IP-MPA

MULTIPLE PROTOCOL INTEGRATED ACCESS DEVICE USER'S MANUAL

Release: 2.x

102 SW Orange Blossom
Lake City, Florida
32025-1613
phone: 386-754-5700
email: sales@trdcusa.com
http://www.trdcusa.com

Manufacture & Distribution:

CBM
Communications Technology Solutions

http://www.cbmusa.com

1 IMPORTANT SAFETY INSTRUCTIONS 5

2 INTRODUCTION 7

2.1 CLOSED USER GROUPS 7
2.2 HUNT GROUPS 7
2.3 DNS FEATURES 7
2.4 TACACS+ RADIUS LOGIN SUPPORT 8
2.5 X.25 MEDIATION FEATURES 8

3 PHYSICAL DESCRIPTION 9

3.1 POWER INTERFACES 9
3.2 CONSOLE INTERFACE 10
3.3 RS-232/V.11/RS-530SERIAL INTERFACE 10
3.4 10BASE-T INTERFACE 10
3.5 USER PORTS 10
3.6 LEDS 12

4 INSTALLATION 13

4.1 REQUIRED EQUIPMENT 13
4.2 INSTALLATION FOR AC-ONLY OPERATION 13
4.3 INSTALLATION FOR DC OPERATION 14
4.4 IPMPA INITIAL CONFIGURATION CONSOLE CABLING 15
4.5 WINCHESTER 34 PIN CABLING. 16
4.6 FIELD UPGRADE AND SOFTWARE REGISTRATION 17

5 CONFIGURATION 20

5.1 OVERVIEW 20
5.2 BASE CONFIGURATION 20
5.2.1 Console Security 20
5.3 USER PORT CONFIGURATION 20
5.3.1 IP Originating Ports 20
5.3.2 IP Receive Ports 21
5.3.3 IP Closed User Groups 22

6 COMMAND REFERENCE 23

6.1 BASE CONFIGURATION COMMANDS 23
6.1.1 LOGIN 23
6.1.2 LOGOUT 23
6.1.3 CHANGE PASSWORD 23
6.1.4 LOCAL 24
6.1.5 GATEWAY 24
6.1.6 DOMAIN NAME SERVER 24
6.1.7 TACACS+ RADIUS Servers 25
6.1.8 HELP 25
6.1.9 VERSION 25
6.1.10 REBOOT 25
6.1.11 REMOVE MODULE 26
6.1.12 RESTORE MODULE 26
6.1.13 CLEAR 26
6.1.14 DISPLAY MODULE MEASUREMENTS 26
6.1.15 DISPLAY LOG 26
6.1.16 VERIFY MODULE 27

6.1.17 HOST NAME ADMINISTRATION ... 27
6.1.18 VERIFY HOST ... 27
6.1.19 SNMP ... 27
6.1.20 RSTPASS (Resetting the Password) ... 28
6.1.21 CONSOLE TIMEOUT ... 29
6.1.22 Label ... 29
6.1.23 PING ... 29
6.1.24 TraceRoute ... 30
6.1.25 DATA-BASE RESET ... 30
6.1.26 DISCONNECT CONSOLE ... 31
6.1.27 ADMINISTER SECURITY BANNER ... 31
6.1.28 CLOSED USER GROUP (CUG) ADMINISTRATION ... 31
6.1.29 VERIFY CUG ... 32
6.1.30 ASSIGNING A CUG TO THE CONSOLE ... 32
6.1.31 Administrative Logins & Command Security ... 32
6.2 USER PORT COMMANDS ... 34
6.2.1 PORT ... 34
6.2.2 REMOVE PORT ... 42
6.2.3 RESTORE PORT ... 42
6.2.4 DISPLAY PORT MEASUREMENTS ... 42
6.2.5 VERIFY PORT ... 43
6.2.6 VERIFY VIRTUAL CIRCUIT ... 43
6.2.7 DISPLAY PORT STATUS ... 43
6.2.8 DISPLAY CONNECTIONS ... 43
6.2.9 DIAGNOSE USER PORT ... 43
6.2.10 DISCONNECT USER PORT ... 44
6.2.11 X.25 Protocol Analyzer Snooper ... 44
6.2.12 Configuring User Prompt ... 44

7 SNMP ... 46

7.1 SNMP VERSION 1 COMMANDS ... 46
7.2 IPMPA 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 CLOSED USER GROUP DEMO ... 52

12 CABLING ... 54

12.1 CABLING DIRECTLY TO THE NETWORK ELEMENT ... 54
12.2 THE RJ45 TO IPMPA DB25 CONSOLE ADAPTER ... 54
12.3 THE RJ45 LAN CROSSOVER CABLE ... 55

13 SPECIFICATIONS ... 56

13.1 CONSOLE PORT ... 56

13.2 USER SERIAL PORT 56
13.3 10 BASET LAN PORT 56
13.4 PHYSICAL DIMENSIONS 56
13.5 ENVIRONMENTAL OPERATING RANGE 56
13.6 POWER REQUIREMENTS 56
13.7 REGULATORY INFORMATION 57
13.7.1 IPMPA Stand-Alone 57
13.7.2 FCC Part 68 Information 57
13.7.3 Industry Canada CS03 Certification Information 57
13.7.4 NEBS COMPLIANCE 58

14 HARDWARE WARRANTY 59

15 END-USER LICENSE AGREEMENT FOR SOFTWARE 59

15.1 SOFTWARE LICENSE 59
15.2 INTELLECTUAL PROPERTY RIGHTS 59
15.3 SOFTWARE SUPPORT 59
15.4 EXPORT RESTRICTIONS 59
15.5 LIMITED WARRANTY 59
15.6 NO OTHER WARRANTIES 60
15.7 LIMITATION OF LIABILITY 60
15.8 SPECIAL PROVISIONS 60

16 SALES & DISTRIBUTION 61

17 AUTHOR 61

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 unit must be powered from either –48 V DC, or AC voltage sources. Additionally, the **IPMPA** may also be powered via the Ethernet Interface.
- The –48 V DC input terminals are only provided for installations in Restricted Access Areas locations.
- 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 unit 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 symbol is marked on the **IPMPA**, adjacent to the ground (earth) area for the connection of the ground (earth) conductor.

- 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.
- For a unit equipped with an AC Wall Plug-In Unit, read and understand the following:
  - For the **IPMPA**, use only the Astrodyne Part # SPU15A-111 48 volt power supply adapter.
  - Unplug this product from the wall outlet before cleaning. Do not use liquid cleaners or aerosol cleaners. Use a damp cloth for cleaning.
  - Do not staple or otherwise attach the power supply cord to the building surfaces.
  - Do not overload wall outlets and extension cords as this can result in the risk of fire or electric shock.
  - The socket outlet shall be installed near the equipment and shall be readily accessible.
  - The Wall Plug-In unit may be equipped with a three-wire grounding type plug, a plug having a third (grounding) pin. This plug is intended to fit only into a grounding type power outlet. Do not defeat the safety purpose of the grounding type plug.
  - Do not allow anything to rest on the power cord. Do not locate this product where persons walking on it may abuse the cord.
  - Unplug this product from the wall outlet and refer servicing to qualified service personnel under the following conditions:
    a) When the powers supply cord or plug is damaged or frayed.
    b) If liquid has been spilled into the product.
    c) If the product has been exposed to rain or water.
    d) If the product does not operate normally by following the operating instructions. Adjust only those controls that are covered by the operating instructions because improper adjustment of other controls may result in damage and will often require extensive work by qualified technician to restore the product to normal operation.
    e) If the product has been dropped or the cabinet has been damaged.
    f) If the product exhibits a distinct change in performance.

SAVE THESE INSTRUCTIONS

2 INTRODUCTION

The **IPMPA** is a Multiple Protocol Inter-Networking devices.

The **IPMPA** include optional enhanced vertical service feature packages such as X.25 mediation in various capacities. Other feature packages are similarly available.

The **IPMPA** is a single port device. The serial port is synchronous, or asynchronous that support speeds up to 115.2kbps. Popular protocols such as Asynchronous, HDLC, SDLC, and X.25 are all supported interchangeably on a per-port basis.

In addition, vertical services typically found on Embedded Network processors have been incorporated into the **IPMPA** 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 **IPMPA** 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 **IPMPA** power options are 48VDC nominal, **Power over Ethernet (POE)**, or AC via the power cube.

The IPMPA provides a serial port that directly supports multiple physical signal levels. It can directly support RS-232, and V.35 via soft configuration.

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 **IPMPA** 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 **IPMPA** 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 **IPMPA** provides this capability for user ports configured to receive calls from the IP network.

2.3 DNS FEATURES

The **IPMPA** can maintain a set of mnemonic host names, analogous to the */etc/hosts* file on both UNIX and Microsoft Windows platforms. This allows the **IPMPA** 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 **IPMPA** will always accept an IP address in its numeric form.) The **IPMPA** 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 **IPMPA** 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.

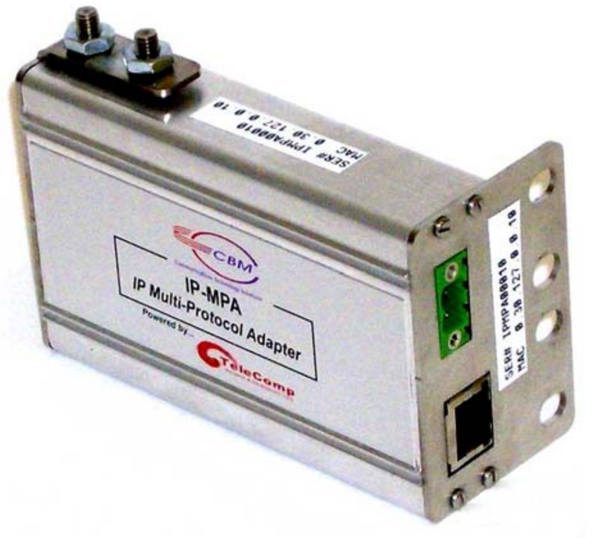
2.5 X.25 Mediation Features

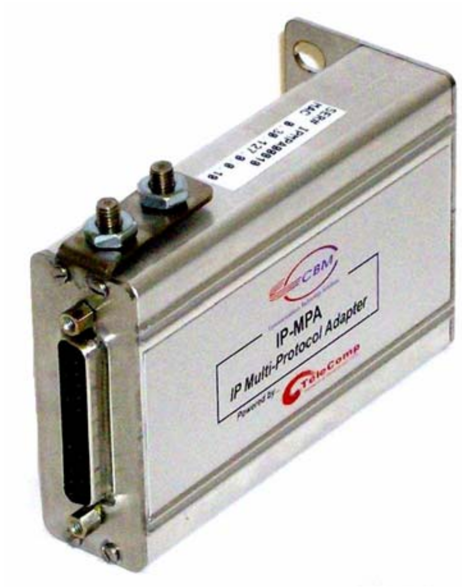
The **IPMPA** has one instance of the X25PAD mediation application.

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.

3 PHYSICAL DESCRIPTION





3.1 POWER INTERFACES

48VDC Power

The **IPMPA** accept DC power input directly from a 48V DC power source which connects to the two position female block. The companion male terminal block accommodate 10 awg (American Wire Gauge) to 14 awg wire. The polarity of the wiring is not important as the **IPMPA** circuitry automatically selects the correct polarity. The **IPMPA** –48VDC voltage tolerance is +/- 10%.

Ground

The **IPMPA** has a two lug grounding block for external footprint grounding. The **IPMPA** may also be grounded via the case screws.

AC Power

For this application, a separate AC power supply is available which plugs into a standard 115/240V AC outlet. The power supply has a six-foot cable that terminates with individual leads. The leads are screwed into the male terminal block that mates with its companion on the **IPMPA**.

Power Over Ethernet

The **IPMPA** will accept power on the LAN connection using the **POE** specification. When used, no additional power is required by the device.

Redundant Power

The **IPMPA** may be connected to power on each of their supported interfaces. For example, the "**Power over Ethernet**" may be used at the same time as 48VDC power on the power block. The power supplies are isolated from each other and completely redundant.

3.2 CONSOLE INTERFACE

The console interface is used for initial configuration, and for StarKeeper® II NMS monitoring on an on-going basis.[1]

On the **IPMPA**, the serial console interface is available on unused pins of the RS-530 DB25 connector (Pins 18 & 25). Once initially configured, all operations may use the telnet console.

The console interface always uses RS-232 signaling without regard to the configuration of the DB25 interface. It is configured as asynchronoyus, 9600 bps, 8 bits, no parity and one stop bit.

3.3 RS-232/V.11/RS-530SERIAL INTERFACE

The DB25 RS-530 female connector on the **IPMPA** provides support for software-selectable device interfaces (V.35 and RS232-C) . The DB25 RS-530 interface is a native DCE. The female connector electrically presents a data terminal equipment (DCE) interface and supports RS-232C directly. For V.35 winchester cabling, a standard RS-530 DB25 Female to V.35 Winchester-34 Male adapter is available.

3.4 10BASE-T INTERFACE

The LAN connection on the **IPMPA** is a 10 BaseT interface on the front of the unit and is labeled “LAN”. 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 DB25 RS-530 female connector on the **IPMPA** provides support for software-selectable device interfaces (V.35 and RS232-C) . The DB25 RS-530 interface is a native DCE. The female connector electrically presents a data terminal equipment (DCE) interface and supports RS-232C directly. For V.35 winchester cabling, a standard RS-530 DB25 Female to V.35 Winchester-34 Male adapter is available.

[1] The **IPMPA** 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.

The DB25 is the user port and supports either asynchronous and/or synchronous protocol sets. Physical DCE modes are supported. Logical modes may be DCE or DTE as configured. Configuration is software selectable on a per port basis. Baud rates up to 115.2kbps are supported. Synchronous ports do not support isochronous modes. Asynchronous ports do not support NRZI, nor isochronous modes.

3.6 LEDs

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

LED Function	LED Color	LED Description
PWR	Green	Unit Power Indicator
LNK/ACT	Green	Link & Activity (Blink) Indicator

4 INSTALLATION

This chapter contains the steps needed to install and cable the **IPMPA**. The **IPMPA** is directly attached to the network element via a DB25 interface. A #2 Phillips and medium-sized flathead screwdrivers are required.

4.1 REQUIRED EQUIPMENT

To install either a rack-mounted or stand-alone device, the following items are needed:

- One **IPMPA** unit
- For AC operation, AC power supply
- For DC operation, a strain-relief clamp for wire stabilization

Cables – refer to CABLING sections **4.4** through **4.7** below to determine specific requirements for this installation. ***Note: Shielded cables must be used in order to maintain compliance with EMC requirements.***

- The Environmental Operating Range of 5 to 40 degrees C (41 to 124 degrees F) is necessary to maintain compliance with UL.

4.2 INSTALLATION FOR AC-ONLY OPERATION

1) Preconfigure unit as needed.
2) Attach data transport cables – refer to section **4.5**
3) Attach power leads from the 115VAC power supply to the screwdown connector labeled 48VDC on the **IPMPA**.
4) Plug the power supply into a standard 115V AC outlet.

4.3 INSTALLATION FOR DC OPERATION

1. Preconfigure unit as required.

2. Attach data transport cables – refer to section **4.5**

3. Run 48V DC (return, -48, and ground) wires from a central source through the strain relief clamp for DC wire stabilization. On the faceplate, attach the return, -48, and ground wires to the return, -48, and ground connections, respectively, on the terminal block labeled 48V DC.

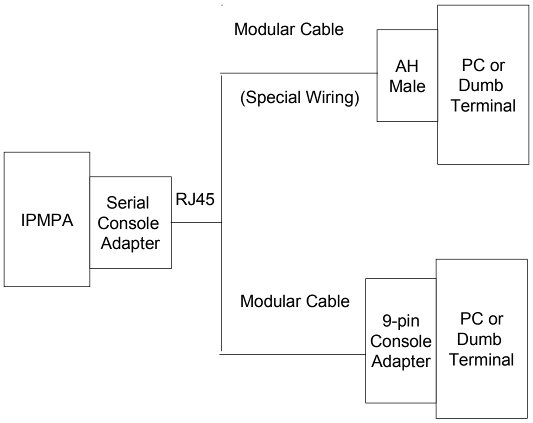
4. The Environmental Operating Range of 5 to 40 degrees C (41 to 124 degrees F) is necessary to maintain compliance with UL.

4.4 IPMPA INITIAL CONFIGURATION CONSOLE CABLING

The serial console is needed to initially configure the **IPMPA**'s IP parameters. These are limited to the IP address, the Gateway address, and IP Network Submask.

Otherwise, the serial console is normally disconnected during normal operation, and *telnet* console access via TCP port 1023 is used. The **IPMPA** does not preclude a serial console connection during normal operation. Should such be desired, a "Y" cable is needed on the DB25 implementing the console connection.

The **IPMPA** serial console configuration wiring options are as follows:



IPMPA Serial Console Options

The **IPMPA** has no RJ45 jack, like other TeleComp R&D Migration Products, for connection of a serial console. Before connection to the Network Element, a DB25 to RJ45 adapter with special wiring must be attached to the **IPMPA**. The serial console is connected via this adapter and cabling as shown in the figure above. Specific wiring information is found in the cabling section of this document.

The serial console is configured as 9600 baud, 8 bits, and no parity.

4.5 Winchester 34 Pin cabling.

The IPMPA directly supports V.35 through the industry standard DB25 interface. To connect the IP-MPA to a 34 Pin winchester interface, the Black Box FA058 (DCE), and FA059 (DTE) DB25 to winchester 34 adapters are utilized.

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

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**[2] into a staging area and is not active. The software then is activated by 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 –mIPMPA 192.169.90.90 ipmpa.1.1
```

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

The steps are as follows:

[2] 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 “dt_device.info” in the current directory.
2. The “dt_device.info” file is then sent via email to keys@trdcusa.com for registration processing.
3. A file name “dt_device.register” file is returned via email to be used as input in the next step. A file named “dt_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 “dt_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 “dt_device.info” file and the “dt_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 dt_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 dt_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 “dt_device.info” that is always created in the current directory.

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

After receiving the “dt_device.register” file, the **setreg** utility is invoked with the relative path of the “dt_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 “dt_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 “dt_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.

```
<4280> login passwd=initial ↵
<4280> local ipaddr=192.169.90.90 submask=255.255.255.0 ↵
<4280> gateway ipaddr=192.169.90.1 ↵
<4280> 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 **IPMPA Destination>** prompt where **IPMPA** 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.

```
<4280> port 2 type=orig baud=9600 dbits=8 parity=none ↵
<4280> 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 **IPMPA** itself is already configured for IP networking, and in service.

```
<4280> port 1 type=rcv hport=51000 baud=9600 dbits=8 parity=none
pap=on ↵

<4280> port 9 type=rcv hport=51000 baud=9600 dbits=8 parity=none
pap=on ↵

<4280> port 13 type=rcv hport=51000 baud=9600 dbits=8 parity=none
pap=on ↵

<4280> restore port 1 ↵
<4280> restore port 9 ↵
<4280> 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 **IPMPA**.

6 COMMAND REFERENCE

These commands are used to configure the operation of the **IPMPA** device.
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: chgpass 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 DISPLAY LOG

Syntax: dlog

This command is available only on the **4000XA**, and **4180**, and displays the **IP-GATE** exception logs. The **IP-GATE** exception log provides details about the last 32 errors recorded. Not all errors generate exception entries. These logs may be cleared using the ***clear logs*** command.

6.1.16 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.

6.1.17 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.

6.1.18 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.

6.1.19 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 **IPMPA** allows setting of an SNMP community in addition to the *public* community. When configured, the **IPMPA** will respond to SNMP manager requests in that community. The **IPMPA** 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 **IPMPA** 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 **IPMPA** non-volatile database. Setting the value to **NONE** will clear the entries in the **IPMPA** 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**.

6.1.20 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 **IPMPA** 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 **IPMPA** 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 **IPMPA** 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 **IPMPA**. The **IPMPA** 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 **IPMPA**.

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 **IPMPA**.

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 **IPMPA** 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 **IPMPA**, 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 **IPMPA** address may be assigned to the console. The net effect is to disallow any and all connections via the telnet console.

6.1.31 Administrative Logins & Command Security

```
Syntax: admpass lev=<#> [old=<Existing Password>]
                        new=<New Password>
                        confirm=<New Password>
```

The **IPMPA** supports the concept of “Administrative Passwords”. When defined, there are four levels of “Administrative Passwords” in addition to the general user password. The command set is divided among the various levels of administrators. The General User has the least permissions, and a Level 4 administrator has global permissions.

If the administrative passwords are not defined, the general user has global permissions. The level 4 administrative password must be define first. Once the level 4 administrative password is defined, it is required to change any of the administrative passwords.

The **old=<Existing Password>** is not required in the initial setting of the level4 administrative password. It is also not required if the level 4 administrator wishes to change any of the lower level passwords.

Once administrative passwords are set, the **IPMPA** command set requires the following authority:

ADMPASS	Level 4 Administrator
BANNER	Level 4 Administrator
CHGPASS	General User
CLEAR	Level 1 Administrator
CONSOLE	Level 3 Administrator
CUG	Level 3 Administrator
DBRESET	Level 4 Administrator
DCACHE	General User
DCONN	General User
DIAG	Level 2 Administrator
DISC	Level 2 Administrator
DLOG	General User
DMEAS	General User
DNS	Level 4 Administrator
DSTAT	General User
GATEWAY	Level 4 Administrator
HELP	General User
HOST	Level 3 Administrator
INSTALL	General User
LABEL	Level 4 Administrator
LOCAL	Level 4 Administrator
LOGOUT	General User
MAP	General User
PING	Level 1 Administrator
PORT	Level 2 Administrator
REBOOT	Level 4 Administrator
REMOVE (mod)	Level 4 Administrator
REMOVE (port)	Level 2 Administrator
REMOVE (IP-GATE)	Level 2 Administrator
REMOVE (TSR)	Level 2 Administrator
RESTORE (mod)	Level 4 Administrator
RESTORE (port)	Level 2 Administrator
RESTORE (IP-GATE)	Level 2 Administrator
RESTORE (TSR)	Level 2 Administrator
RSTPASS	General User
SAMEXT	Level 2 Administrator
SNMP	Level 3 Administrator
SNOOP	General User
TIMEOUT	Level 4 Administrator
TSR	Level 2 Administrator
VER	General User
UPROMPT	Level 3 Administrator
VFY	General User

Please note that if multiple administrators have the same password, the lowest value is used. It is recommended that passwords be unique.

6.2 USER PORT COMMANDS

The User Port commands are used to configure the operation of the individual RS-232C ports on the **IPMPA**. 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 > ]
               [ prot = < protocol > ]
               [ phy = < 232 | v35 > ]
               [ baud = < baud rate > ]
               [ enc = < nrz | nrzi > ]
               [ ccar = < 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 > ]
               [ comment = ”user comment” ]
               [ x25dxe=< 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 > ]
           [ pvcreset=< 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 >]
           [ padcrlf=<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 one for the **IPMPA**.

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 **IPMPA 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^{st} 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 **IPMPA** 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 **IPMPA** 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, or SDLC.** 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 or via telephone @ (386) 754-5700, with any other protocol requests.

The **IPMPA** uses a **dxe** value of **DCE**. When the protocol is synchronous (e.g. SDLC*)*, a **dxe** value of **DCE** implies that the **IPMPA** should generate the clock signals. This would require the standard synchronous DCE cable adapter.

The **phy**=<232 | V35 > option specifies the physical interface specification to be used by the **IPMPA** on the user port. The IPMPA supports directly the signal levels without additional equipment.

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 **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, 19200, 28800, 38400, 48000, 57600, 67200, 76800, and 115200. For synchronous DCE ports, the same rates apply up to and including 57600 (56K) baud. The default value is 9600. A special value "dt9001" (without quotes) should be entered if the port is being used to connect to a **9001**.

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 ASII 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 **IPMPA**, 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 **IPMPA** 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 **crypt=< ON | OFF >** option is used to select peer to peer secure cryptography of the session. Both session endpoints should be set identically. When the feature is set **OFF**, there is no cryptography on the session. When the feature is set **ON**, a peer to peer session cryptography is used. The key selection is dynamic, and automatically performed by the **IPMPA**.

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 **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 ciruit. When the **PVC** option is selected, connections will not generate call setup or call clear X.25 packets. However, the **IPMPA** 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 **GRPx** 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 1/20th 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 wit 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 **IPMPA**. 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 **IPMPA**. 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 **IPMPA**. 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 **IPMPA**. The **<all>** parameter will verify all ports. The **<range>** parameter will verify a sequential range of ports.

6.2.6 VERIFY VIRTUAL CIRCUIT

Syntax: vfy vc < portnum > <vc range>

This command is only visible when the unit is logged in. It displays the configuration of the X.25 virtual circuits on the port number specified. The **<portnum>** parameter may be a number in the range 1 through the number of ports on the **IPMPA**. The port must be configured for X.25 or the command will fail. The value of **all** in the **<vc range>** parameter will display the configuration of all virtual circuits for the port.

6.2.7 DISPLAY PORT STATUS

Syntax: dstat port < < portnum > | < all > | < range > >

This command is only visible when the unit is logged in. It displays the status of the port number specified. The **<portnum>** parameter may be a number in the range 1 through the number of ports on the **IPMPA**. The **<all>** parameter will display the status of all ports. The **<range>** parameter is in the form of "start-end", and will display the status of the ports in that sequential range inclusive.

6.2.8 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.

6.2.9 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.

6.2.10 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.

6.2.11 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.

6.2.12 Configuring User Prompt

Syntax: uprompt [“User Prompt” | STD]

The **uprompt** command command supports custom user prompting for ports of **type=orig**. In the default condition, a user is prompted with a **IPMPA Destination>** prompt string where **IPMPA** 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 **IPMPA** user prompt to its default, or standard, configuration.

7 SNMP

The **IPMPA** 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 IPMPA 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	SnmpInASNParseErrs	MIB-II	None	RO	
1.3.6.1.2.1.11.30.0	SnmpEnableAuthenTraps	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 **IPMPA**. Alarms are visible at the console and via StarKeeper® II NMS.

Alarm	Severity
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
Over-Temperature Condition Detected.	MAJOR
Over-Temperature Condition Cleared.	INFO
High Temperature Condition Detected.	MINOR
High Temperature Condition Cleared.	INFO
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
Gate Path XX disconnected. Half Open TCP error.	INFO
Duplicate IP address @ MAC XXX.XXX.XXX.XXX.XXX.XXX	MAJOR
TSR Loss-of-Frame Detected	MINOR
TSR Loss-of-Frame Cleared	INFO
Insufficient Administrative Authority	MINOR
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.

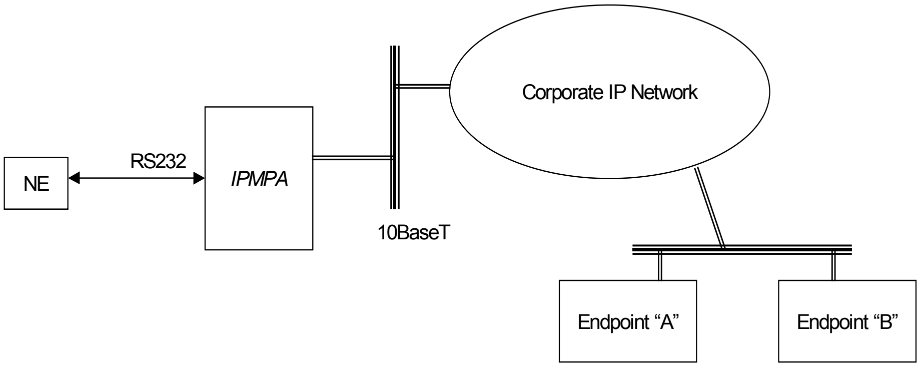
Interface	**Description**
TCP	Number of Intervals with Ingress Data.
TCP	Number of Intervals with Egress Data.
TCP	Number of Intervals with Port errors.

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

11 CLOSED USER GROUP DEMO

The **IPMPA** supports the notion of ***Closed User Groups (CUGs)*** for IP networking applications. A CUG applies to sessions being established to endpoints on the **IPMPA**. 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 **IPMPA**, 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 **IPMPA** 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 **IPMPA** and TCP port number 26, access to the NE connected to port 1 on the **IPMPA** 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.

12 CABLING

12.1 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. The IPMPA provides this clocking and may be directly attached to the network element without intervening cabling. The **IPMPA** port would be assigned a baud rate appropriate for the Network Element (e.g. 2400 baud), and a cable type of DCE.

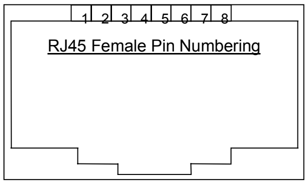
12.2 The RJ45 to IPMPA DB25 Console Adapter

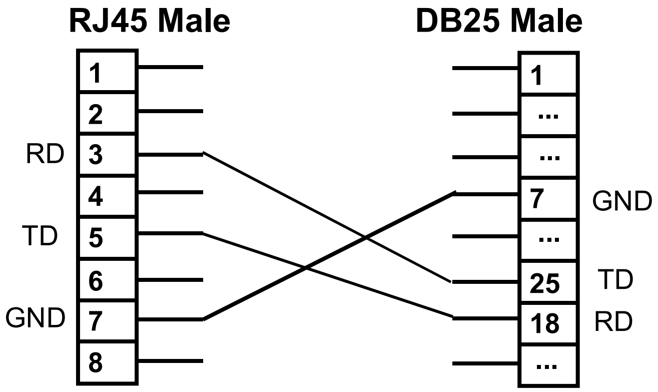
The **IPMPA** implements the serial console as an RS-232 interface on the unused pins of the DB25 connector. It is used only for initial configuration of the IP parameters. Thereafter, the **IPMPA** is connected directly to the Network Element and the serial console is no longer used.

The following diagram shows a simple RJ45 to DB25 adapter to connect any **4000**, **4000XA**, **4180**, **4280**, **4284**, Datakit TY, or SAM port to the **IPMPA** console for initial configuration.

The diagram for the console cable is as follows:

RJ45 to IPMPA Console Adapter



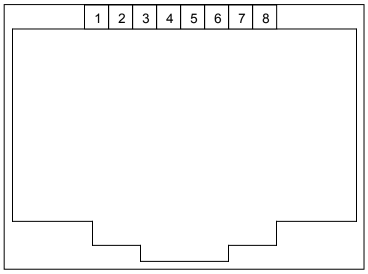


12.3 The RJ45 LAN Crossover Cable

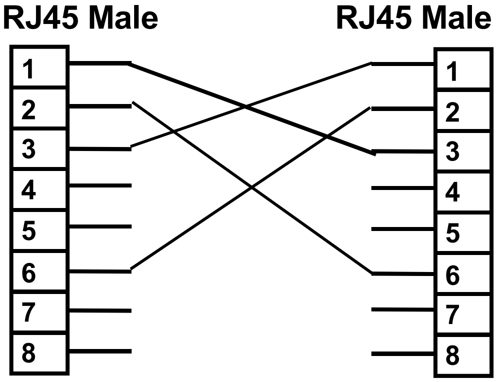
It is sometimes necessary to cross-over the LAN connection. This is used to interconnect equipment without an external Ethernet Hub or Switch.

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



Pin	Symbol	Function	Signal Type
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		



13 SPECIFICATIONS

13.1 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.

13.2 User Serial Port

The RS-232 serial port on the **IPMPA** are either RS-23, or V.35 as configured. They are implemented as a DB25 RS-530 female connector. The **IPMPA** provide data rates up to 115.2Kbps.

13.3 10 BaseT LAN PORT

The **IPMPA** has an 8-pin LAN modular connector is used to interface to a 10/100 Mbps baseband CSMA/CD local area network. The LAN interface is capable of 10BaseT operation.

13.4 PHYSICAL DIMENSIONS

IPMPA	Width = 3.1” x Depth = 4.3” x Height = 1.1” (1.7” w/bracket)

13.5 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.

13.6 POWER REQUIREMENTS

IPMPA Operating Voltage:

Stand-alone AC to DC power supply:	115V @ 9 mA Nominal 115V @ 15 mA Maximum
Stand-alone DC power supply:	48V @ 21 mA Nominal 48V @ 30 mA Maximum

13.7 REGULATORY INFORMATION

13.7.1 IPMPA Stand-Alone

Safety:	UL, CSA, Low Voltage Directive 73/23/EEC
EMC:	FCC Part 15B Class A, ICES-003 Class A, EMC Directive 89/336/EEC
European Teleconnect	TTE Directive TBR 13
NEBS:	Level 3

To maintain compliance with the above-mentioned EMC standards, shielded cables must be used on all **IPMPA** interface connections, and the shields must make an electrical connection to the **IPMPA**'s grounding system.

13.7.2 FCC Part 68 Information

The **IPMPA** complies with Part 68 of the FCC rules. On the bottom of the unit is a label that contains, among other information, the FCC registration number for the **IPMPA**. If requested, this information must be provided to the telephone company.

The RJ45-style jack labeled DSU, located on the front of the **IPMPA*,*** has been tested as part of the registration process for FCC Part 68.

An FCC-compliant modular jack is provided with the **IPMPA**. This jack is designed to be connected to the telephone network or premises wiring using a compatible modular plug which is Part 68 compliant.

If the **IPMPA** causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuation of service may be required. If advance notice is not practical, the telephone company will notify you as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes to its facilities, equipment, operations or procedures that could affect the operation of the **IPMPA**. If this happens, the telephone company will provide advance notice, in order for you to make necessary modifications to maintain uninterrupted service.

If trouble is experienced please refer to the warranty section of this user manual. No repairs can be performed by the user going beyond the scope of the troubleshooting section of this user manual.

13.7.3 Industry Canada CS03 Certification Information

NOTICE: The *Industry Canada* label identifies certified equipment. This certification means that the equipment meets the telecommunications network protective, operational and safety requirements as prescribed in the appropriate Terminal Equipment Technical Requirements document(s), but does not guarantee that the equipment will operate to the user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to connect to the facilities of the local telecommunications company. The customer should be aware that compliance with the above conditions may not rule out degradation of service in some situations.

Repairs to certified equipment should be coordinated by a representative designated by the supplier. Any repairs or alterations made by the user to this equipment may give the telecommunications company cause to request the user to disconnect the equipment.

For their own protection, users should ensure that the electrical ground connections of the power utility, telephone lines, and internal metallic water pipe system, if present, are connected together. This precaution is particularly important in rural areas.

Caution: Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.

13.7.4 NEBS COMPLIANCE

- **GR-1089-CORE NEBS**
  Section 6 DC Potential Difference
  Section 8 Corrosion Requirements
- **GR-1089-CORE NEBS Level 3**
  Section 2 ESD
  Section 3.1, 3.2 EMI Emissions
  Section 3.3 Immunity
  Section 4 Lightning and AC Power Fault
  Section 5 Steady State Power Induction
  Section 7 Electrical Safety Analysis
  Section 9 Bonding and Grounding
- **GR-63-CORE NEBS**
  Section 2 Spatial Requirements
  Section 4.1.3 Altitude
  Section 4.6 Acoustic Noise
  Section 4.7 Illumination Requirements
- **GR-63-CORE NEBS Level 3**
  Section 4.1.1 Transportation and Storage
  Section 4.1.2 Operating Temperature and Humidity Criteria
  Section 4.2.3 Equipment Assembly Fire Test
  Section 4.3.1 Packaged Equipment Shock Criteria
  Section 4.3.2 Unpackaged Equipment Shock Criteria
  Section 4.4.1 Earthquake Environment and Criteria
  Section 4.4.3 Office Vibration Environment and Criteria
  Section 4.4.4 Transportation Vibration Criteria

14 HARDWARE WARRANTY

The warranty period for the IPMPA 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.

15 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.

15.1 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.

15.2 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).

15.3 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.

15.4 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.

15.5 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.

15.6 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.

15.7 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.

15.8 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.

16 Sales & Distribution

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

17 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 or via telephone at 386-754-5700.