARM RELAY UNIT INTERFACE.....	9
3.3	CONSOLE INTERFACE.....	9
3.4	10 BASE-T INTERFACES.....	10
3.5	USER PORTS .....	10
3.6	LEDs .....	11
<b>4</b>	<b>INSTALLATION.....</b>	<b>12</b>
4.1	IOJ2020 INSTALLATION CONSISTS OF: .....	12
4.1.1	<i>Inserting the IOJ2020 Module.....</i>	<i>12</i>
4.1.2	<i>Removing the IOJ2020 Module .....</i>	<i>12</i>
4.1.3	<i>Inserting the Trunk Module .....</i>	<i>12</i>
4.1.4	<i>Removing the Trunk Module.....</i>	<i>13</i>
4.2	CABLING THE IOJ2020 CONSOLE .....	14
4.3	DATA TRANSPORT CABLING .....	16
4.3.1	<i>User Ports.....</i>	<i>16</i>
4.4	ORDERING INFORMATION .....	16
4.5	THE 9008 RS-530/V.35/RS-422/V.11 ADAPTER .....	17
4.6	FIELD UPGRADE AND SOFTWARE REGISTRATION.....	18
<b>5</b>	<b>CONFIGURATION .....</b>	<b>21</b>
5.1	OVERVIEW.....	21
5.2	BASE CONFIGURATION .....	21
5.2.1	<i>Console Security.....</i>	<i>21</i>
5.3	USER PORT CONFIGURATION.....	21
5.3.1	<i>IP Originating Ports.....</i>	<i>21</i>
5.3.2	<i>IP Receive Ports .....</i>	<i>22</i>
5.3.3	<i>IP Closed User Groups.....</i>	<i>23</i>
<b>6</b>	<b>COMMAND REFERENCE.....</b>	<b>24</b>
6.1	BASE CONFIGURATION COMMANDS.....	24
6.1.1	<i>LOGIN.....</i>	<i>24</i>
6.1.2	<i>LOGOUT.....</i>	<i>24</i>
6.1.3	<i>CHANGE PASSWORD.....</i>	<i>24</i>
6.1.4	<i>LOCAL.....</i>	<i>25</i>
6.1.5	<i>GATEWAY.....</i>	<i>25</i>
6.1.6	<i>DOMAIN NAME SERVER.....</i>	<i>25</i>
6.1.7	<i>TACACS+ RADIUS Servers .....</i>	<i>26</i>
6.1.8	<i>HELP.....</i>	<i>26</i>
6.1.9	<i>VERSION.....</i>	<i>26</i>
6.1.10	<i>REBOOT .....</i>	<i>26</i>

6.1.11	REMOVE MODULE .....	27
6.1.12	RESTORE MODULE .....	27
6.1.13	CLEAR .....	27
6.1.14	DISPLAY MODULE MEASUREMENTS .....	27
6.1.15	VERIFY MODULE.....	28
6.1.16	HOST NAME ADMINISTRATION.....	28
6.1.17	VERIFY HOST.....	28
6.1.18	SNMP .....	28
6.1.19	INSTALL ( Software Registration ) .....	29
6.1.20	RSTPASS ( Resetting the Password ) .....	30
6.1.21	CONSOLE TIMEOUT.....	30
6.1.22	Label.....	31
6.1.23	PING .....	31
6.1.24	TraceRoute.....	31
6.1.25	DATA-BASE RESET.....	32
6.1.26	DISCONNECT CONSOLE.....	32
6.1.27	ADMINISTER SECURITY BANNER.....	32
6.1.28	CLOSED USER GROUP (CUG) ADMINISTRATION .....	32
6.1.29	VERIFY CUG.....	33
6.1.30	ASSIGNING A CUG TO THE CONSOLE.....	33
6.2	USER PORT COMMANDS .....	33
6.2.1	PORT.....	34
6.2.2	REMOVE PORT.....	42
6.2.3	RESTORE PORT.....	43
6.2.4	DISPLAY PORT MEASUREMENTS.....	43
6.2.5	VERIFY PORT.....	43
6.2.6	DISPLAY PORT STATUS.....	43
6.2.7	DISPLAY CONNECTIONS.....	43
6.2.8	DIAGNOSE USER PORT.....	44
6.2.9	DISCONNECT USER PORT.....	44
6.2.10	X.25 Protocol Analyzer Snooper .....	44
6.2.11	Configuring User Prompt.....	45
7	SNMP.....	46
7.1	SNMP VERSION 1 COMMANDS.....	46
7.2	IOJ2020 SNMP MIB VARIABLE DATABASE.....	46
7.3	SUPPORTED TRAPS .....	48
8	ALARMS.....	49
8.1	MAJOR ALARMS.....	49
8.2	MINOR ALARMS.....	49
8.3	INFO ALARMS .....	49
9	MODULE MEASUREMENTS .....	50
10	USER PORT MEASUREMENTS .....	51
11	IP-GATE PORT MEASUREMENTS.....	51
12	CLOSED USER GROUP DEMO .....	52
13	CABLING.....	53

13.1 SAM PORTS AND THE UDS 202T MODEM ..... 53

13.2 SAM PORTS AND AT&T/PARADYNE 2024 MODEM ..... 53

13.3 SAM PORTS AND GENERAL DATA COMM 201-7 MODEMS ..... 54

13.4 CABLING TO A MODEM SET ..... 54

13.5 CABLING DIRECTLY TO THE NETWORK ELEMENT ..... 54

13.6 THE SYNCHRONOUS DTE ADAPTER ..... 55

13.7 THE SYNCHRONOUS DCE ADAPTER ..... 56

13.8 THE ASYNCHRONOUS DTE ADAPTER ..... 57

13.9 THE ASYNCHRONOUS DCE ADAPTER ..... 58

13.10 THE DB9 CONSOLE ADAPTER ..... 59

13.11 THE RJ45 TO RJ45 CROSSOVER CONSOLE CABLE ..... 60

13.12 THE RJ45 TO RJ45 FULL CROSSOVER CABLE ..... 61

13.13 THE RJ45 LAN CROSSOVER CABLE ..... 62

**14 SPECIFICATIONS ..... 63**

14.1 CONSOLE PORT ..... 63

14.2 SERIAL PORTS ..... 63

14.3 10 BASE-T PORTS ..... 63

14.4 PHYSICAL DIMENSIONS ..... 63

14.5 ENVIRONMENTAL OPERATING RANGE ..... 63

14.6 POWER REQUIREMENTS ..... 63

**15 HARDWARE WARRANTY ..... 64**

**16 END-USER LICENSE AGREEMENT FOR SOFTWARE ..... 64**

16.1 SOFTWARE LICENSE ..... 64

16.2 INTELLECTUAL PROPERTY RIGHTS ..... 64

16.3 SOFTWARE SUPPORT ..... 64

16.4 EXPORT RESTRICTIONS ..... 64

16.5 LIMITED WARRANTY ..... 64

16.6 NO OTHER WARRANTIES ..... 65

16.7 LIMITATION OF LIABILITY ..... 65

16.8 SPECIAL PROVISIONS ..... 65

**17 SALES & DISTRIBUTION ..... 66**

**18 AUTHOR ..... 66**

# 1 IMPORTANT SAFETY INSTRUCTIONS



The exclamation point within an equilateral triangle is intended to alert the user to the presence of important operating and maintenance (servicing) instructions in the literature accompanying the product.

When installing, operating, or maintaining this equipment, basic safety precautions should always be followed to reduce the risk of fire, electric shock, and injury to persons, including the following:

- ❑ Read and understand all instructions.
- ❑ Follow all warnings and instructions marked on this product.
- ❑ For information on proper mounting instructions, consult the User's Manual provided with this product.
- ❑ The telecommunications interface should not leave the building premises unless connected to telecommunication devices providing primary and secondary protection.
- ❑ This product should only be operated from the type of power source indicated in the User's Manual.
- ❑ This IO module is powered directly from the **SAM** concentrator. It is not powered via either of the two Ethernet Interfaces.
- ❑ Do not use this product near water, for example, in a wet basement.
- ❑ Never touch non-insulated wiring or terminals carrying direct current or leave this wiring exposed. Protect and tape wiring and terminals to avoid risk of fire, electric shock, and injury to service personnel.
- ❑ To reduce the risk of electrical shock, do not disassemble this product. Only trained personnel should perform servicing. Opening or removing covers and/or circuit boards may expose you to dangerous voltages or other risks. Incorrect re-assembly can cause electric shock when the unit is subsequently used.
- ❑ For a SAM intended to be powered from -48 V DC voltage sources, read and understand the following:
  - ❑ This equipment must be provided with a readily accessible disconnect device as part of the building installation.
  - ❑ Ensure that there is no exposed wire when the input power cables are connected to the unit.
  - ❑ Installation must include an independent frame ground drop to building ground. Refer to User's Manual.
- ❑ This Equipment is to be Installed Only in Restricted Access Areas on Business and Customer Premises Applications in Accordance with Articles 110-16, 110-17, and 110-18 of the National Electrical Code, ANSI/NFPA No. 70. Other Installations Exempt from the Enforcement of the National Electrical Code May Be Engineered According to the Accepted Practices of the Local Telecommunications Utility.

---

## SAVE THESE INSTRUCTIONS

---

## 2 INTRODUCTION

The **IOJ2020** is a multiple protocol a mediation product. The **IOJ2020** allows the re-use of SAM concentrator endpoints on an IP infrastructure without any BNS equipment presence. The **IOJ2020** provides an integrated solution replacing the existing CEY2 I/O card of the SAMSL trunk module. This provides a very low cost mediation solution.

The **IOJ2020** supports optional enhanced vertical service feature packages such as X.25 mediation in various capacities. The feature package may be added at any time.

The **IOJ2020** provides support for 64 ports in the standard configuration. This provides a minimum cost solution for a SAM64, the most common configuration. A 128 port version of the **IOJ2020** is available to support a SAM128. The **IOJ2020-128** may be used in a SAM64 without limitations. An **IOJ2020-64** used in a SAM128 will support only TERM32 boards 1 & 2 for a total of 64 ports. If either **IOJ2020-64** or **IOJ2020-128** are used in a SAM504, then only the first two, or first four, boards respectively are supported.

The **IOJ2020** uses the serial ports resident in the SAM concentrator to provide mediation services via the TCP/IP network(s). A SAM64 has 64 serial ports, and a SAM128 has 128 serial ports. All of the serial ports are synchronous, or asynchronous. The supported speed is limited by the SAM architecture and is 19.2Kbps asynchronous, and 9.6 synchronous. Popular protocols such as Asynchronous, various Bi-Synchronous variants, HDLC, SDLC, X.25, and E2A are all supported interchangeably on a per-port basis.

In addition, vertical services typically found on Embedded Network processors have been incorporated into the devices as feature packages. For example, this allows for the direct mediation of X.25 to individual circuits over TCP connections when the X.25 vertical service is selected on a port. The **IOJ2020** supports 8 VCs per serial port with VC #0 being a control VC and 1-7 inclusive being available for user interfaces.

The **IOJ2020** is an internet protocol (IP) access device. That is, it mediates any of the supported protocols and the IP protocol suite. This includes IP, TCP, Telnet, RTP, ARP, SNMP, etc.

The **IOJ2020** provides hardware to support redundant networks in the future. At the present time, only one network interface is utilized, and the redundant networking feature package is not available.

### 2.1 CLOSED USER GROUPS

This is an important feature for protecting sensitive endpoints in a corporate-wide network without the burden of special "security servers". The **IOJ2020** provides security with an implementation of Closed User Group (CUG) membership and calling security. This is a capability similar to that provided in X.25 networks but now available for an IP infrastructure. A closed user group restricts access between **IOJ2020** ports and domains

or individual endpoints in the IP network. No external security systems of any kind are required. A CUG application example is presented at the end of this manual.

### 2.2 HUNT GROUPS

A Hunt Group is a set of ports arranged to receive calls to a common address. The **IOJ2020** provides this capability for user ports configured to receive calls from the IP network.

### 2.3 DNS FEATURES

The **IOJ2020** can maintain a set of mnemonic host names, analogous to the */etc/hosts* file on both UNIX and Microsoft Windows platforms. This allows the **IOJ2020** to perform a translation between a user-provided name and its associated IP address and TCP port number. (The use of a mnemonic name is optional, as the **IOJ2020** will always accept an IP address in its numeric form.) The **IOJ2020** also allows for the definition of an external Domain Name Server (DNS) to be used for mnemonic addresses not defined in the host table. Multiple Domain Name Servers are supported. They are searched in priority order.

### 2.4 TACACS+ RADIUS LOGIN Support

The **IOJ2020** supports up to two TACACS+ RADIUS servers for login authentication. These are a primary, and a secondary, although each is individually enabled. The TACACS+ support is for either encrypted, or clear authorization. Encryption keys may contain spaces.

### 2.5 ALARM RELAY UNIT ALARM GRID INTERFACE

The **SAM** provides a standard wiring for activation of the alarm grid should the hardware encounter a fault condition. The fault conditions include a total loss of power to the device. The alarm grid interface may be wired for normally open or normally closed connections. The **IOJ2020** supports the SAM connection to the alarm grid.

### 2.6 X.25 Mediation Features

The **IOJ2020-64** may be enabled for sixty-four instances of the X25PAD mediation application with the X25 feature package.

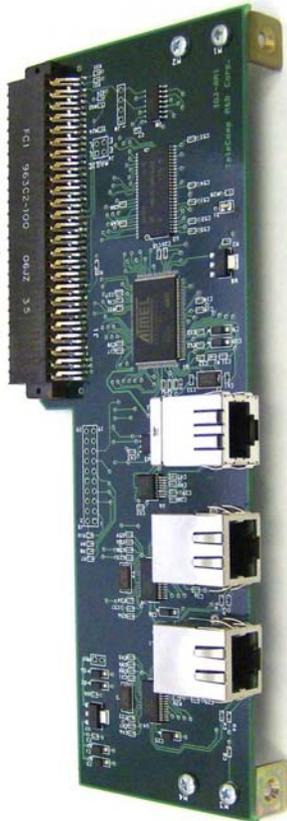
The **IOJ2020-128** may be enabled for one-hundred-twenty-eight instances of the X25PAD mediation application with the X25 feature package.

Use of the X25PAD application is exclusive of any other vertical service application or feature package.

Each of the serial ports on these devices may be connected to a (B)X.25 interface. The X25PAD mediation application allows a telnet client to interface on a per VC basis. In addition, X.25 pass-through for VC aggregation is fully supported. Each VC may be individually configured as a PAD or a PASS-THROUGH interface. A specialty interface for the MacStar operations system is supported. The *Record Boundary Preservation* protocol is supported. SVC hunt groups across X.25 lines are specifically supported allowing fault tolerant X.25 links to be established. The (B)X.25 session layer is

specifically supported via an API. Special features needed for AMA processing are all supported.

### 3 PHYSICAL DESCRIPTION



#### 3.1 POWER INTERFACES

Power for the IOJ2020 is provided by the host SAM concentrator. There are no power interfaces on the IOJ2020 module.

#### 3.2 ALARM RELAY UNIT INTERFACE

The Alarm Relay Unit connector is a three position (Failed Open, Closed, Failed Closed) terminal block labeled ALARM on the **SAM** concentrator. The terminal block connectors accommodate 10-awg to 14-awg wire.

#### 3.3 CONSOLE INTERFACE

The console interface is used for initial configuration, and for StarKeeper® II NMS monitoring on an on-going basis.<sup>1</sup>

---

<sup>1</sup> The **IOJ2020** also provides access to the console function through a TCP telnet connection via a reserved telnet server port (TCP port 1023). This service is available only when the unit is in service, and may be protected by Closed User Group membership.

This interface requires a standard RJ45-terminated twisted-pair data cable on the **IOJ2020**. It connects as a data terminating equipment (DTE) to an asynchronous device and uses RS-232C signaling. It is configured as 9600 bps, 8 bits, no parity and one stop bit.

### **3.4 10 BASE-T INTERFACES**

There are two LAN connections on the **IOJ2020**. LAN #1 is the middle connector, and LAN #2 is the lowest connector. Each has link status and activity LEDs for that interface. At the present time, only LAN #1 connector is to be used. The interface requires a standard RJ45 terminated Category 5 twisted-pair data cable. It connects to a 10/100 Hub, EtherSwitch, or router on a local LAN segment providing access to a wide-area IP based network. This port supports TCP/IP peer-level protocols (e.g. TELNET, TCP, IP, ARP, SNMP, etc.).

### **3.5 USER PORTS**

The user serial ports support both asynchronous and synchronous protocols in either DCE or DTE modes. Configuration is selectable on a per port basis. Baud rates up to the TERM32 per port limits are supported. Synchronous ports support NRZ & NRZI.

The V.35 and RS-530 interfaces require a **9008** adapter. When using a RJ45 interface, an industry standard RJ45 to DB25 adapter is utilized. The **9008** adapter provides a DB25 interface. See the cabling information contained in this user manual.

## 3.6 LEDs

The IOJ faceplate contains light emitting diodes (LEDs) used to report activity and status.

LED Function	LED Color	LED Description
PWR	Green	Unit Power Indicator
LNK (each PHY)	Green	LAN Link Indicator
COL (each PHY)	Red	LAN Collision Indicator
RX (each PHY)	Yellow	LAN Receive Packet Indicator
TX (each PHY)	Yellow	LAN Transmit Packet Indicator

## 4 INSTALLATION

This chapter contains the steps needed to install and cable the **IOJ2020**. A #1 Phillips, #2 Phillips and medium-sized flathead screwdrivers are required.

### 4.1 IOJ2020 Installation Consists of:

- Power Down the SAM Concentrator.
- Remove the Front Cover of the SAM Concentrator.
- Unseat or remove the SAMSL trunk module.
- Remove the CEY2 I/O module.
- Install the **IOJ2020** I/O Module.
- Reseat or Reinstall the SAMSL trunk module.
- Install Front Cover.
- Install Rear Cover using a CEY5 cutout panel or similar.
- Apply Power to the SAM Concentrator.

#### *When installing the IOJ2020:*

- To avoid damage to electronic components from ESD (Electro Static Discharge) always wear an ESD wrist strap.
- To prevent damage to module circuitry, always insert the I/O board before inserting its corresponding module. Never remove the I/O board before removing the module.

#### 4.1.1 Inserting the IOJ2020 Module

The I/O board plugs into the backplane at the rear of the shelf; it is held in place by shrouds on the backplane pinfield, and secured with two screws. Insert the I/O board before inserting its corresponding Trunk module..

1. Align the I/O board backplane connector with the backplane pinfield, and align the screw slots with the screw holes.
2. Slip the backplane connector onto the pins. The board should seat easily. If seating is difficult, the board may be canted or some pins may be bent.
3. Insert the screws, and tighten them securely.

#### 4.1.2 Removing the IOJ2020 Module

Remove the **IOJ2020** only for relocation, replacement, or board-type confirmation.

**Requirement: The Trunk Module in the slot corresponding to the IOJ2020 must be removed first.**

1. Disconnect all cabling to I/O board ports, labeling the cable ends if appropriate.
2. Remove the screws holding the I/O board in place.
3. Carefully rock the board as you pull it out.

#### 4.1.3 Inserting the Trunk Module

**Requirement: The IOJ2020 for the trunk module must be installed in its corresponding slot on the backplane at the rear of the shelf first.**

1. Set the mode switch on the module faceplate to Disable.

2. With the module latch extended, carefully push the module all the way into the slot. The backplane pins slip into the module receptacle.
3. Close the latch to lock the module into position.
4. Move the mode switch on the module faceplate to Enable.

#### 4.1.4 Removing the Trunk Module

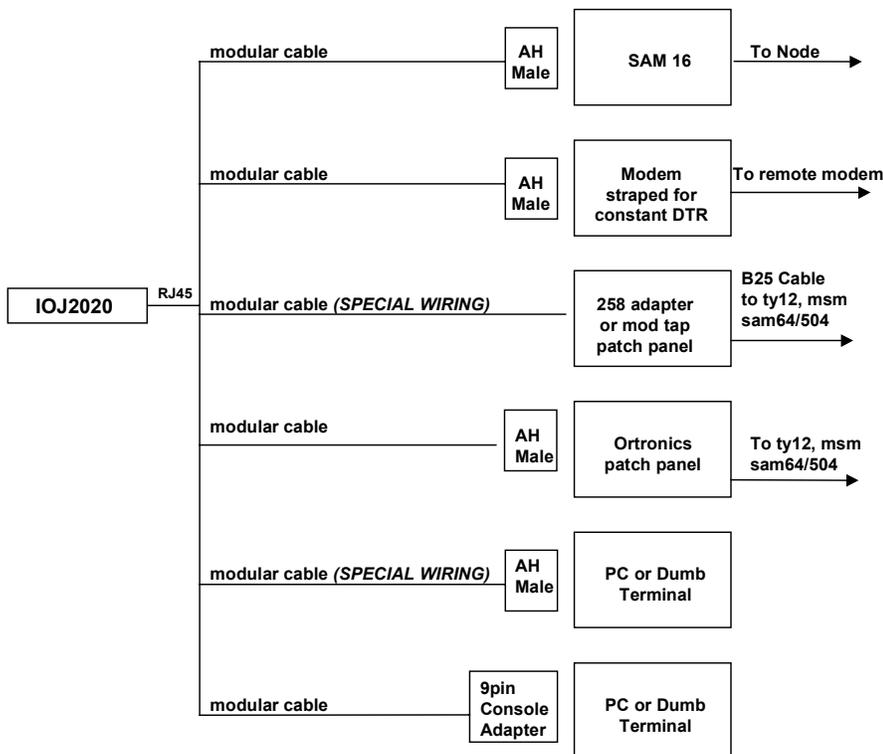
You can remove and replace a trunk module in an operating SAM without damaging the module itself or the **IOJ2020**.

**Requirement: IOJ2020 board for the module must still be in its corresponding slot on the backplane at the rear of the shelf.**

1. If the mode switch is in the Enable position, move it to Disable.
2. Open the latch on the module faceplate.
3. Pull the module straight out of the slot.

### 4.2 CABLING THE IOJ2020 CONSOLE

This section describes the options for cabling the IOJ2020 console port, to allow the IOJ2020 to be managed by a terminal, PC, dial-up modem, or asynchronous network connection. The following diagram shows the connection options:



**Important!** A modular cable with “SPECIAL WIRING” can be ordered using the table below or built using the wiring diagrams provided in this manual.

- Configure SAM, TY12 and MSM console connections as 9600 bps with 8 bits and no parity, and use a DCE type cable.
- Configure SAM and MSM console connections as type “host” and as a “pap” (permanently active port).
- Configure TY12 console connections as type “console”.

Additional instructions for configuration of SAM, TY12 or MSM asynchronous ports may be found in the appropriate BNS module reference guide.

## IOJ2020 User Manual

The following cables and adapters are available for console connections:

<b>Cable or Adapter</b>	<b>Order Information (Lucent)</b>	<b>Order Information (Reseller)</b>
modular cable (10')	407981646	modular cable (length)
modular cable ( <b>special wiring</b> )	408198133	modular cable ( <b>special wiring</b> )
AH male connector	ED5P055-31 G-139	AH male connector
Ortronics Patch Panel	406485755	Ortronics Patch Panel
258 Adapter	ED5P055-31 G(155)	258 Adapter

**4.3 DATA TRANSPORT CABLING**

**4.3.1 User Ports**

Thus, all adapters and cables used with these SAM types will apply to the unit after the **IOJ2020** is installed. Refer to the Cabling section of *Data Networking Products Synchronous/Asynchronous Multiplexer Reference*. In most cases, a standard RJ45-terminated Category 5 twisted-pair data cable can be used, with the appropriate adapter (depending on the gender) on the connector on the endpoint device.

**4.4 Ordering Information**

<b>Cable or Adapter</b>	<b>Description</b>	<b>Order Information (Lucent)</b>	<b>Order Information (Reseller)</b>
V.35(M) to DB25(F)	34-pin-M 25-pin-F	408418911	V.35(M) to DB25(F)
D8AG-F	25-pin-F mod socket, null modem wiring	ED5P055-31 G-138	D8AG-F
D8AH-F	25-pin-F mod socket	ED5P055-31 G-147	D8AH-F
D8W	Mod plug Mod plug, straight through, 3ft.	408421803	D8W
SYNC DCE-F	25-pin-F mod socket	ED5P055-31 G-150	SYNC DCE-F
SYNC DTE-F	25-pin-F mod socket	ED5P055-31 G-151	SYNC DTE-F

## 4.5 The 9008 RS-530/V.35/RS-422/V.11 Adapter

The **9008** series of adapters are used to provide balanced physical interfaces to the SAM Concentrator user ports.

The **9008** supports V.35, V.11, RS-422, and RS-530 interfaces.

The **9008** is available in DCE and DTE variants. It uses an industry standard RJ45 to connect to the SAM. It provides an industry standard RS-530 DB25 interface for the balanced physical interface. For legacy interfaces that require a Winchester 34 connection, the Black Box FA059 (DTE), and FA058 (DCE) wiring adapters may be used.

The picture below depicts a 9008-DTE with the Black Box FA059 Winchester 34 pin adapter.



## 4.6 Field Upgrade and Software Registration

The unit, when initially delivered, will need one or more software keys to activate the software. Software keys are also required when an optional individual feature packages are added to the device. Finally, when the unit is upgraded with revised software, one or more software keys are required to register the installed software and any feature packages registered for the device.

When performing an upgrade, the revised software is initially downloaded by **upgrade<sup>2</sup>** into a staging area and is not active. The software then is automatically activated by the **IOJ2020** via a **reboot**. The new software will execute normally prior to registration. However, no backup, reloads, or upgrades can be performed. Module level parameters, such as the device IP address, may be changed and activated. If a user port is taken out of service, the port cannot be restored.

The procedure for performing a software registration has been mechanized. Manual procedures are error prone and not recommended. They are no longer covered in this user manual.

The mechanized Software Upgrade Registration procedure allows simplified administration of one or more devices. When a quantity of devices are upgraded, manual software registration of each device has the potential of becoming increasingly tedious. The mechanized software upgrade registration process was designed to alleviate the problems associated with multiple device upgrades. It is also preferred for single device upgrades as it eliminates any potential for error.

The new software is downloaded to the unit via the **upgrade** command. This may be performed for one or more devices. The “-r” option to the dtupgrade command will restart the device on the new software after the download completes successfully. It is highly recommended. In the alternative, the device may be downloaded without a restart and restarted at a later time during a scheduled maintenance window. Restarting the device on the new software prior to registration is required. After the restart, the devices will continue to operate normally on the new software without registration. Some operations interface functions are inhibited pending software registration. Below is an example of a typical **upgrade** invocation. Note the use of the “-r” option as it is recommended.

```
upgrade -v -d -r -i -mIOJ2020 192.168.0.20 ioj2020.12.2
```

Mechanized registration is performed in three steps. Each of which does not require user intervention.

The steps are as follows:

---

<sup>2</sup> Utilities may be renamed to any other name. The names shown are those on the distribution.

1. The **getinfo** utility is invoked on a file containing a list of devices to be administered. This file is called the master device list file and is typically named "device.master". The master device list file may have any name and it is provided as an argument to the **getinfo** utility. The master device list may also contain devices that do not require registration. The **getinfo** utility makes inquiry of each device in the master device list and creates a device information file named "device.info" in the current directory.
2. The "device.info" file is then sent via email to [keys@trdcusa.com](mailto:keys@trdcusa.com) for registration processing.
3. A file name "device.register" file is returned via email to be used as input in the next step. A file named "device.msgs" is a text file that may be displayed or printed showing the results of the registration function.
4. The **setreg** utility is invoked and uses the "device.register" file provided as an argument. If no argument is provided, the file is assumed to be in the current directory. The **setreg** utility contacts each device that requires registration and have been assigned keys. One or more keys are installed during the dialogue.
5. The "device.info" file and the "device.register" file are deleted as they are transient and have no further value. Neither can be reused for the purpose of registration. However, the device.info file may be used for inventory reports..

The source for the registration procedure is the inventory master device list file that is created, and maintained, by the administrator using their favorite text editor.

The master device list file contains one IP address per line, with an optional TCP port, and an optional password override, to access the device. The IP address is the console *connection address*, and not necessarily the actual device IP address. Registration via the serial console is explicitly supported. Comments are allowed between addresses, and after addresses. A password override is only required if the default password of "initial" has been changed.

The master device file line format is as follows:

```
<IP ADDRESS> [<TCP PORT>] [-P<Password>] # Comment
```

An example "device.master" file follows:

```
# This is a Sample master device list file "device.master".
# Note that there is one device ( Connect IP Address ) per line.
# TCP Port Override is allowed. Registration may use the serial console.
# Password Override is allowed.
# It is OK to have devices that do not need registration listed for inventory.
# Comments in this file are preceded with a pound symbol.
# Blank Lines are treated as comments.
# Basic Line Format is as follows:
10.0.1.80 # Device at Location 'A'
192.168.7.82 # Device at Location 'B'
192.168.7.155 50001 # Example of TCP port Override.
```

192.168.7.156 50001 –pcustom1 # Example of Password Override.

Once the “device.master” file is prepared, it is used as an input to the **getinfo** utility.

```
getinfo device.master
```

This **getinfo** utility will collect information on each device in the master file. The **getinfo** utility will also make a determination if a registration is actually required. Consequently, the **getinfo** utility is also useful in performing inventory functions outside of the device registration. The output of the **getinfo** utility is a file named “device.info” that is always created in the current directory.

The file “device.info” is attached to an email and sent to the address [keys@trdcusa.com](mailto:keys@trdcusa.com). The registration procedure is performed and a file named “device.register” is attached to return email to the original sender. A messages file named “device.msgs” is also attached and may be printed as a report of the key generation function.

After receiving the “device.register” file, the **setreg** utility is invoked with the relative path of the “device.register” file as it’s sole argument. The **setreg** utility will only contact the devices that actually need registration, and for which one or more keys were successfully generated. All of the appropriate keys, including a device key and multiple per port feature package keys, are installed by the **setreg** utility. The device is not restarted and this operation may occur during normal transport operation.

A report utility **devrep** is available. The **devrep** utility uses the “device.info” file to display the inventory information. The usage is as follows:

```
devrep [-v] dt_device.info
```

If the file is not specified, the **devrep** utility attempts to use the “device.info” file resident in the current directory.

## 5 CONFIGURATION

### 5.1 OVERVIEW

The overall configuration process can be divided into three phases:  
Base Configuration – setting up the unit for IP network connectivity, console security, and other general maintenance operations such as displaying measurements and exception logs

User Port Configuration – setting up the unit to enable connections to be established between specific user ports and endpoints on IP networks, performing measurements and diagnostics on user ports

Actual command sequences will be presented throughout this section to illustrate the configuration process. Section 6 of this document should be used as the reference for console commands.

### 5.2 BASE CONFIGURATION

For IP networking, it is necessary to configure the IP address and subnet mask, the IP address of the gateway router, the IP address of an SNMP manager (optional), and the IP address of a domain name server (optional).

To illustrate an IP networking configuration, the following is a command sequence for a basic installation.

```
<IOJ2020> login passwd=initial ↵  
<IOJ2020> local ipaddr=135.17.59.165 submask=255.255.255.0 ↵  
<IOJ2020> gateway ipaddr=135.17.59.1 ↵  
<IOJ2020> restore mod ↵
```

#### 5.2.1 Console Security

Console-security parameters, i.e., an administrative login password and the (optional) timeout for automatic console logoff, will also be set up at this time.

### 5.3 USER PORT CONFIGURATION

#### 5.3.1 IP Originating Ports

User ports designated as *originating*, using the **port** command, are used to establish connections **to** endpoints on the IP network. A predefined destination (PDD), in the form of a destination IP address and TCP port number, is required for a user port configured for a synchronous protocol. A PDD is optional for an asynchronous port.

For asynchronous ports, operation from the perspective of a user is determined by whether or not a PDD has been specified. An **originating** user port which has a PDD associated with it will have that connection automatically established when the user device goes “off hook”, i.e., signals DTR, or when the user sends the attention sequence. If no PDD has been specified, the calling user is instead greeted with a **IOJ2020 Destination>** prompt where **IOJ2020** is the actual product number. The user would then enter the destination IP address plus TCP port number desired. If no TCP port number is entered, the telnet default (23) is used. The user also has the option to enter a mnemonic host name previously administered into the unit’s host table. The session is terminated when the calling user types the attention sequence.

If a Domain Name Server has been defined on the unit, the calling user may also enter a fully qualified destination name (e.g. “server.ab.company.com”) to be resolved. It is also possible to override the TCP port while still resolving the IP address. For example, the dial string “server.ab.company.com 50030” selects TCP port 50030 and then asks DNS to resolve “server.ab.company.com” to an IP address.

An **originating** port optioned for one of the supported synchronous protocols should be configured as a permanently active port (PAP), and also have a PDD specified. This will cause the desired connection to be established as soon as the port is restored to service.

The following example command sequence would set up an **originating** user port that would allow the connected endpoint to “dial” other endpoints in the IP network. It will be configured for 9600 baud, 8 bits, no parity, and no PDD defined. It will default to asynchronous operation. Assume the unit is already configured for IP networking, and in service.

```
<IOJ2020> port 2 type=orig baud=9600 dbits=8 parity=none ↵  
<IOJ2020> restore port 2 ↵
```

### 5.3.2 IP Receive Ports

A unit is accessible from anywhere in the IP network via a single IP address. That is the address administered using the **local** command, as previously shown. At this address, each user port configured as **receive**, using the **port** command, “listens” on a configured TCP port for the arrival of an incoming call **from** somewhere in the IP network. Once a call is established, the telnet over TCP protocol is used for transport. A hunt group may be established, by assigning the same TCP port number to more than one **receive** user port. Ports included in a given hunt group do not need to be contiguous.

The following example command sequence would establish a hunt group of **receive** user ports to support a modem pool reachable from anywhere in the IP network. Ports #1, #9, and #13 are to be part of the hunt group, at TCP port 51000. They will be configured for 9600 baud, 8 bits, no parity, and permanently active. Assume the **IOJ2020** itself is already configured for IP networking, and in service.

```
<IOJ2020> port 1 type=rcv hport=51000 baud=9600 dbits=8  
parity=none pap=on ↵
```

```
<IOJ2020> port 9 type=rcv hport=51000 baud=9600 dbits=8  
parity=none pap=on ↵
```

```
<IOJ2020> port 13 type=rcv hport=51000 baud=9600 dbits=8  
parity=none pap=on ↵
```

```
<IOJ2020> restore port 1 ↵
```

```
<IOJ2020> restore port 9 ↵
```

```
<IOJ2020> restore port 13 ↵
```

### 5.3.3 IP Closed User Groups

The unit has its own implementation of closed user groups (CUGs) to control access between its user ports and endpoints on the IP network. The **cug** command is used to create a closed user group, as a single IP address or range of addresses in a sub net. The **port** command allows up to 16 CUGs to be associated with a port. Calls in either direction are restricted as follows:

- A call to an IP address from an **orig**-type user port will be blocked unless the destination IP address belongs to at least one of the CUGs associated with that user port.
- A call to the TCP port number corresponding to a **receive**-type user port will be blocked unless the calling IP address belongs to at least one of the CUGs associated with the port.

Please see the CUG example at the end of this manual for a CUG application example using the **IOJ2020**.

## 6 COMMAND REFERENCE

These commands are used to configure the operation of the **IOJ2020** modules. Not all commands are visible all the time. Should the unit be logged out, only the **login** command is visible. The **reboot** command places the unit in the logged-out mode.

- ❑ Commands may be entered in upper or lower case.
- ❑ Parameters of the form **name=<value>** may use upper or lower case for **name**.
- ❑ Case is preserved for values.
- ❑ Backspace erases one character.
- ❑ Changes are cumulative.

After running a configuration command (especially those with many parameters) it is always a good idea to run the corresponding **verify** command, to check for any defaulted values which may need to be overridden.

### 6.1 BASE CONFIGURATION COMMANDS

#### 6.1.1 LOGIN

**Syntax #1: login passwd=<password>** (default password is: initial)

**Syntax #2: login**

This command is a security command required for accessing the bulk of the command set. It is only available when the user is logged off. The command has two forms, and three modes of operation.

The first syntax example provides legacy compatibility for operations systems that use that form. The password must contain between one and seven alphanumeric characters. The typed password is case sensitive.

In the second example, the password is not provided on the command line. The login command will then prompt for a password. A password given at the prompt will not be echoed. There is a timeout of approximately 30 seconds on the password prompt.

If one or more **TACACS+** RADIUS Servers are defined, the *second* form is used to log into the device. When used, a connection is made to the first available server. Prompts for "Username" and "Password" are requested. These Usernames and Passwords are administered on the **TACACS+** RADIUS server; and not on the device.

#### 6.1.2 LOGOUT

**Syntax: logout**

This command returns the unit to its logged-out mode, thus preventing unauthorized access.

#### 6.1.3 CHANGE PASSWORD

**Syntax: chgpas old=<password> new=<password> confirm=<password>**

This command allows the user to change a previously configured password. The old password is the one currently in effect. The new and confirm passwords should be identical. The password must contain between one and seven alphanumeric characters. The typed password is case sensitive. All arguments are required to complete the command.

#### 6.1.4 LOCAL

**Syntax:** local [ipaddr=<IP address>  
[submask=<submask>  
[tcpunreach=< ICMP | RESET >]

This command sets up IP networking for this unit. The **mac** (address) parameter is a fixed attribute for each unit that is set at the factory. The **ipaddr** parameter is the IP address of this unit. The **submask** parameter is the subnet mask of the LAN segment on which this unit is located, with a default value of 255.255.255.0.

The operation of the unit, when it is called to an invalid TCP port, is specified with the **tcpreach=<ICMP | RESET>** parameter. When set to **ICMP**, the caller is sent an "ICMP Port Unreachable" message. When set to **RESET**, the TCP connection is sent a TCP reset to the initiator.

#### 6.1.5 GATEWAY

**Syntax:** gateway ipaddr=<IP address>

This command identifies the IP address of the local gateway router, if any. The gateway router is the first hop packets travel through to reach a remote destination address residing on a different LAN segment.

#### 6.1.6 DOMAIN NAME SERVER

**Syntax:** dns [ ipaddr1=<IP Address> ]  
[ ipaddr2=<IP Address> ]  
[ ipaddr3=<IP Address> ]  
[ name1=<Domain Name> ]  
[ name2=<Domain Name> ]  
[ name3=<Domain Name> ]

The **dns** command is only visible when the unit is logged in.

Each **ipaddrX** field is the IP address of a Domain Name Server to be used for mnemonic addresses not defined in the host table. When all are set to 0.0.0.0, the DNS functions are disabled. The DNS addresses are used in order. If only one address is to be defined, it is required to be **ipaddr1**.

The **name1**, **name2**, and **name3** parameters are domain names. These domain names are appended to a dial string which is not fully specified for DNS purposes. For example, a name "bender.ho.lucent.com" is fully specified, so nothing is appended. A name such as "bender" would need to have a domain appended before the DNS server could resolve it. The unit will append the specified domain names in the order of **name1**

through **name3**, and send the resulting strings to the DNS server in succession until the latter is able to perform a resolution.

### 6.1.7 TACACS+ RADIUS Servers

**Syntax:** `tac < PRI | SEC > [ ipaddr=<IP Address> ]  
[ port=<TCP Port> ]  
[ key="Encryption Key" | NONE ]  
[ ENABLE ]  
[ DISABLE ]`

The **tacplus** command is only visible when the unit is logged in. The **tac** command allows the configuration of up to two **TACACS+ RADIUS** servers for the device. the servers are used as a primary server and a secondary server, although they may be individually disabled.

The **< PRI | SEC >** syntax specifies which server is to be configured. A server may not be configured while enabled

The **[ ipaddr=<IP Address> ]** specifies the IP address of the configured server.

The **[ port=<TCP Port> ]** specifies the TCP port to use when communicating with the server. The TACACS+ service defaults to TCP port 49, but any port may be specified.

The **[ key="Encryption Key" | NONE ]** specifies an encryption key to use. The Encryption key must be enclosed in double quotes, and the double quotes are not part of the key. If no encryption is desired, the value of **NONE** is used to designate unencrypted service.

The **ENABLE** command allows this server to be used for service, and prevents further configuration.

The **DISABLE** command prevents this server from being used for service, and subsequently allows configuration.

### 6.1.8 HELP

**Syntax:** `help`

This command produces a display of the entire command set and syntax available for the mode (logged out or logged in) the unit is currently in.

### 6.1.9 VERSION

**Syntax:** `ver`

This command displays the current software and database revisions of the unit and is only visible when the user is logged in. The **ver** command also displays the authorization level of the user currently logged into the administrative console. The command has no arguments. If new software has been downloaded and no reboot has been performed; the new software version is also displayed.

### 6.1.10 REBOOT

**Syntax:** `reboot [newip=<New IP Address>]  
[newmask=<New Network Mask>]`

**[newgate=<New Gateway Address>]**

This command resets the unit, which allows configured physical attributes to take effect. The command is only visible if the user is logged in. The command has optional arguments to allow the remote alteration of the network configuration. If any network configuration change is required, the user is prompted for the password as a verification check before the reboot is actually executed. After the reboot, the console interface returns to the logged-out mode.

The **reboot** command will always prompt for a password for validation purposes even if the administrator is logged at the appropriate level or higher.

## 6.1.11 REMOVE MODULE

**Syntax: remove mod**

This command is only visible when the unit is logged in. The command has no additional arguments. The command takes the unit out of service. This command must be performed before any unit-level configuration changes can occur.

The **remove mod** command will always prompt for a password for validation purposes even if the administrator is logged at the appropriate level or higher.

## 6.1.12 RESTORE MODULE

**Syntax: restore mod**

This command is only visible when the unit is logged in. The command has no additional arguments. It returns the unit to service. If any physical attribute was changed on the unit, including the MAC address, the unit will be automatically rebooted by this command.

## 6.1.13 CLEAR

**Syntax: clear < meas >**

This command is only visible when the unit is logged in. When the argument value is **meas**, the current measurements are all set to zero. No other options are allowed at this time.

## 6.1.14 DISPLAY MODULE MEASUREMENTS

**Syntax: dm mod**

This command is only visible when the user is logged in. It displays the current, unit-level measurements in a formatted report on the console (see for an itemization of the unit-level measurements at the end of this manual). **Port** information is not displayed on the unit-level report.

**6.1.15 VERIFY MODULE****Syntax: vfy mod**

This command is only visible when the unit is logged in. The command displays the unit-level configuration in a formatted report on the console.

**6.1.16 HOST NAME ADMINISTRATION****Syntax: host <host #>[name=<host name>][ipaddr=<IP address>]  
[port=<TCP port>][del]**

The units all support mnemonic destination name translation for non-PDD originating user ports. These mnemonic names are translated into an IP address and TCP port during call setup. The **host** command is used to configure the translation table

The **name** field is a mnemonic for a destination up to nine characters in length. The **ipaddr** (of the host) and TCP **port** (on the host) parameters specify the translation to be performed during call setup. If the parameter **del** is used, the entry is deleted.

**6.1.17 VERIFY HOST****Syntax: vfy host**

This command is only visible when the unit is logged in. It displays host-address configuration in a formatted report on the console.

**6.1.18 SNMP****Syntax: snmp [ ipaddr= < trap mgr addr > ]  
[ port= < trap mgr port > ]  
[ CUG=<<+|-> CUG Number > ]  
[ PUBLIC=< YES | NO > ]  
[ COMM="Double Quoted String" | NONE ]  
[ SYSCONTACT="Double Quoted String" | NONE ]  
[ SYSNAME="Double Quoted String" | NONE ]  
[ SYSLOC="Double Quoted String" | NONE ]**

This command is used to configure the IP address of the SNMP trap manager. Since traps are unsolicited alarms, an agent can take the initiative to inform the manager of the occurrence of a predefined condition. Typical conditions include the cold-start or warm-start of equipment and a link-down or link-up condition.

A single and multiple SNMP managers can access the unit. However, only one SNMP manager can be defined as the trap manager. As a result of this command, all traps will be directed to the chosen trap manager.

The **ipaddr** field defines the IP address of the SNMP manager to which the traps are to be sent.

The **port** field indicates the UDP port on that SNMP manager and defaults to the standard value of 162.

Any combination of closed user group membership may be assigned to the SNMP interface using the parameter of **cug=[+|-]<CUG Number>**. The closed user group membership is displayed on the “verify module” output. Packets which have failed the SNMP Closed User Group Test are discarded. An alarm is not presented, but the failure is counted. The number may be displayed with the “dmeas mod” command.

The unit allows setting of an SNMP community in addition to the *public* community. The *public* community is recognized when the [ **PUBLIC=YES** ] option is selected. Recognition of the public community is the default operation. When [ **PUBLIC=NO** ] is selected, the *public* community is not recognized.

The **IOJ2020** allows setting of an SNMP community in addition to the *public* community. When configured, the **IOJ2020** will respond to SNMP manager requests in that community. The **IOJ2020** will always respond to a request in the *public* community. The settable SNMP community is configured with the [ **COMM="Double Quoted String" | NONE** ] option. The community may be in any case. The double quote encapsulation is not part of the community string. The settable community may be cleared by setting it to the keyword **NONE**.

The MIB-II variables sysName, sysContact, and sysLocation may be initialized from the **IOJ2020** non-volatile database using the **SNMP** command. These variables are volatile in that they may be over-written by an SNMP manager. However, any change made by the SNMP manager will not impact the **IOJ2020** non-volatile database. Setting the value to **NONE** will clear the entries in the **IOJ2020** non-volatile database. Each field may be of 31 characters or less. The double quote encapsulation is not part of the respective variable. Any of the variables may be cleared by setting it to the keyword **NONE**.

### 6.1.19 INSTALL ( Software Registration )

**Syntax: install [ key=<software key> ]  
[ fpkey=<software key>]**

The **IOJ2020** has a unique device software key, and multiple per port feature package keys. This section is included in the user manual for completeness. Under normal circumstances, only the mechanized utilities utilize this command. It may be executed manually under an emergency situation. Depending on the device, the keys may or may not be installed by the factory. The per port feature package keys may be added at any time, and do not affect the operation of the unit. The registration procedure does not require a restart to take effect on a device running the registered software.

When executed without arguments, the **install** command will display the significant information needed to manufacture the device software key. The device IP address may also be required. No additional information is needed to create the feature package keys.

The **key=<software key>** argument allows the entry of an eight-character alphanumeric software registration that is unique to this **IOJ2020** device. If an invalid key is entered, a MINOR alarm is generated to that effect. The passwords are not altered. The **rstpass** command has been created to reset the passwords should that become necessary.

The **fpkey=<software key>** argument allows the entry of an eight-character alphanumeric software registration that is unique to a port, and software feature package, on this **IOJ2020** device for the current software build. The specific feature package referenced by the software key becomes immediately available on the port without subsequent download. The <software key> has effect on only one port. Other ports on the device are not affected. If the same software feature package is needed on multiple ports, then multiple feature package keys are applied.

The **install** command is always available.

### 6.1.20 RSTPASS ( Resetting the Password )

**Syntax: rstpass [ key=<Password Key> ]**

The **rstpass** command is a command whose function is to reset the password(s) of the device to factory default values. This function was formerly performed as part of the software registration. Breaking it out into a separate command allows the software to be registered without password updates to take place.

When invoked without arguments, the **rstpass** command will display the relevant information needed to generate the **<Password Key>**. This information is relayed to the technical support staff. The generated key is then used with the **key=<Password Key>** argument. The **rstpass** command should not be run between the time the key data is generated and the **<Password Key>** is utilized. Similarly, if the device is restarted, the resultant **<Password Key>** will not perform its intended function.

### 6.1.21 CONSOLE TIMEOUT

**Syntax: timeout [ off | < number of minutes > ]**

The **IOJ2020** console uses a three-wire interface (RD, TD, GND), and the lead state of other signals is not relevant. This would imply that the only way to change the state of the console is to explicitly log in or log out or via a reboot or reset, which forces the console to be logged out.

For users who wish the console to automatically log off after a period of inactivity, there is a console timer. The console timer defaults to the disabled condition, and may be activated by the **timeout** command. This command is only visible when the console is logged in. The **<number of minutes>** value must be between 1 and 255, inclusive. When the **IOJ2020** determines a period of inactivity of the specified time, it automatically forces the console to log off. An **INFO**-level alarm is issued at that time.

## 6.1.22 Label

**Syntax:** `label [ "Double Quoted String" | none ]`

The **label** command is used to give the command console a unique prompt. The command is visible only when logged into the **IOJ2020** administrative console. If the **label** command is invoked without arguments, the current configuration of the label is displayed. If the argument to the **label** command is the word 'none', any current label is set to a null value. If the argument to the **label** command is a double quoted string, the contents of the string becomes the application console prompt label. A console label may be up to 31 characters in length.

## 6.1.23 PING

**ping** `<IP address> [ Interval Seconds ]`

The **ping** command is only visible when the unit is logged in. The command has a single required argument, the IP address that is to be pinged.

The **ping** command formats an ICMP echo request packet which is then sent to the IP Address specified. The device with that address will issue an ICMP echo reply to the request. This is required of all IP implementations by RFC 791. If a reply is received, an informational alarm is issued on the UMI console. If no reply is received, there is a timeout message that will appear for that ICMP echo request.

The ping command issues a single ICMP echo request packet and awaits a response. The response is printed, and another ICMP echo request is issued. The operation continues until the user presses *any* character. The **[ Interval Seconds ]** argument specifies the amount of time to wait in seconds between the individual ICMP echo requests.

It should be noted that some host Internet Protocol implementations issue duplicate responses to a single ICMP request. The **ping** command will suppress duplicate replies.

## 6.1.24 TraceRoute

**trte** `<IP address>`

The **trte** command is only visible when the unit is logged in. The command has a single required argument, the IP address that is to be pinged.

The **trte** command formats an ICMP echo request packet that is then sent to the IP Address specified. The valid packet "time to live" is set to an initial value of "1". If the IP address is on the local subnet, the ICMP echo will respond immediately. If the IP address is on a different subnet, the gateway router will decrement the "time to live" upon routing the packet. When the "time to live" reaches zero, the gateway sends an ICMP "time exceeded" message to the **IOJ2020**. The **IOJ2020** then displays the gateway device, and increments the "time to live" on the next ICMP echo request packet.

This continues until the IP address is reached. The result is a display of all the intermediary gateway devices used to reach the IP address from the **IOJ2020**.

If no answer is received, each “time to live” value is tried 3 times before an increment. The timeout is 5 seconds for each attempt. The maximum number of “time to live” is set to 30 in this build of the **IOJ2020**.

Since a traceroute command can be unusually long in duration, any character sent to the console will interrupt the operation of the traceroute command.

### 6.1.25 DATA-BASE RESET

**Syntax:** `dbreset passwd=<password>`

This command returns the **IOJ2020** to the default configuration set up by the factory. The password will return to the factory default of *initial*.

The **dbreset** command will always prompt for a password for validation purposes even if the administrator is logged at the appropriate level or higher.

### 6.1.26 DISCONNECT CONSOLE

**Syntax:** `disc console`

The **disc** command is only visible when the unit is logged in. If a telnet console is connected to the **IOJ2020**, the session is terminated. This is useful in IP networks when the remote peer vanishes due to a remote reboot or a network error.

The **disc** command will always prompt for a password for validation purposes even if the administrator is logged at the appropriate level or higher.

### 6.1.27 ADMINISTER SECURITY BANNER

**Syntax:** `banner [clear] [L#="Line # Message"]`

The **banner** command is only visible when the unit is logged. It is used to administer the security banner. The default is a NULL banner. If a security banner is configured, it is displayed at each user login. The **clear** option is a shortcut to erase the entire message.

### 6.1.28 CLOSED USER GROUP (CUG) ADMINISTRATION

**Syntax:** `cug < cug num > [ ipaddr=< ip address > ]  
[ submask=< ip submask > ]`

The **cug** command is only visible when the unit is logged in. The **<CUG\_num>** parameter is the closed user group identifier used to assign the CUG to a user port (with the **port** command), or the console (with the **console** command). The **<CUG\_num>** may be a value between 1 and 16, inclusive.

A single IP address and subnet mask pair specifies each CUG. The **ipaddr** parameter is an address of an endpoint (or base address of a group of endpoints) to be allowed into the group. The **ipaddr** value *ANDed* with the **submask** value must agree with the caller's or destination's IP address *ANDed* with the same **submask** for a call to be allowed to or from a user port to which the CUG is assigned. Depending on the **submask** value, this allows an individual (submask=255.255.255.255), intermediate, or network-wide level of authorization.

Setting the **ipaddr** value to 0.0.0.0 deletes any prior configuration for the **<CUG\_num>**. A **<CUG\_num>** may not be deleted if it is currently assigned to any user port.

A list of all configured CUGs is reported via the **vfy cug** command. The list of closed user groups associated with a given user port is presented in response to the **vfy port** command.

## 6.1.29 VERIFY CUG

**Syntax:** **vfy cug**

This command is only visible when the unit is logged in. It displays the configuration of all Closed User Groups.

## 6.1.30 ASSIGNING A CUG TO THE CONSOLE

**Syntax:** **console cug=<+|->< cug num >**

The **console** command is only visible when the unit is logged in. The **<CUG\_num>** parameter is the closed user group identifier as defined with the **cug** command. A prefix of **+** will add the **<CUG\_num>** to the list associated with the telnet console. A prefix of **-** will delete the **<CUG\_num>** from the list associated with the telnet console.

If the telnet console is connected at the time a closed user group is defined, the connection must be allowed in the closed user group. If the connection is not allowed, an error message is displayed and the association will not take place.

If it is desirable to disable the telnet console entirely, a closed user group consisting only of the **IOJ2020** address may be assigned to the console. The net effect is to disallow any and all connections via the telnet console.

## 6.2 USER PORT COMMANDS

The User Port commands are used to configure the operation of the individual RS-232C ports on the **IOJ2020**. The ports are endpoints on an IP infrastructure. They may be

configured to originate or receive connections by the commands in this section. When used with a “built in” X.25 mediation interface, the connectivity configuration is not required.

### 6.2.1 PORT

**Syntax:** port < PortNum > [ type = <orig | rcv | X25 > ]  
 [ pdd = < PDD DNS destination address > ]  
 [ dest = < ipaddr > ]  
 [ dport = <tcp port > ]  
 [ hport = <tcp port > ]  
 [ peer = <IP-DSU Peer IP Address> ]  
 [ prot = < protocol > ]  
 [ dx = < dce | dte > ]  
 [ baud = < baud rate > ]  
 [ enc = < nrz | nrzi > ]  
 [ ccar = < on | off > ]  
 [ swcar = <on | off > ]  
 [ pap = < on | off > ]  
 [ fill = < mark > | < flag > ]  
 [ dbits = < 5 | 6 | 7 | 8 > ]  
 [ parity = < even | odd | none > ]  
 [ stop = < 1 | 1.5 | 2 ]  
 [ attn = < 1brk | 2brk | none | char > ]  
 [ flow = < xon | hw | none > ]  
 [ cug = [+ | - ] < cug num > ]  
 [ crfix = < trans | nonnull > ]  
 [ crlf = < trans | nolf > ]  
 [ PDDonCR = < on | off > ]  
 [ crypt = < on | off > ]  
 [ loopback = < OFF | NET | PORT | BOTH > ]  
 [ comment = "user comment" ]  
 [ moveto=<New Port Num> ]  
 [ copyto=<Port Number Range> ]  
 [ x25dx=< DTE | DCE > ]  
 [ x25win=<LAPB Tx Window Size> ]  
 [ x25t1=< LAPB T1 Timer > ]  
 [ x25n2=< LAPB N2 Retry Counter > ]  
 [ x25dar=< ON | OFF > ]  
 [ x25pass=< OFF | DFLT | "Password String" > ]  
 [ x25xid=< XID Link ID > ]  
 vc=<Range> [ vcsvc=< PAD | PASS | ISO  
 RBP | MAC | SESS > ]  
 [ vcckt=< SVC | PVC > ]  
 [ vcwin=<VC Tx Window> ]  
 [ vcpkt=< 128 | 256 | 512 | 1024 > ]  
 [ pvcrest=< ON | OFF > ]  
 [ pvcrstlnk=< ON | OFF > ]

```

[ svctclass=< NONE | Throughput > ]
[ padecho=< ON | OFF > ]
[ paderase=< NONE | BS | <Hex Byte> ]
[ padidle=< #X.3 Ticks > ]
[ padbreak=< NONE | INTR |
                RESET | BRKIND > ]
[ padparity=< TRANS | EVEN | ODD > ]
[ padcrif=<NONE | RMT | VC | BOTH>]
[ padfwd=<NONE | CR | CRDROP |
                SEMI | ALL | GRPx    > ]
[ padcmap=< ON | OFF > ]
[ padapi=< RAW | TELNET > ]
[ PADCUG=[+|-]<CUG Number> ]
[ calling=< DNIC+NTN > ]
[ called=< DNIC+NTN > ]
[ ulen=< UData Length > ]
[ udata#=< HEX BYTE > ]
[ ext_calling=< OSI NSAP >]
[ ext_called=< OSI NSAP >]
[ hport=<VC Hunt Group TCP Port>]
[ vccom="User Comment" ]
    
```

This command configures an individual user port. The **<PortNum>** parameter is a number in the range of 1 through the N that corresponds to the RS-232C user port being configured. The value N is sixty-four for an **IOJ2020-64**, and one-hundred-twenty-eight for an **IOJ2020-128**.

When a port uses TCP/IP for communications, it is either a port which waits for an incoming call (**type=rcv**), or an originator of a call (**type=orig**). The (optional) PDD for an **orig-type** port is defined by **dest=<ipaddr>** and **dport=<tcp\_port>**. A caller on an originating port without PDD information configured will be presented a **IOJ2020 Destination>** prompt for “dialing”.

A port with (**type=x25**) is internally connected to a corresponding instance of the X25PAD application. One or more of the various X25PAD feature packages is required for this option. The X.25 options then become available for this port. The virtual circuits for the X.25 ports will default to a TCP port number of 30,000 for the 1<sup>st</sup> port plus the virtual circuit number (e.g. 30001, 30002, ...). Each subsequent X.25 port will add 200 to this value. The second X.25 port begins at 30200, the third at 30400 and so on.

When the PDD destination information is specified with the **pdd=<DNS destination address>** option, the **IOJ2020** uses the specified DNS server to resolve the name. A DNS server address must be entered prior to configuration of any of the ports. The **pdd** parameter is mutually exclusive with specifying the IP address directly via the **dest** and

**dport** parameters. A value of none (i.e. **pdd=none**) will clear the DNS destination address.

A **rcv-type** user port is assigned a default TCP port number of 50000 + user port number, i.e., 50001 to 50016. The port may then be addressed uniquely at that address. However, when a specific TCP port number is specified via the **hport=<tcp\_port>** option, it is used in lieu of the default value. Multiple ports may share the same TCP port number, to define a **hunt group**. When a connection is directed to a TCP port number associated with a **hunt group**, the **IOJ2020** selects the next available physical port by round robin. The **hport** parameter only applies to **rcv-type** ports.

The **hport** option also operates on virtual circuits to create hunt groups. This operation is selected when the **hport** option is used on an X.25 port. The virtual circuits must be specified. The virtual circuits need not be contiguous, and may span X.25 ports. For example, a 21 virtual circuit hunt group may be created by placing 7 virtual circuits each from three ports into the same TCP port number hunt group.

The **prot=<protocol>** option defines the protocol used by the port. It may take on the values of **Raw**, **Async**, **HDLC**, **SDLC**, **EBSC** (EBCDIC BiSync), **ABSC** (Ascii BiSync), **UNI** (Uniscope BiSync), **ALC** (ALC BiSync), **DDCMP**, or **VIP** (VIP 7600 BiSync). The default protocol is **Async**. The **Raw** protocol is asynchronous, without the benefit of Telnet RFC encapsulation. It is used for direct TCP connections to the user ports. Please send email to the author at [angel@trdcusa.com](mailto:angel@trdcusa.com) or via telephone @ (386) 754-5700, with any other protocol requests.

The **dxe=< DCE | DTE >** option specifies the clocking and signaling mode of the port. The default value is DCE.

When the protocol is asynchronous, a **dxe** value of **DCE** implies that the port is operating as a modem device. It will assert CTS when presented with RTS. A value of **DTE** for the asynchronous protocol implies that the port is operating as a 2-wire DTE. When there is data available to send, it will assert RTS and wait for CTS before sending data. Please note that a four wire DTE interface should be configured as **DCE** even though it uses a DTE asynchronous connector.

When the protocol is synchronous (e.g. SDLC), a **dxe** value of **DCE** implies that the **SAM** should generate the clock signals. This would require the standard synchronous DCE cable adapter. A **dxe** value of **DTE** implies that the **IOJ2020** should accept the clock signals presented on the port. This would require the standard synchronous DTE cable adapter. When the protocol uses a recovered clock instead of a separate clock lead (e.g. SDLC NRZI two wire), the **dxe** value operates like the asynchronous protocol described above since external clocking is not necessary. The appropriate asynchronous adapters should be used.

The **enc=<NRZ|NRZI>** option specifies the physical encoding of the line. The default is Non-Return to Zero (NRZ).

The **ccar=<ON|OFF>** field defines constant carrier. This is an option in which the CD (or DTR if the port is a DTE) EIA signal is maintained asserted regardless of call status. The constant carrier feature is mutually exclusive with switched carrier.

The **swcar=<ON|OFF>** field defines a switched carrier for the SAM port. This is an option in which the CD EIA signal is switched consistent with two-wire modem operation. It is designed only for DCE operation. That is, CD is active just prior to and during data transmission to the connected device. It is inactive otherwise without regard to the state of the TCP connection. The switched carrier also implies a true “two wire” circuit. The **SAM** will not send data to the device while the device has been given clearance to send data via the CTS EIA lead. The **SAM** port will not give clearance via the CTS EIA lead in response to an RTS assertion request while it is sending data with CD asserted. The switched carrier feature is used only with the E2A protocol, and then only for specific devices requiring a true “two wire” functionality. The switched carrier feature is mutually exclusive with the constant carrier feature.

The **pap=<ON|OFF>** field defines a permanently active port. The default value is OFF. Setting this flag ON means that the port is ready to communicate regardless of its DTR (or DCD if the port is a DTE) EIA signal.

The **fill=<mark|flag>** option indicates what kind of line fill should be applied between frames in the **HDLC** or **SDLC** protocols.

The **baud=<baud\_rate>** determines the speed of the line. It is not required for synchronous DTE ports since the clocking is derived from the line. For asynchronous ports, the allowed values are 75, 110, 150, 300, 600, 1200, 1800, 2400, 4800, 9600, 14400, and 19200. For synchronous DCE ports, the same rates apply up to and including 9600 baud. The default value is 9600.

The **dbits=<5|6|7|8>** option specifies the number of data bits in an asynchronous word. It excludes start, stop, and parity bits.

The **parity=<even|odd|none>** option specifies the parity of an asynchronous word.

The **stop=<1|1.5|2>** option determines the number of stop bits for asynchronous ports.

The **attn=<1BRK|2BRK|NONE|char>** sets the attention character. This is a character that when typed will interrupt the local session. The **1BRK** option specifies a single break. The **2BRK** option specifies two breaks within a short period. The **NONE** option specifies that no attention character is defined. Finally, any ASCII character may be used as the attention. It should be entered in decimal ASCII representation.

The **flow=<XON|HW|none>** option determines the flow control for the port. The **XON** option uses XON/XOFF in-band flow control characters. The **HW** option uses the CTS and RTS leads for flow control. All flow control is disabled when the “**none**” option is used.

The **cug=[+]-<CUG\_num>** option allows the inclusion or deletion of a Closed User Group in the list of CUGs assigned to the user port. The “+” will add the <CUG\_num> to the CUG list. The “-” is used to delete the <CUG\_num> from the list.

The **crfix=< TRANS | NONULL >** option accommodates an anomaly in some early variants of telnet implementation on UNIX systems, which insert a NULL character in the data stream after a carriage return. Most end devices are not affected by this NULL character. However, some devices (e.g. the BNS control computer) have erroneous operation if these characters are received. The value **TRANS** indicates transparent operation, where all data received by the **IOJ2020**, including a NULL after a carriage return, is forwarded to the end device. The value of **NONULL** removes a NULL character immediately following a carriage return. No other NULL characters are affected. The default operation is transparent, and the **crfix** option may only be specified if the protocol selected is asynchronous.

The **crlf=< TRANS | NOLF >** option is used to strip LF (line-feed) after CR (carriage return) in the asynchronous protocol.

The **PDDonCR=< ON | OFF >** option is used in conjunction with the **DEST**, and **DPORT** options to define a permanent destination which is not automatically dialed. The **IOJ2020** will display a message that the user should enter a “carriage return”. Once entered, the permanent destination is defined. This option is used for a secure connection via a network security server. Please note that making the port permanently active with the **PAP** command will over-ride this feature.

The **comment="User Comment"** option allows the administrator to post a note related to the user port. The string is double quoted, and may have any length up to sixteen characters between the quotes. Per Port comments can be changed even if the user ports are "in service".

The **moveto=<New Port Number>** option allows the administrator to move this configured port to another port number without re-entering the configuration. The original port number configuration is then deleted.

The **copyto=<Port Number Range>** option allows the administrator to replicate this port exactly on other ports. The <Port Number Range> may cross the port being replicated.

The **x25dxe=<DTE | DCE>** option is available only when the port is of type **x25**. It allows changing the logical sex of the interface. Each X.25 interface needs a single DTE and a single DCE. Normally, the network side is the DCE. For some network elements, the converse is true. An example is the LTS, and a #5ESS IOP.

The **x25win=<LAPB Tx Window>** option is available only when the port is of type **x25**. It allows changing the number of frames sent without acknowledgement. The default number is seven per the specification. The <LAPB Tx Window> may have a value of one through seven inclusive.

The **x25t1=<T1 Timer Value>** option is available only when the port is of type **x25**. It allows changing the X.25 LAPB T1 protocol timer.

The **x25n2=<N2 Retry Counter>** option is available only when the port is of type **x25**. It allows changing the number of retries at the LAPB layer for protocol operations.

The **x25dar=< ON | OFF >** option is available only when the port is of type **x25**. When enabled, the **BX.25** link layer will be immediately restarted should the peer disconnect. When disabled, the **B)X.25** link layer remains in disconnect mode pending further action from the peer. The option was added for TR-TSY-000385 AMATPS interfaces.

The **x25pass=< OFF | DFLT | “Password String” >** option is available only when the port is of type **x25**. This option allows the setting of a **BX.25** I-Frame Password for the link. When set to **OFF**, the link does not issue nor does it expect an I-Frame Password. When the **DFLT** option is set, the TR-TSY-000385 AMATPS passwords are installed. Otherwise, a custom password may always be configured as a double quoted string. Specifics of this interface may be found in **BX.25** Issue 3.

The **x25xid=< XID Link ID >** option is available only when the port is of type **x25**. This option allows the setting of the XID link ID to be used when BX.25 I-Frame Passwords are exchanged. If the **x25pass** option is enabled and the **x25xid** has not been set, the default link id is 4. Specifics of this interface may be found in **BX.25** Issue 3.

The **vc=<Virtual Circuit Number>** is a modifier on the port number when the port is of type **x25**. It is required for configuration options that relate to an individual virtual circuit.

The **vcsvc=< PAD | PASS | RBP | MAC | ISO | SESS >** option determines the type of service for a virtual circuit. The VC must have been specified on the command line. When set to the value of **PAD**, the virtual circuit is terminated in an X.3 PAD. When a value of **PASS** is selected, an X.25 pass-through service is selected. The latter is used for VC aggregation. When a value of **MAC** is selected, a special interface for the MacStar operation system is used. When a value of **RBP** is selected, the *Record Boundary Preservation* protocol is selected. The **ISO** value selects ISO X.25 used with FTAM implementations. The **SESS** value selects the (B)X.25 session layer interface.

The **vcckt=< SVC | PVC >** option determines the operation of a virtual circuit. When the **PVC** option is selected, connections will not generate call setup or call clear X.25 packets. However, the **IOJ2020** will still respond to call setup and call clear packets generated by the attached device. When the **SVC** option is selected, a TCP connection to the virtual circuit will generate a call setup X.25 packet transaction. A disconnect will generate a call clear transaction. If the X.25 device clears the call, the TCP connection will also be dropped.

The **vcwin=<VC Tx Window Size>** specifies the packet layer window size to be used for transmission purposes on the affected VCs. The valid values are one through seven inclusive. The VC must have been previously specified on the command line.

The **vcpkt=< 128 | 256 | 512 | 1024 >** specifies the packet size boundary upon which a packet is generated when the selected forwarding condition is not met. Any such packet will have the “More” bit set to indicate the transaction is not complete.

The **pvcreset=<ON | OFF >** option specifies the operation of a PVC when a connection is made. When set to **ON**, the PVC is issued a RESET upon a user connection. When set to **OFF**, the PVC continues with it’s previous state. Some legacy devices cannot tolerate a PVC RESET and this option allows interoperability. The default is to have RESET enabled (ON).

The **pvcrstlnk=<ON | OFF>** option specifies the operation of the link supporting the PVC when a connection is made. When set to **ON**, the entire link is issued a RESTART upon a connection to the PVC. The PVC itself may also get a RESET depending on the setting of the **pvcreset** option. When set to **OFF**, the link behaves per the relevant (either **X.25** or **BX.25**) specification and no RESTART is issued at user connect. The **pvcrstlnk=on** option also switches the DCD lead as the BX.25 link layer is controlled. This yields a more effective simulation of a dynamic modem connection as is required by some legacy devices. This option is provided strictly for interoperability with select legacy devices. As a general rule, it should remain in the **OFF** condition. The default is the **OFF** condition.

The **svctclass=< NONE | Throughput >** option specifies a throughput class declared on X.25 call connect, and call accept packets. The throughput class is the same in both transmit and receive directions. As a general rule, it should always be set to **NONE** such that no limiting throughput class is established. All specification allowable values for throughput class are supported. These range from 75bps to 48000bps inclusive. The option is provided for interface to devices that require a throughput class to be explicitly negotiated.

The **padecho=< ON | OFF >** refers to reference #2 in the X.3 parameter list. When set to **OFF**, the PAD will not echo characters back to the IP endpoint. When set to the value of **ON**, all characters are to be echoed back to the IP source.

The **paderase=< NONE | BS | <HEX BYTE> >** option specifies reference #16 in the X.3 parameter list. It is used with manual telnet connections to an X.25 VC. It sets the buffer editing “erase” character. When the special “erase” character is received by the X25PAD for a specific virtual circuit, the previous character in the packet accumulation buffer is deleted. If the **padecho** option was also enabled, a “Backspace Blank Backspace” sequence is emitted to the user. When the **paderase** option is set to **NONE**, the PAD will not have a special “erase” character. When the value is **BS**, it is set to the ASCII backspace character 0x08. Otherwise, any character may be entered as a hexadecimal byte in 0xXX notation. This option is only valid on X.25 virtual circuits configured with the PAD interface.

The **padfwd=<NONE | CR | CRDROP | SEMI | ALL | GRPx>** option specifies reference #3 of the X.3 parameter list. This is the forwarding condition (outside the PAD timer) which will forward data towards the X.25 virtual circuit. A value of **NONE** indicates that there are no character forwarding conditions. A value of **CR** indicates that a carriage

return will forward any accumulated data (including the carriage return). A value of **CRDROP** indicates that a carriage return will forward any accumulated data (but not including the carriage return). A value of **SEMI** indicates that a semicolon will forward any accumulated data including the semicolon. A value of **ALL** indicates that all data is to be forwarded immediately. The **ALL** option has the effect of generating single user character X.25 packets on this virtual circuit. The **GRP<sub>x</sub>** values specify selected groups of forwarding characters. **GRP1** forwards on ESC, BEL, ENQ, and NAK. **GRP2** forwards on DEL, CAN, DC2. **GRP3** forwards on ETX, EOT. **GRP4** forwards on HT, LF, VT, and FF. Multiple forwarding conditions are allowed simultaneously. Setting **padfwd** to a value aggregates with the previous value of **padfwd**. The **padfwd=none** is required to clear the forwarding conditions.

The **padidle=<#X.3 ticks>** parameter refers to reference #4 of the X.3 parameter list. This is the time forwarding condition. When it expires, it will forward any data collected to the X.25 circuit. The timer is reset to the specified timer value whenever a forwarding condition is reached. The value is based on ticks of 1/20<sup>th</sup> of a second each per the X.3 specification.

The **padbreak=< NONE | INTR | RESET | BRKIND >** parameter refers to reference #7 of the X.3 parameter list. This is the action to be taken when a break indication ( a standard Telnet encapsulated value ) is received from the remote IP endpoint. A value of **NONE** will ignore the break, and it is deleted from the data stream. The value of **INTR** will generate an X.25 interrupt packet. The value of **RESET** will generate an X.25 virtual circuit . The value of **BRKIND** will generate an X.29 "indication of break" message on the X.25 virtual circuit.

The **padparity=< TRANS | EVEN | ODD >** parameter is not present in the X.3 parameter list. It allows special parity treatment for interface to network elements that require parity. The default value is transparent operation. The value of **TRANS** sets the operation to be transparent. When the parity treatment is transparent, the data is not modified in either direction. The value of **EVEN** sets the operation to be even parity towards the (B)X.25 device, and stripped parity towards the TELNET. The value of **ODD** sets the operation to be odd parity towards the (B)X.25 device, and stripped parity towards the TELNET.

The **padcrlf=<NONE | RMT | VC | BOTH>** parameter refers to reference #13 of the X.3 parameter list. This is the action to be taken when a CR is received in the data stream from the remote IP endpoint. A value of **NONE** indicates that there is to be no LF (line feed) insertion. A value of **RMT** will insert an LF following a CR whenever it is sent towards the remote IP endpoint. A value of **VC** will insert an LF following a CR whenever it is sent towards the X.25 virtual circuit. A value of **BOTH** will insert an LF following a CR in either direction.

The **padcmap=< ON | OFF >** option provides the automatic case mapping from lower case to upper case. When the option is set to **ON**, all lower case characters are automatically converted to upper case. When **OFF**, no transformations are performed.

The **padapi=< TELNET | RAW >** option provides a means of selecting the PAD virtual circuit to use **raw** protocol. The **raw** protocol is essentially asynchronous, but without the benefit of Telnet RFC encapsulation. It is used for applications that do not implement the Telnet RFC. The default for this option is to use the Telnet encapsulation.

The **padcug=[+]-<CUG Number>** parameter allows the virtual circuit connection to be protected by closed user group membership. The closed user group feature is significant only for PAD service. The closed user group address entries are defined with the **cug** command. Any or all closed user group entries may be assigned with a virtual circuit.

The **calling=<DNIC+NTN>** parameter is used to specify the “calling address” on an SVC call setup packet. Most devices do not require a calling address. This option allows the specification for a device which does require same.

The **called=<DNIC+NTN>** parameter is used to specify the “called address” on an SVC call setup packet. Most devices do not require a called address. This option allows the specification for a device that does require same.

The **ext\_calling=<OSI NSAP>** parameter is used to specify the “extension calling address” on the SVC call setup packet of an OSI X.25 connection. The option may be deleted with the value ‘delete’. This parameter is only required with the OSI X.25 interface.

The **ext\_called=<OSI NSAP>** parameter is used to specify the “extension called address” on the SVC call setup packet of an OSI X.25 connection. The option may be deleted with the value ‘delete’. This parameter is only required with the OSI X.25 interface.

The **ulen=< UDATA Length >** parameter specifies the length of the user data field to be used in an SVC call setup packet. The default is one byte of value 0xC1.

The **udata#=< Hex Byte >** parameter allows modification of the user data field to be used in an SVC call setup packet. The **#** may be a number in the range of one through sixteen. The **< Hex Byte >** is of the form 0xXX.

The **vccom="User Comment"** parameter allows the specification of a comment line for the one or more VCs. The comment may be up to 32 characters in length, and may contain spaces and some special characters. It may not contain an embedded double quote. Comments are allowed in upper and lower case and may be changed with the port in service. Once entered, the comments are displayed on the port verify.

### 6.2.2 REMOVE PORT

**Syntax: remove port < portnum > < all > < range >**

This command is only visible when the unit is logged in. The command takes a user port out of service, and must be performed before any port-level configuration changes can occur. The **<PortNum>** parameter may be a number in the range 1 through the number of ports on the **IOJ2020**. The **<all>** parameter removes all the serial ports. The **<range>** parameter removes a sequential range of ports.

## 6.2.3 RESTORE PORT

**Syntax: restore port < portnum > < all > < range >**

This command, only visible when the unit is logged in, returns a user port to service. The **<PortNum>** parameter may be a number in the range of 1 through the number of serial ports on the **IOJ2020**. The **<all>** parameter restores all the ports. The **<range>** parameter restores a sequential range of ports.

## 6.2.4 DISPLAY PORT MEASUREMENTS

**Syntax: dmeas port < portnum | all | range >**

The **dmeas (dm) port** command is only visible when the unit is logged in. It displays the current port-level measurements for the RS-232C port specified by **<portnum>**, in a formatted report on the console. The **<portnum>** parameter may be a number in the range 1 through the number of ports on the **IOJ2020**. The **<all>** parameter will display the measurements on all ports. The **<range>** parameter is in the form of “start-end”, and will display the measurements of the ports in that sequential range inclusive.

## 6.2.5 VERIFY PORT

**Syntax: vfy port < portnum | all |range >**

This command is only visible when the unit is logged in. It displays the configuration of the port number specified. The **<portnum>** parameter may be a number in the range 1 through the number of ports on the **IOJ2020**. The **<all>** parameter will verify all ports. The **<range>** parameter will verify a sequential range of ports.

## 6.2.6 DISPLAY PORT STATUS

**Syntax: deia < portnum >**

This command is only visible when the unit is logged in. It displays the EIA status of the port number specified. The **<portnum>** parameter may be a number in the range 1 through the number of ports on the **IOJ2020**.

## 6.2.7 DISPLAY CONNECTIONS

**Syntax dconn < <Port# Range> | ALL >**

The **dconn** command is only visible when the unit is logged in. The command displays the connections between user ports and their destinations. The service state of all ports

currently 'In Service' are displayed. For X.25 ports, the connection state of the virtual circuits are displayed. The **dconn** command takes one argument to limit the report size. The argument may be the port number, a range of port numbers, or the value of **ALL** to specify all connections.

### 6.2.8 DIAGNOSE USER PORT

**Syntax: diag port < portnum > < int | ext | all >**

The **diagnose (diag)** command is only visible when the unit is logged in. The command accepts arguments to specify a user port on which to perform diagnostics. Two types of diagnostics are available. The internal port diagnostic checks the operation of the hardware exclusive of the cabling, connectors, and drivers. The external port diagnostic checks the operation of everything, including the attached cable. The port **must** be out of service to diagnose.

The **<port\_num>** parameter specifies the RS-232C user port. The diagnostic type is either **INT** for the internal test, **EXT** for the external test, or **ALL** for both the internal and external tests.

### 6.2.9 DISCONNECT USER PORT

**Syntax: disc port < portnum >**

The **disc** command is only visible when the unit is logged in. If an IP stand-alone port is in service, any existing circuit established via the port will be dropped. This is useful in IP networks when the remote peer vanishes due to a remote reboot or a network error. It is essentially equivalent to the **remove port + restore port** command sequence.

The **disc** command will always prompt for a password for validation purposes even if the administrator is logged at the appropriate level or higher.

### 6.2.10 X.25 Protocol Analyzer Snooper

**Syntax: snoop <X.25 Port #> <L2 | OFF | <VC Range>> [ verbose ]**

The **snoop** command is only available to X.25 ports. It implements the X.25 protocol analyzer. The **snoop** command may be invoked multiple times with the results aggregating. Every time the **snoop** command is invoked, the relative timestamp is set to zero. The **<x.25 Port #>** is the number of the port to be snooped. The port must be of **type=x25**. The parameter of **L2** will select snooping at the LAPB layer. Both transmit and receive directions will be displayed. The parameter of **<VC Range>** allows the specification of one or many virtual circuits on the port. This snooping is performed at the packet layer.

Normally, the packet control and size is displayed in short format. If all of the bytes in the packet are desired, the **[ verbose ]** option may be specified.

In order to disable snooping on one or more components of an X.25 port, the **OFF** option is specified. The **OFF** parameter will disable snooping at all levels on the specified X.25 port.

## 6.2.11 Configuring User Prompt

**Syntax:** `uprompt [ "User Prompt" | STD ]`

The **uprompt** command supports custom user prompting for ports of **type=orig**. In the default condition, a user is prompted with a **IOJ2020 Destination>** prompt string where **IOJ2020** is the actual device number. If the **uprompt** command is issued with a double quoted string, that string is presented as the user prompt without the double quotes. The maximum size of the prompt string is 31 characters. The value of **STD** returns the **IOJ2020** user prompt to its default, or standard, configuration.

## 7 SNMP

The **IOJ2020** SNMP V1 agent supports a multitude of SNMP MIB variables, SNMP *Traps*, and *Set* and *Get* operations.

### 7.1 SNMP Version 1 Commands

Command	Operational Result
Get	Requests the values of one or more Management Information Base (MIB) variables.
GetNext	Enables MIB variables to be read sequentially, one variable at a time.
Set	Permits one or more MIB values to be updated.
GetResponse	Used to respond to a Get, GetNext, or Set.
Trap	Indicates the occurrence of a predefined condition.

### 7.2 IOJ2020 SNMP MIB Variable Database

RO = Read-Only Variable

R/W = Read/Write Variable

SIV = Storage is Volatile

MIB Variable Number	Name	MIB	Console Equivalent	Access	Notes
1.3.6.1.2.1.1.1.0	SysDescr	MIB-II	Banner Message	RO	
1.3.6.1.2.1.1.2.0	SysObjectID	MIB-II	None	RO	
1.3.6.1.2.1.1.3.0	SysUpTime	MIB-II	None	RO	
1.3.6.1.2.1.1.4.0	SysContact	MIB-II	None	R/W	SIV
1.3.6.1.2.1.1.5.0	SysName	MIB-II	None	R/W	SIV
1.3.6.1.2.1.1.6.0	SysLocation	MIB-II	None	R/W	SIV
1.3.6.1.2.1.1.7.0	SysServices	MIB-II	None	RO	
1.3.6.1.2.1.4.1.0	IpForwarding	MIB-II	None	RO	
1.3.6.1.2.1.4.2.0	IpDefaultTTL	MIB-II	None	RO	
1.3.6.1.2.1.4.3.0	IpInReceives	MIB-II	Number of Ethernet Pkts Rcvd	RO	
1.3.6.1.2.1.4.4.0	IpInHdrErrors	MIB-II	Nbr of Packets w/Header Errs	RO	
1.3.6.1.2.1.4.5.0	IpInAddrErrors	MIB-II	Nbr Rx Packets w/Wrong Addr	RO	
1.3.6.1.2.1.4.6.0	IpForwDatagrams	MIB-II	None	RO	
1.3.6.1.2.1.4.7.0	IpInUnknownProtos	MIB-II	Nbr of Packets w/Unk Protocol	RO	
1.3.6.1.2.1.4.8.0	IpInDiscards	MIB-II	Nbr of Packets Disc due to Resource	RO	
1.3.6.1.2.1.4.9.0	IpInDelivers	MIB-II	Inferred from DMEAS counters	RO	
1.3.6.1.2.1.4.10.0	IpOutRequests	MIB-II	Number of Device Frames Transmitted	RO	
1.3.6.1.2.1.4.11.0	IpOutDiscards	MIB-II	Nbr of Port frames Disc due to Resource	RO	
1.3.6.1.2.1.4.12.0	IpOutNoRoutes	MIB-II	None	RO	
1.3.6.1.2.1.4.13.0	IpReasmTimeout	MIB-II	None	RO	

1.3.6.1.2.1.4.14.0	IpReasmReqds	MIB-II	None	RO	
1.3.6.1.2.1.4.15.0	IpReasmOKs	MIB-II	None	RO	
1.3.6.1.2.1.4.16.0	IpReasmFails	MIB-II	None	RO	
1.3.6.1.2.1.4.17.0	IpFragOKs	MIB-II	None	RO	
1.3.6.1.2.1.4.18.0	IpFragFails	MIB-II	None	RO	
1.3.6.1.2.1.4.19.0	IpFragCreates	MIB-II	None	RO	
1.3.6.1.2.1.4.21.0	IpRoutingDiscards	MIB-II	None	RO	
1.3.6.1.2.1.5.1.0	IcmpInMsgs	MIB-II	None	RO	
1.3.6.1.2.1.5.2.0	IcmpInErrors	MIB-II	ICMP Errors	RO	
1.3.6.1.2.1.5.3.0	IcmpInDestUnreach	MIB-II	None	RO	
1.3.6.1.2.1.5.8.0	IcmpInEchos	MIB-II	Nbr of Pings	RO	
1.3.6.1.2.1.5.9.0	IcmpInEchoReps	MIB-II	None	RO	
1.3.6.1.2.1.6.1.0	TcpRtoAlgorithm	MIB-II	None	RO	
1.3.6.1.2.1.6.2.0	TcpRtoMin	MIB-II	None	RO	
1.3.6.1.2.1.6.3.0	TcpRtoMax	MIB-II	None	RO	
1.3.6.1.2.1.6.4.0	TcpMaxConn	MIB-II	None	RO	
1.3.6.1.2.1.6.5.0	TcpActiveOpens	MIB-II	None	RO	
1.3.6.1.2.1.6.6.0	TcpPassiveOpens	MIB-II	None	RO	
1.3.6.1.2.1.6.7.0	TcpAttemptFails	MIB-II	None	RO	
1.3.6.1.2.1.6.8.0	TcpEstabResets	MIB-II	None	RO	
1.3.6.1.2.1.6.9.0	TcpCurrEstab	MIB-II	None	RO	
1.3.6.1.2.1.6.10.0	TcpInSegs	MIB-II	None	RO	
1.3.6.1.2.1.6.11.0	TcpOutSegs	MIB-II	None	RO	
1.3.6.1.2.1.6.12.0	TcpRetransSegs	MIB-II	None	RO	
1.3.6.1.2.1.6.13.X	TcpConnTable Entries	MIB-II	None	RO	
1.3.6.1.2.1.6.14.0	TcpInErrs	MIB-II	None	RO	
1.3.6.1.2.1.6.15.0	TcpOutRsts	MIB-II	None	RO	
1.3.6.1.2.1.7.1.0	UdpInDatagrams	MIB-II	Derived from other Counts.	RO	
1.3.6.1.2.1.7.2.0	UdpNoPorts	MIB-II	Non-Peer and Spurious UDP errors	RO	
1.3.6.1.2.1.7.3.0	UdpInErrors	MIB-II	Frame Errors	RO	
1.3.6.1.2.1.7.4.0	UdpOutDatagrams	MIB-II	Frames Sent, Keep Alive Messages sent, etc.	RO	
1.3.6.1.2.1.7.5.X	udpEntry Table	MIB-II	None	RO	
1.3.6.1.2.1.11.1.0	SnmpInPkts	MIB-II	None	RO	
1.3.6.1.2.1.11.3.0	SnmpInBadVersions	MIB-II	None	RO	
1.3.6.1.2.1.11.4.0	SnmpInBadCommunityNames	MIB-II	None	RO	
1.3.6.1.2.1.11.5.0	SnmpInBadCommunityUses	MIB-II	None	RO	

1.3.6.1.2.1.11.6.0	SnmpInASNPar eErrs	MIB-II	None	RO	
1.3.6.1.2.1.11.30.0	SnmpEnableAuth enTraps	MIB-II	None	R/W	SIV
1.3.6.1.2.1.11.31.0	SnmpSilentDrops	MIB-II	None	RO	
1.3.6.1.2.1.11.32.0	SnmpProxyDrops	MIB-II	None	RO	

### 7.3 Supported Traps

Alarm Text	Severity	Trap Type	Notes
None	N/A	ColdStart	Generated when the unit starts up
None	N/A	AuthFail	SNMP Authorization Failure

## 8 ALARMS

The following table lists alarm types generated by the **IOJ2020**. Alarms are visible at the console and via StarKeeper® II NMS.

<b>Alarm</b>	<b>Severity</b>
LAN Link is Down	MAJOR
LAN Link is Up at 10Mbps.	INFO
User Requested Reboot in Progress	INFO
Invalid Login Attempt.	MINOR
Invalid Password Change Attempt.	MINOR
SNMP Trap Manager not reachable (ICMP).	INFO
ICMP Destination Unreachable Msg Received.	MINOR
Port XXX received a call from XXX.XXX.XXX.XXX outside CUG list.	MINOR
Serial Number is not valid. Module defective.	MAJOR
Console session in-activity timeout.	INFO
Password Reset Attempt Failed.	MINOR
User Port XX disconnected. Half Open TCP error.	INFO
Duplicate IP address @ MAC XXX.XXX.XXX.XXX.XXX.XXX	MAJOR
Installation Attempt Failed.	MINOR
The database is being automatically converted.	INFO
Warning: Database appears corrupted. Repair Attempted.	MAJOR
Warning: Database is corrupted. Not Repairable.	MAJOR

### 8.1 Major Alarms

A major alarm indicates a serious, service-degrading condition.

### 8.2 Minor Alarms

A minor alarm indicates a secondary or transient error that is not likely to affect overall service unless multiple minor alarms are issued. In this case, a serious condition exists that may affect overall system performance.

### 8.3 Info Alarms

An information alarm is a message that does not necessarily require attention. It typically is important for network administration, but does not adversely affect service.

## 9 MODULE MEASUREMENTS

This appendix itemizes the measurements available using the display measurements (**dm**) command with the **mod** option. These are unit-level measurements. The base measurements are always displayed; the error and exception counters are only displayed if nonzero.

Interface	Type	Protocol	Description
LAN	Base	All	Number of LAN Packets Received
LAN	Base	All	Number of LAN Packets Transmitted.
LAN	Except	All	Number of ICMP Echo Requests Received.
LAN	Error	All	Number of Ethernet Discards (Resource).
LAN	Error	All	Number of Late Collisions ( TX ).
LAN	Error	All	Number of Under-run. ( TX ).
LAN	Error	All	Number of packets which exceeded the Retry Limit ( TX ).
LAN	Error	All	Number of Carrier Sense Lost ( TX ).
LAN	Error	All	Number of Frame Collisions (RX).
LAN	Error	All	Number of Receiver Overruns (RX).
LAN	Error	All	Number of Receive CRC Errors. (RX).
LAN	Error	All	Number of Short Frame Errors. (RX).
LAN	Error	All	Number of Non-Aligned Frame Error. (RX).
LAN	Error	All	Number of Frame Length Violations. (RX).
LAN	Error	All	Number of Unsupported Protocol Frames. (RX).
LAN	Error	All	Number of Invalid UDP frames. (RX).
LAN	Error	All	Number of Rx Frames w/IP Header Checksum Errors. (RX).
LAN	Error	All	Number of Rx Frames w/ICMP Checksum Errors. (RX).
LAN	Error	All	Number of ICMP Unreachable Destination Messages (RX).
LAN	Error	IP-DSU	Number of Rx Frames from Non-Peer Entity.
LAN	Error	All	Number of Unknown ICMP Messages. (RX).
LAN	Error	IP-DSU	Number of Packets lost from TTL Network Error. (RX).
LAN	Error	All	Number of Packets with wrong IP Destination Address (RX).
LAN	Error	All	Number of Rx Packets with Unknown ARP Operations. (RX).
LAN	Error	All	Number of Bad ARP Reply Packets Received.
LAN	Error	All	Number of RFC894 Packets with an Unknown protocol type field. (RX).
LAN	Error	All	Number of 802.3 Frames with an Unknown protocol type field. (RX).
LAN	Error	SNMP	Number of SNMP Packets Received outside CUG (RX).

## 10 USER PORT MEASUREMENTS

This appendix itemizes the measurements available using the display measurements (**dm**) command with the **port** option. These are user-port-level measurements.

<u>Interface</u>	<u>Description</u>
TCP	Number of Intervals with Ingress Data.
TCP	Number of Intervals with Egress Data.
TCP	Number of Intervals with Port errors.

Note: In the measurements above, an interval is defined as 3.2 seconds.

## 11 IP-GATE PORT MEASUREMENTS

This appendix itemizes the measurements available using the display measurements (**dm**) command with the **ipgate** option. These are path-level measurements.

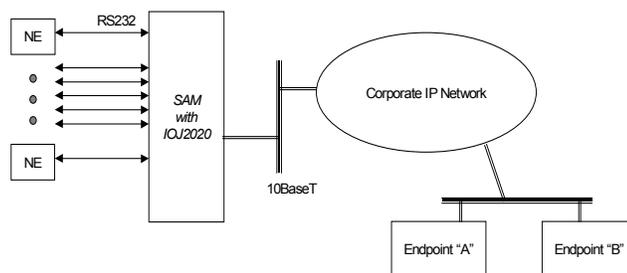
<u>Interface</u>	<u>Description</u>
TCP	Number of Intervals with Ingress Data.
TCP	Number of Intervals with Egress Data.
TCP	Number of Intervals with Port errors.

Note: In the measurements above, an interval is defined as 3.2 seconds.

## 12 CLOSED USER GROUP DEMO

The **IOJ2020** supports the notion of **Closed User Groups (CUGs)** for IP networking applications. A CUG applies to sessions being established to endpoints on the **IOJ2020**. This is an important feature for protecting sensitive endpoints in a corporate-wide network without the burden of special “security servers”.

The following diagram depicts a corporate IP network infrastructure which may be accessed by endpoints throughout the network. Some endpoints require access to the Network Elements (NEs) reachable via IP-type ports on the **IOJ2020**, and some endpoints are not to be allowed such access. IP network endpoints, which are allowed to access the NEs, are placed in a CUG to be associated with the appropriate user ports. (The same CUG may be associated with any number of user ports. Any one-user port may belong to up to 16 CUGs.)



Referring to the previous diagram, Endpoint **A** must be allowed access to all the NEs, but Endpoint **B** is not allowed such access. The **IOJ2020** is configured with CUG 1 with the address of Endpoint **A**, as follows:

**cug 1 ipaddr=135.17.59.5 submask=255.255.255.255**

Each **protected** user port (i.e., those connected to the NEs) is set up with CUG 1 assigned to it, as follows:

**port 1 type=rcv hport=26 cug=+1**

When Endpoint **A** calls the **IOJ2020** and TCP port number 26, access to the NE connected to port 1 on the **IOJ2020** is granted, and everything proceeds transparently. If an endpoint outside CUG 1 (e.g., Endpoint **B**) attempts to call the same TCP port, however, the following happens:

1. The call is terminated during authentication without any data being transported in either direction.
2. An **authentication alarm** is generated and sent to an attached Starkeeper, an attached Telnet Console (if any) and the SNMP Trap Manager (if any). The Alarm contains the IP address of the remote endpoint that attempted the unauthorized access.

## 13 CABLING

### 13.1 SAM Ports and the UDS 202T Modem

The UDS 202T modem has an RTS lead that must be either driven, or optioned to be enabled permanently. The **SAM** Synchronous DTE adapter (depicted in this section) will drive RTS whenever a call is present and therefore DTR is also driven. However, the obsolete AT&T SAM Synchronous DTE adapters had a race condition between RTS and CTS. If the AT&T Synchronous DTE adapters are to be used, the UDS 202T modem must be configured as **permanent** when operating with a SAM.

In either situation, the “cable type” configured in the SAM connection is DTE. The adapter presents a 25 pin male connection to the UDS modem.

It should be noted that a UDS 202T in operation with a standard DCN most likely does not have the RTS option configured as permanent. It is recommended that the Synchronous DTE adapter depicted in this section be used for such connections.

### 13.2 SAM Ports and AT&T/Paradyne 2024 Modem

The AT&T Paradyne 2024 modem is a 2400 baud synchronous or asynchronous modem used for leased facilities. These modems are used on a great deal of Network Element connections. The AT&T Paradyne 2024 modem is optioned by commands on a front panel via three levers and an “execute” button. The AT&T Paradyne 2024 modem does not provide proper clocking for a SAM in its default configuration.

There are two methods to provide proper clocking from the AT&T Paradyne 2024 modem. Both methods will work properly with the Synchronous DTE adapter depicted in this section. Only one method will work with the obsolete AT&T synchronous DTE adapter.

The first method, which will operate correctly with the Synchronous DTE adapter, involves setting the modem such that the Tx Clock (Pin 15) is derived from the external clock (Pin 24). This option is configured by setting option **B3** on the AT&T Paradyne 2024 modem from the front panel.

The second method, which will operate correctly with both the Synchronous DTE adapter and the obsolete AT&T Synchronous DTE adapter, involves setting the modem such that the Tx Clock (Pin 15) is a slave of the internal DDS timing. This option is configured by setting option **B2** on the AT&T Paradyne 2024 modem from the front panel.

The default configuration for the AT&T Paradyne 2024 modem is **B1** which is “internal” timing. In this default configuration, the clocks are not properly phased.

The AT&T Paradyne Modem does not have an RTS issue with either the Synchronous DTE adapter or the obsolete AT&T Synchronous DTE adapter.

The configuration of the AT&T Paradyne 2024 is described on pages 28 and 40 of its Operations manual. A synopsis of those instructions are as follows:

The modem is placed into command mode by setting the CMD/Test switch to CMD. The MDCK will display. Press EXEC twice to enable command input. The operating mode will change from MD/O to MD/I.

Using the FWD/BCK key, select the CHOP option, execute, and then enable **B3** (or **B2**) using the EXEC key.

The modem must be taken out of command mode by returning the MDCK display and setting the operating mode from MD/I to MD/O.

### 13.3 SAM Ports and General DataComm 201-7 Modems

The General DataComm 201-7 Modem is a 1200 or 2400 baud synchronous or asynchronous modem used for leased facilities. It is present on some Network Element connections. The modem is optioned by DIP switches, and berg jumpers. The 201-7 modem does not provide proper clocking for a SAM in its default configuration. In order to provide proper clocking, the Synchronous DTE adapter depicted in this section must be used. The obsolete AT&T synchronous DTE adapter will not function properly with the General DataComm 201-7 modem.

The modem is properly configured by setting DIP Switch #9, position #1, to the "external" position. The default is the "internal" position. All other configuration is not altered. This option will instruct the General DataComm 201-7 to use clock provided on Pin 24 of the interface as its Tx (or Pin 15) clock. This clock is bridged from the Rx Clock (Pin 17) by the Synchronous DTE adapter depicted below. The result is that both clocks are then properly phased.

The General DataComm 201-7 requires RTS asserted before proper operation can proceed. This modem does not allow a permanent enable of that lead. The Synchronous DTE adapter depicted in this section properly asserts RTS when the **SAM** port has a call active.

### 13.4 Cabling to a Modem Set

The Cabling to a Modem Set requires the use of a Synchronous DTE adapter. This is not the same as an asynchronous DTE adapter and has a different order code. However, the same Synchronous DTE adapter may be used on SAM64, SAM128, or SAM504. The **IOJ2020** port would be configured with a cable type of DTE.

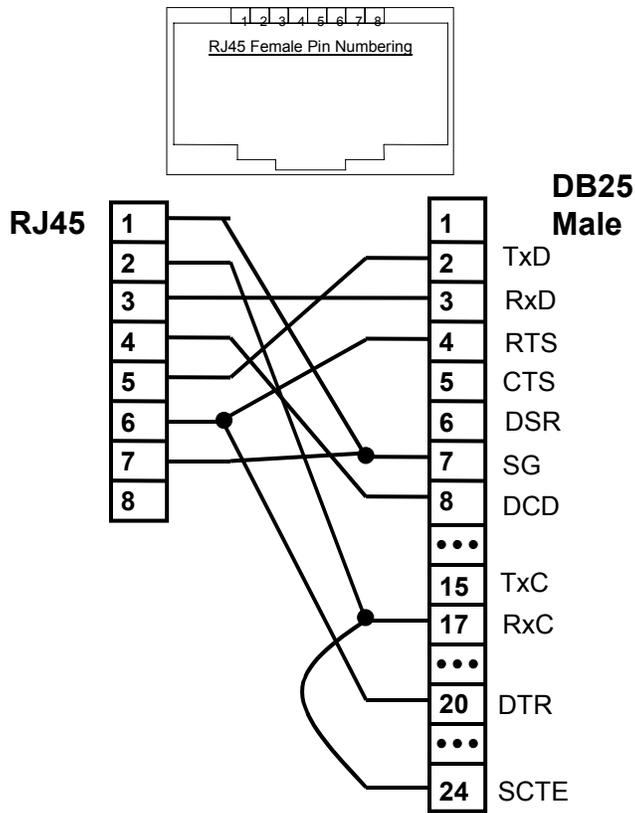
### 13.5 Cabling Directly to the Network Element

The Network Element is a physical synchronous DTE. It requires a clock source that is usually provided by a modem set. When cabling a **SAM** directly to the Network Element; it requires the use of a Synchronous DCE adapter. This is not the same as an asynchronous DCE adapter and has a different order code. However, the same Synchronous DCE adapter may be used on the SAM64, SAM128, and SAM504. The port would be assigned a baud rate appropriate for the Network Element (e.g. 2400 baud), and a cable type of DCE.

### 13.6 The Synchronous DTE Adapter

Depicted below is the cabling description for the Synchronous DTE adapter to be used with ports configured as a cable type of synchronous DTE. This adapter is applicable when the port is receiving the clocking to the interface between itself and a device. Generally, this interface adapter is used with Modem connections.

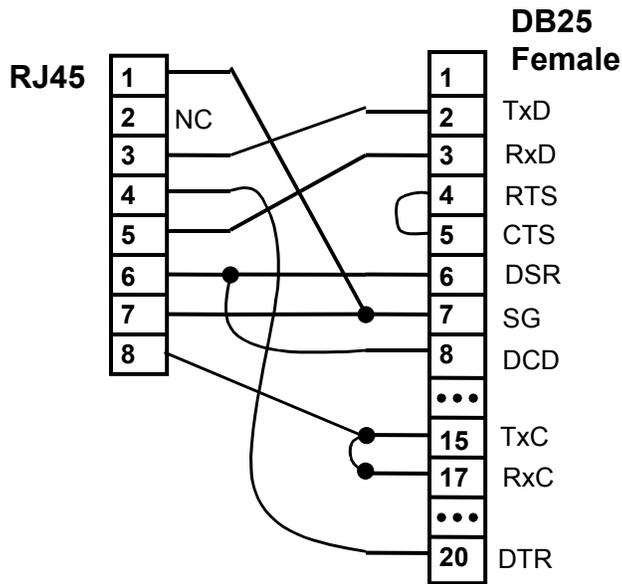
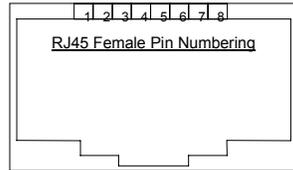
### Synchronous DTE Adapter



### 13.7 The Synchronous DCE Adapter

Depicted below is the cabling description for the Synchronous DCE adapter to be used with ports configured as a cable type of synchronous DCE. This adapter is applicable when the port is providing the clocking to the interface between itself and a device.

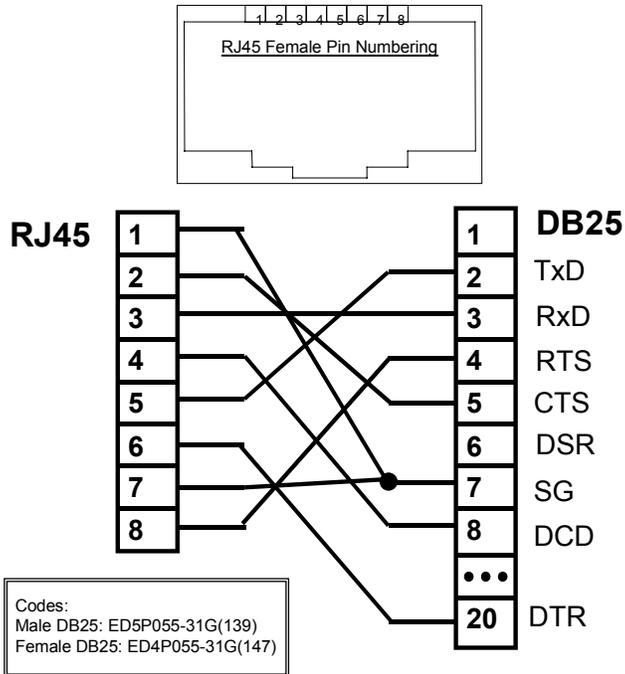
#### Synchronous DCE Adapter



### 13.8 The Asynchronous DTE Adapter

Depicted below is the cabling description for the asynchronous DTE adapter to be used with ports configured with a protocol of asynchronous (or raw), and a cable type of DTE. Generally, this interface adapter is used with Modem connections.

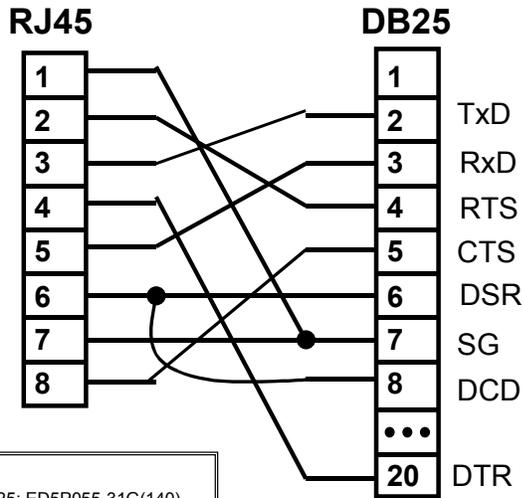
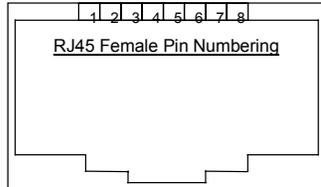
## Asynchronous DTE Adapter (AH)



### 13.9 The Asynchronous DCE Adapter

Depicted below is the cabling description for the asynchronous DCE adapter to be used with ports configured with a protocol of asynchronous (or raw) and a cable type of DCE.

## Asynchronous DCE Adapter (AG)



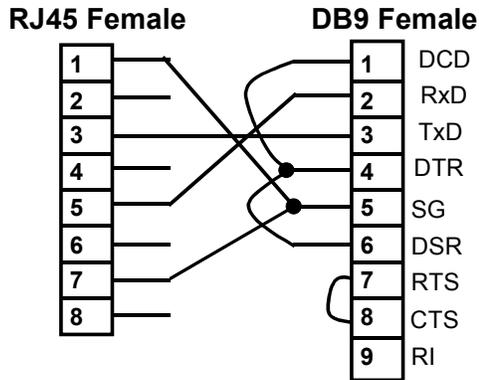
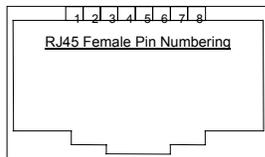
Codes:  
 Male DB25: ED5P055-31G(140)  
 Female DB25: ED4P055-31G(138)

### 13.10 The DB9 Console Adapter

Some Personal Computers use a 9 pin DB9 interface for serial communications. The terminal emulation programs may require certain lead status. Since console connections are generally implemented as three wire interfaces (i.e. RxD, TxD, and SG); this may pose a problem for the terminal emulation programs.

Below is depicted the wiring of a DB9 adapter which eliminates the problems associated with these terminal emulation programs. It is used with a standard **straight** category 5 RJ45 cable.

#### DB9 DCE Console Adapter



Note: This cable for use on console ports only.

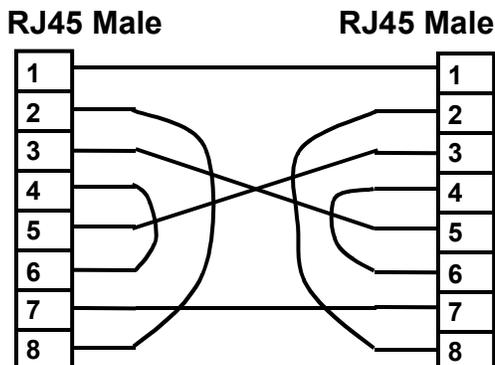
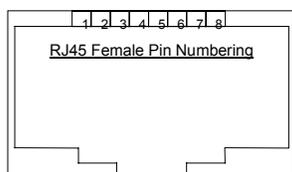
Use with a straight CAT-5 RJ45 cable.

### 13.11 The RJ45 to RJ45 Crossover Console Cable

The RJ45 to RJ45 console cable implements a three wire interface for attaching to a console on a **IOJ2020**. There is signal looping at either end. It is used to connect a serial console directly to a **4000**, **4000XA**, **4180**, **4280**, **4284**, a Datakit SAM port, or a Datakit TY port. No adapter is required. It may also be used in conjunction with an Asynchronous DCE or DTE adapter to provide console interfaces for personal computers or terminals where looped signals are required.

The diagram for the console cable is as follows:

#### RJ45 to RJ45 Console Cable



Note: This cable for use on console ports only.

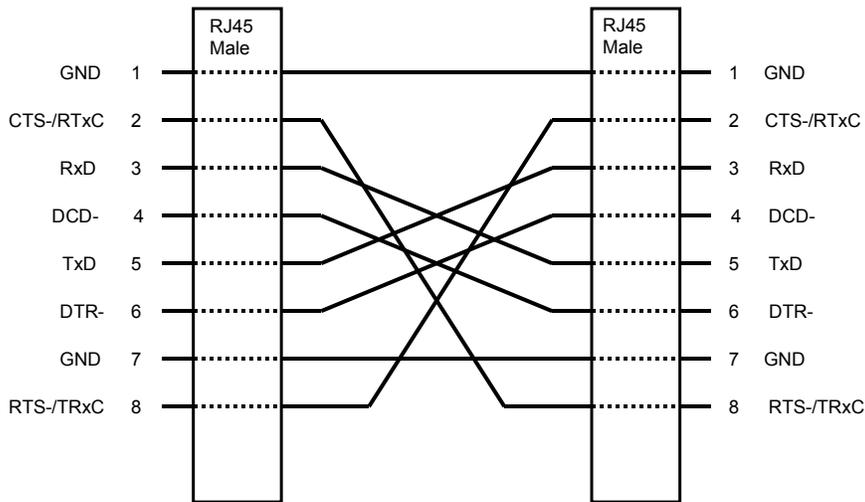
Comcode: 408198133

### 13.12 The RJ45 to RJ45 Full Crossover Cable

It is sometimes useful to interconnect two devices without adapters. The full cross-over cable will accomplish that function and preserve all of the lead functions. It is a generic cable that will work with any DT series, any Datakit/BNS series interface, and many other popular device interfaces.

A diagram of that cable is as follows:

**RJ45 Full Cross-Over Cable**

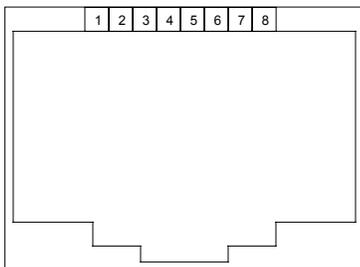


**13.13 The RJ45 LAN Crossover Cable**

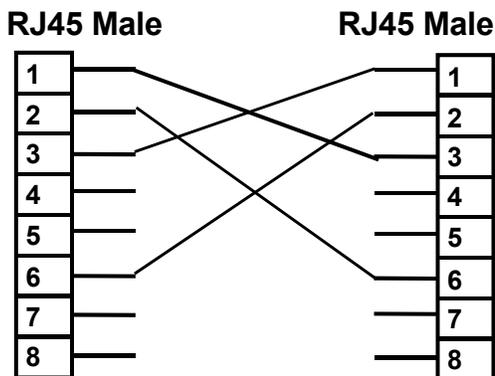
It is sometimes necessary to cross-over the LAN connection. This is used to interconnect equipment without an external Ethernet Hub or Switch.

The LAN crossover cable is a standard cable available at any supply outlet. However, it is shown here for informational purposes.

RJ45 Female Pin Numbering



<b>Pin</b>	<b>Symbol</b>	<b>Function</b>	<b>Signal Type</b>
1	Tx+	Data Transmission +	Output
2	Tx-	Data Transmission -	Output
3	Rx+	Data Reception +	Input
4	NC		
5	NC		
6	Rx-	Data Reception -	Input
7	NC		
8	NC		



## **14 SPECIFICATIONS**

### **14.1 CONSOLE PORT**

A standard RS-232C interface that uses binary data interchange between DTE and DCE. This interface uses an RJ45 connector and operates at 9600 bits per second (bps), 8 bits per character, no parity, and one stop bit.

### **14.2 Serial Ports**

The RS-232 serial ports on the **SAM** are RS-232. They are implemented as Telco or high density connectors that may be broken out to six RJ45 interfaces per cable. The **SAM** user ports are RS-232 and provide data rates up to 19.2Kbps asynchronous and 9.6 synchronous. The **SAM** user ports may be interfaced to V.35 devices with the use of a **9008** adapter.

### **14.3 10 BASE-T PORTS**

The **IOJ2020** provides two 8-pin LAN modular connector used to interface to a 10/100 Mbps baseband CSMA/CD local area network(s). Each LAN interface is limited to 10BaseT operation.

### **14.4 PHYSICAL DIMENSIONS**

<b>IOJ2020</b>	Width = 0.75" x Depth = 3" x Height = 7" (1 I/O mini)
----------------	-------------------------------------------------------

### **14.5 ENVIRONMENTAL OPERATING RANGE**

Operating Temperature: 5° to 40°C (41°F to 124°F) per GR-63-CORE.

Operating Humidity: 5% to 90% non-condensing per GR-63-CORE.

Altitude: From 60 m (197 ft.) below sea level to 1800 m (5905 ft.) above sea level and less than 4000 m (13122 ft) derated by 2° C per 300 m per GR-63-CORE.

### **14.6 POWER REQUIREMENTS**

**IOJ2020** Operating Voltage: 5V @ 350 mA Nominal (1.75 Watts)  
from SAM I/O Slot.

## **15 HARDWARE WARRANTY**

The warranty period for the IOJ2020 hardware shall be ninety (90) days from the date of shipment from TeleComp R&D or a designated manufacturer. Replacements and repairs are guaranteed for the longer of the remaining original warranty period or 30 days whichever is longer.

## **16 END-USER LICENSE AGREEMENT FOR SOFTWARE**

This License Agreement ("License") is a legal contract between you and the manufacturer ("Manufacturer") of the system ("HARDWARE") with which you acquired software product(s) identified above ("SOFTWARE"). The SOFTWARE may include printed materials that accompany the SOFTWARE. Any software provided along with the SOFTWARE that is associated with a separate end-user license agreement is licensed to you under the terms of that license agreement. By installing, copying, downloading, accessing or otherwise using the SOFTWARE, you agree to be bound by the terms of this LICENSE. If you do not agree to the terms of this LICENSE, Manufacturer is unwilling to license the SOFTWARE to you. In such event, you may not use or copy the SOFTWARE, and you should promptly contact Manufacturer for instructions on return of the unused product(s) for a refund.

### **16.1 Software License**

You may only install and use one copy of the SOFTWARE on the HARDWARE (unless otherwise licensed by Manufacturer). The SOFTWARE may not be installed, accessed, displayed, run, shared or used concurrently on or from different computers, including a workstation, terminal or other digital electronic device ("Devices"). Notwithstanding the foregoing and except as otherwise provided below, any number of Devices may access or otherwise utilize the services of the SOFTWARE. You may not reverse engineer, decompile, or disassemble the SOFTWARE, except and only to the extent that such activity is expressly permitted by applicable law notwithstanding this limitation. The SOFTWARE is licensed as a single product. Its component parts may not be separated for use on more than one HARDWARE. The SOFTWARE is licensed with the HARDWARE as a single integrated product. The SOFTWARE may only be used with the HARDWARE as set forth in this LICENSE. You may not rent, lease or lend the SOFTWARE in any manner. You may permanently transfer all of your rights under this LICENSE only as part of a permanent sale or transfer of the HARDWARE, provided you retain no copies, you transfer all of the SOFTWARE (including all component parts, the media and printed materials, any upgrades, this LICENSE and, if applicable, the Certificate(s) of Authenticity), and the recipient agrees to the terms of this LICENSE. If the SOFTWARE is an upgrade, any transfer must also include all prior versions of the SOFTWARE. Without prejudice to any other rights, Manufacturer may terminate this LICENSE if you fail to comply with the terms and conditions of this LICENSE. In such event, you must destroy all copies of the SOFTWARE and all of its component parts.

### **16.2 Intellectual Property Rights**

The SOFTWARE is licensed, not sold to you. The SOFTWARE is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. You may not copy the printed materials accompanying the SOFTWARE. All title and intellectual property rights in and to the content which may be accessed through use of the SOFTWARE is the property of the respective content owner and may be protected by applicable copyright or other intellectual property laws and treaties. This LICENSE grants you no rights to use such content. All rights not expressly granted under this LICENSE are reserved Manufacturer and its licensors (if any).

### **16.3 Software Support**

SOFTWARE support is not provided by Manufacturer, or its affiliates or subsidiaries separate from the HARDWARE. For SOFTWARE support, please contact your supplier of the HARDWARE. Should you have any questions concerning this LICENSE, or if you desire to contact Manufacturer for any other reason, please refer to the address provided in the documentation for the HARDWARE.

### **16.4 Export Restrictions**

You agree that you will not export or re-export the SOFTWARE to any country, person, or entity subject to U.S. export restrictions. You specifically agree not to export or re-export the SOFTWARE: (i) to any country to which the U.S. has embargoed or restricted the export of goods or services, which as of March 1998 include, but are not necessarily limited to Cuba, Iran, Iraq, Libya, North Korea, Sudan and Syria, or to any national of any such country, wherever located, who intends to transmit or transport the products back to such country; (ii) to any person or entity who you know or have reason to know will utilize the SOFTWARE or portion thereof in the design, development or production of nuclear, chemical or biological weapons; or (iii) to any person or entity who has been prohibited from participating in U.S. export transactions by any federal agency of the U.S. government.

### **16.5 Limited Warranty**

Manufacturer warrants that (a) the SOFTWARE will perform substantially in accordance with the accompanying written materials for a period of ninety (90) days from the date of shipment from TeleComp R&D or a designated manufacturer. Software support is limited to the hours of 9AM to 5PM ET Monday through Friday excluding TeleComp R&D observed holidays. An extended warranty may be purchased at additional cost. Any implied warranties on the SOFTWARE are

limited to ninety (90) days. Some states/jurisdictions do not allow limitations on duration of an implied warranty, so the above limitation may not apply to you.

Manufacturer's and its suppliers' entire liability and your exclusive remedy shall be, at Manufacturer's option, either (a) return of the price paid, or (b) repair or replacement of the SOFTWARE that does not meet this Limited Warranty and which is returned to Manufacturer with a copy of your receipt. This Limited Warranty is void if failure of the SOFTWARE has resulted from accident, abuse, or misapplication. Any replacement SOFTWARE will be warranted for the remainder of the original warranty period or thirty (30) days, whichever is longer.

**16.6 No Other Warranties**

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, MANUFACTURER AND ITS SUPPLIERS DISCLAIM ALL OTHER WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT, WITH REGARD TO THE SOFTWARE AND THE ACCOMPANYING WRITTEN MATERIALS. THIS LIMITED WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHERS, WHICH VARY FROM STATE/JURISDICTION TO STATE/JURISDICTION.

**16.7 Limitation of Liability**

To the maximum extent permitted by applicable law, in no event shall Manufacturer or its suppliers be liable for any damages whatsoever (including without limitation, special, incidental, consequential, or indirect damages for personal injury, loss of business profits, business interruption, loss of business information, or any other pecuniary loss) arising out of the use of or inability to use this product, even if Manufacturer has been advised of the possibility of such damages. In any case, Manufacturer's and its suppliers' entire liability under any provision of this License shall be limited to the amount actually paid by you for the SOFTWARE and/or the HARDWARE. Because some states/jurisdictions do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you.

**16.8 Special Provisions**

The SOFTWARE and documentation are provided with RESTRICTED RIGHTS. Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and HARDWARE Software clause at DFARS 252.227-7013 or subparagraphs (c)(1) and (2) of the Commercial HARDWARE Software-Restricted Rights at 48 CFR 52.227-19, as applicable. Manufacturer is TeleComp R&D or it's designee manufacturer., 102 SW Orange Blossom, Lake City, Florida, 32025.

If you acquired the SOFTWARE in the United States of America, this Software License are governed by the laws of the State of New Jersey, excluding its choice of laws provisions. If you acquired the SOFTWARE outside the United States of America, local law may apply. This LICENSE constitutes the entire understanding and agreement between you and the Manufacturer in relation to the SOFTWARE and supercedes any and all prior or other communications, statements, documents, agreements or other information between the parties with respect to the subject matter hereof.

## **17 SALES & DISTRIBUTION**



**Communications Technology Solutions**

**CBM of America, Inc.  
Mr. Mike Stephens  
1455 West Newport Center Drive  
Deerfield Beach, Florida  
33442**

**800-881-8202  
954-698-9104 Fax: 954-360-0682**

**www.cbmusa.com**

## **18 AUTHOR**

Comments and Questions regarding this document or the products covered within this document should be addressed to the author Angel Gomez via email at [angel@trdcusa.com](mailto:angel@trdcusa.com) or via telephone at 386-754-5700.

©Copyright 2002, 2008 TeleComp Research & Development Corp.

©Copyright 1998, 2002 TeleComp Inc.

All Rights Reserved

Printed in USA

Datakit® and StarKeeper® II NMS are registered trademarks of Lucent Technologies.