COLLISION ELIMINATION MULTIPLE ACCESS
"CEMA"
REFERENCE MANUAL

11/98, III-3

ARIA
WIRELESS SYSTEMS

Table Of Contents

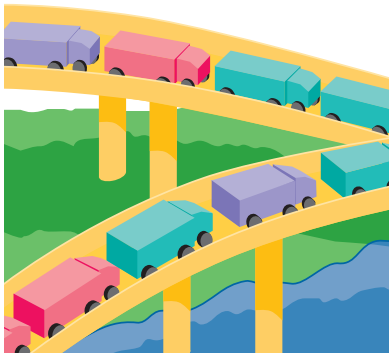
SYSTEM III™

Table Of Contents

1.1 - About this Manual

The CEMA SYSTEM III® Manual is a Reference Guide

This book is the third in a series of four manuals for Users, Installers and Service Technicians. This manual covers the System III software in two parts:



CEMA Software (Section 1-3)

- Description of CEMA and its features
- How CEMA Works
- How to design a CEMA network
- Diagnosing a CEMA network

UserApplications, (Section 4-8) describes:

- Each user Protocol available
- The protocol's features and limitations
- How to configure each protocol
- How to install and interface each protocol

This manual is intended for use by System III network designers and network operators who need a detailed understanding of the CEMA network's system, and how to interface the System III equipment.

It Does NOT Contain

Operation of any of the component equipment - this information is contained in:

Book#	Name
1	IRM Reference Manual
2	Repeater Reference Manual
4	Network Manager Reference Manual

Notes, Warnings and Tables

NOTE

Text in a white box emphasizes information pertinent to a sequential order, or the possibility of damage to the IRM network system.

1.2 - CEMA Description

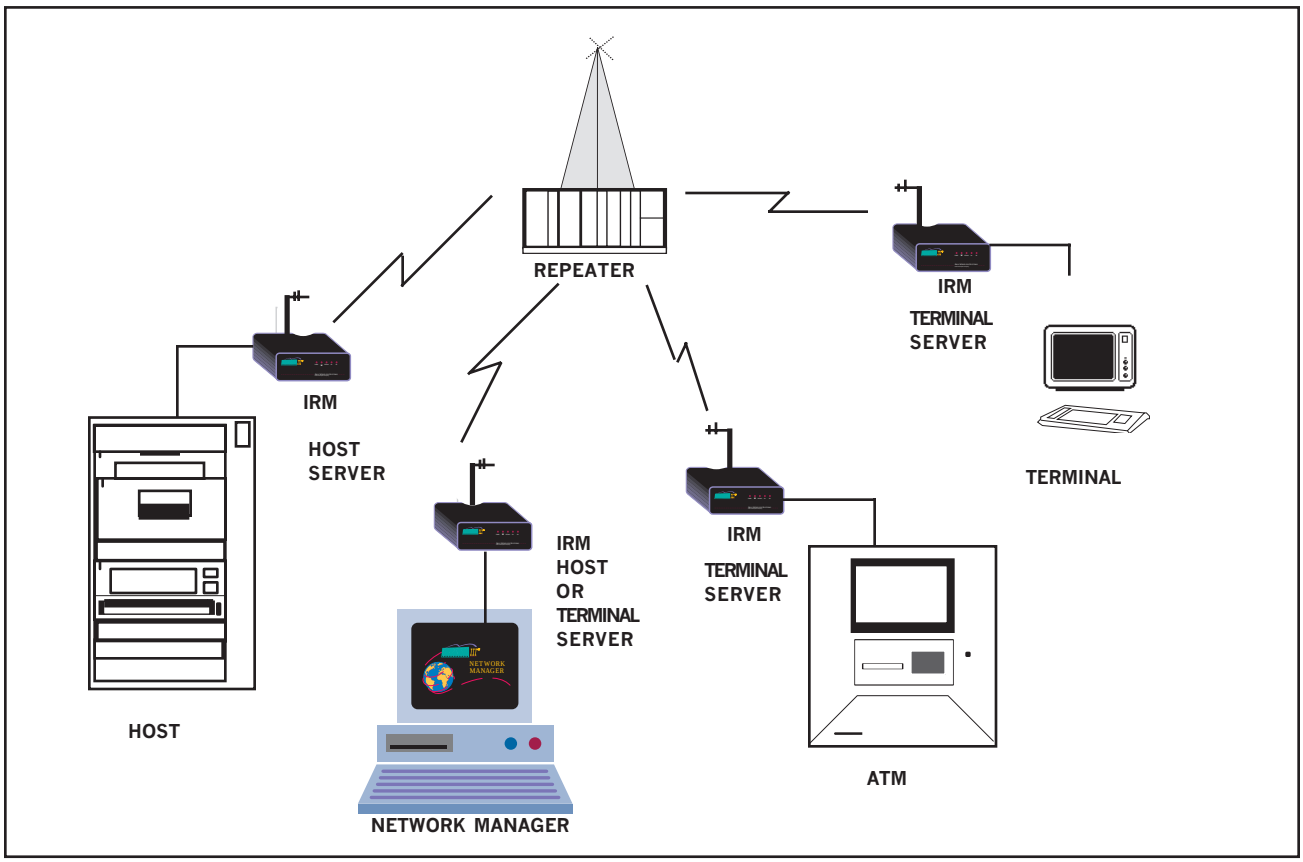
Collision-Eliminating Multiple Access (CEMA) Network

CEMA (SEE-MAH) is a patented, slotted Aloha, multiple access contention protocol with reservation lists. It is specifically designed for radio transmission of transaction oriented data.

Features

- Reliable error-checked data transfer
- Supports multiple users and terminal protocols
- Highly efficient
- Peer-to-peer communications
- Fault tolerant
- Low latency
- Built-in Network management functions

CEMA Sample Metropolitan Area Network



1.2 - CEMA Description

CEMA Protocol

The patented Collision-Eliminating Multiple Access (CEMA) network protocol provides efficient and reliable data transfer from multiple users across a metropolitan area network (MAN). Operating with System II Intelligent Radio Modem (IRM), Repeater and Network Manager Products, CEMA software combines non-polled channel access with user terminal protocol processing to carry data packets efficiently within a wireless MAN.

User Access

In the ISO layered model CEMA performs MAC and Data Link layer functions including reliable error checked data transfer.

Users access the network by submitting a request during contention slot intervals which are reserved at the end of each packet transmission. This mechanism insures uninterrupted data transfer because collisions between simultaneous request-ers can only occur during the contention interval hence the *Collision-Eliminating* feature of the protocol.

Packet Sizes

CEMA transmissions can hold up to eight data packets of 256 bytes each or a total of 2048 bytes of data. This size is optimal for most transaction applications (credit card authorization, remote database access, E-Mail) since these typically contain less than 256 bytes of data.

Error Checking

Error checking is provided by use of a 16 bit CRC (Cyclic Redundancy Code) with positive acknowledgment to the sender of the results of each transmission.

The CEMA Advantage

CEMA provides the network user with significant advantages over other wireless data networks:

Multiple Hosts

A single network may be configured with two or more host computers each communicating with terminals or other host computers over the net. This allows two or more types of financial transactions with different protocols to be carried on the same network.

Fault Tolerance

A dedicated master station is not required. Instead, network control functions are continually handed off from one active remote unit to another. Thus any IRM can come on and off the network when required, and the failure of a single remote unit has no effect on other network traffic.

Collision Free Data Transfer

Unlike CSMA (Carrier Sense Multiple Access) networks, no collisions can occur during transfer of data packets. Instead, CEMA reserves a special contention time period after each packet transmission for nodes to request access to the network. Once nodes successfully contend for network access, their request is placed in a FIFO (First in-first out) queue and interruption free data transmission will occur once the sender's request reaches the top of the queue.

Efficient Data Transfer

CEMA encapsulates user data in a simple packet layout which requires minimal overhead fields. In addition up to eight 256 byte data fields can be combined together into a single transmission. These features can yield transmitted efficiencies of 85% or more compared with less than 50% for

1.2 - CEMA Description

other wireless networks. High efficiency translates into high data throughput and a large capacity of users that a single network can support.

Low Latency

Because of the high network throughput and rapid access time to the network , a CEMA network handles typical financial transactions with very low latency. Any delay imposed by the network is a function of the data packet size, frequency of transactions and the number of network participants.

Reliable Data Transfer

The CEMA protocol supports acknowledgment to the sender of every received packet. This guarantees that every transmitted packet is delivered error free to its intended destination and provides insurance to the user of reliable data transfer. To minimize the effect of acknowledgments on network efficiency, CEMA provides an acknowledgment mechanism combined with the data packet returned to the originator.

Automatic Responder Queuing

When a node successfully contends for access to the network, the recipient node is automatically queued so that it can send its response without waiting for the contention process.

Multicast Messages

CEMA allows a sending node to address its packets to multiple recipient nodes. This capability allows a host computer to transmit common initialization information or other data simultaneously to more than one remote terminal site. This reduces the amount of network capacity needed for such transmissions.

Network Management

CEMA carries the control and status messages required for effective management of network operation from the PC-based Network Manager. The network management functions support network diagnostics, node configuration and error reporting. These functions are compatible with the industry standard Simple Network Management Protocol (SNMP).

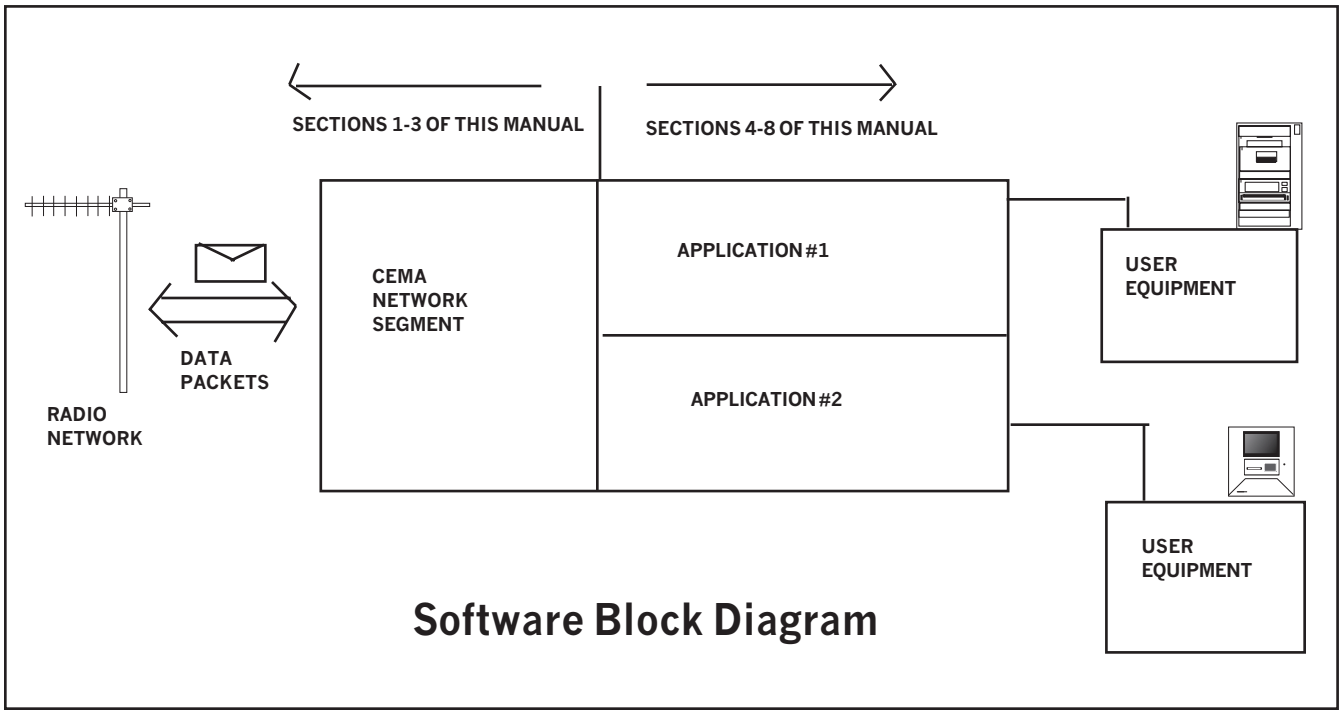
Optimal Performance

These features effectively distinguish CEMA from other wire based and radio network protocols. Moreover, by using features like response with acknowledgment combination and automatic responder queuing, a CEMA network performs optimally when carrying typical financial transactions, which generally consist of a terminal-to-host request followed by a host-to-terminal response message.

User Application Software

Working in conjunction with CEMA are user application modules that interface directly with specific commercially available protocols. Protocol modules are optimized for commonly used terminal protocols such as IBM SDLC (Synchronous Data Link Control) and 3270 Bisync, ISO Poll Select, and X.25. They are integrated into the IRM to allow CEMA to efficiently carry the protocol data on the RF network.

1.2 - CEMA Description



Software Block Diagram

Some of the important attributes of the protocol software are:

Flexible Baud Rates

The terminal baud rate may be different from the network rate to accommodate different speed user devices.

Polling Emulation

Protocol poll commands are never broadcast on the network, but are emulated by the protocol software. If polls were to be broadcast they could easily consume 90% of the network capacity.

Acknowledgment Timing

In order to meet host computer timing requirements, message acknowledgments are often handled by the host IRM. This occurs prior to receiving the real acknowledgment from the remote node.

Multiple Protocols

User protocol frames are interfaced to CEMA such that the CEMA processing of the message data may be independent of the type of protocol. This enables multiple types of protocols to be simultaneously carried on the network.

Data Compression and Security

Compression and encryption (scrambling the data for security) of the incoming data message may be customer-enabled to transfer data efficiently and secure important data.

1.3 - For CEMA 1.7 Users

There are several major changes that distinguish CEMA System III software from CEMA 1.7:

Multiprotocol Capability

Prior to CEMA System III, only a single protocol could be loaded onto a single set of EPROMs; thus each IRM CPU board could execute one (and only one) protocol. CEMA System III eliminates this limitation, providing a mechanism where multi-protocol capability can be obtained within a single IRM CPU.

Quadrupled the Addressing Capacity

CEMA System III separates “node” addresses from “port” addresses. This gives us the ability to increase the network virtual address space from a maximum of 254 addresses to 1016 addresses. In addition, multi-dropped ports (ports that need to address several nodes) can be set up independently from other ports on the same unit; this means that the other ports will not have unused addresses because of the multi-dropped port. These two features change the way nodes and port addressed which is explained further in 3.2.

Node Compatibility

Nodes running CEMA System III can operate on networks containing CEMA 1.7 nodes; CEMA System III is backward compatible with CEMA 1.7, although a node running CEMA System III cannot be paired with a node running CEMA 1.7 (they cannot directly communicate).

Enhanced Contention Mode

CEMA System III has an optional "enhanced" contention mode. In the enhanced mode, the average number of contention slots is reduced to 4, resulting in a 40% reduction in network overhead. This produces a comparable improvement in data throughput over the network for nodes that are configued as "enhanced". There is no effect on older (CEMA 1.7) nodes on the network

Improved Configuration

CEMA System III and the protocols it supports have their own configuration and network monitoring software. All System III units are configured with the Network Manager.

Remote Configuration and Download

All configurable parameters can be remotely programmed over the radio network using the Network Manager. In addition, software updates can be sent over the CEMA network, loaded into non-volatile Flash RAM and then activated without a site visit.

1.3 - For CEMA 1.7 Users

Enhancements Made by CEMA System III

Efficient use of CEMA addresses:

- 1016 port -to port connections
- 508 link possible
- True broadcast and multi-cast capability
- Multiple protocols per CPU - affords any combination to any port.
- Integrated encryption - for secure data
- Integration Compression - uses less band width per transmission
- Increased data throughput

Built-in:

- Diagnostics
- Network Monitoring
- Network Management
- Remote control capability
- Extensive error checking and lost data recovery

2.1 - How CEMA Works

How CEMA Works

CEMA (SEE-MAH) is a patented, slotted Aloha, multiple access contention protocol with reservation lists. It is specifically designed for radio transmission of transaction oriented data.

Peer-to-Peer Contention

A peer-to-peer contention network operates in a manner similar to a group of people conducting a meeting.

Protocol

When people conduct a meeting, there are several ways to communicate efficiently. If all members speak at the same time, the messages become scrambled. Instead, each member waits for a pause in the conversation and then speaks, "contending" for the floor.

If all the other members stay quiet, the speaker is successful. If not, he tries again later. That's how a contention network operates.

Using this contention scheme, there is no master station (Chairman of the Board). All members have equal access and the failure of any one unit does not bring down the network.

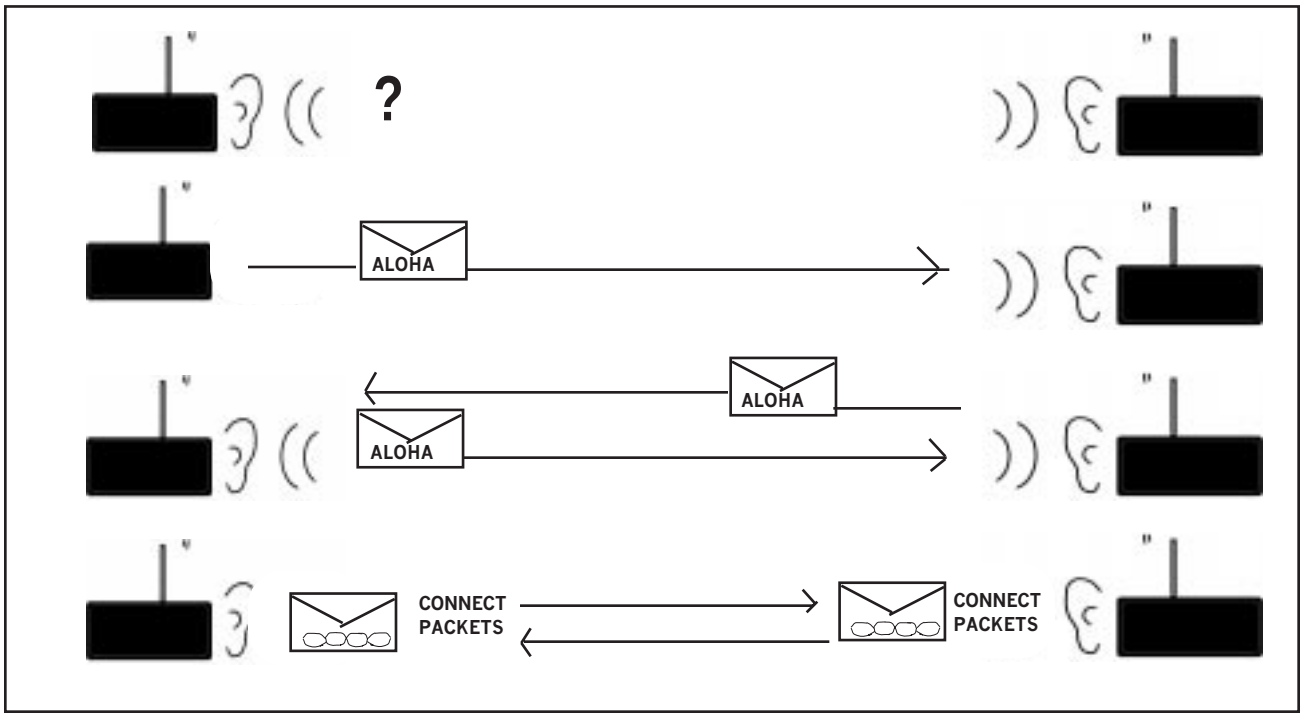
The contention process can be time consuming, so CEMA limits their occurrences to brief time slots, saving more of the time for data transmission.

When a network is first started, the time slot period must be established. This is done by using the standard Aloha (hello) contention network (named after the first network of its kind created at the University of Hawaii many years ago). After the Aloha network is established, the CEMA network synchronization is formed.

2.1 - How CEMA Works

Initialization

You can see the initialization process by experimenting with two IRMs. With two units properly configured to link to each other, monitor the initialization and network activity with the Network Manager.



1. Turn On each IRM.
2. Each unit will first listen to hear if there is a CEMA network operating. If not, they know they must establish one. After several seconds of not hearing any network activity, the IRM will send an Aloha packet.
3. When a unit hears an Aloha packet with its address, it responds with a corresponding Aloha. The IRMs are now time synchronized and can establish a CEMA connection.
4. The IRMs then form a link by sending a sequence of I*nitiate and Connect* packets. When complete, The CEMA network is established and ready to send data.

To maintain CEMA network synchronization, packets will always be sent. If there is no data to be sent, the IRMs will exchange *Arbitration and Version* packets. These are just filler to maintain timing. Once data becomes available, it will replace the filler.

2.1 - How CEMA Works

New CEMA System III feature

After forming the link and establishing the CEMA network, each port of the IRM will exchange Locate/HereIAM packets with its remote partners. The process allows each port to be individually addressed without using a CEMA address. This increases the number of ports you can have on each network. Multiple port addressing allows for more efficient use of addressing space, while maintaining compatibility with older networks.

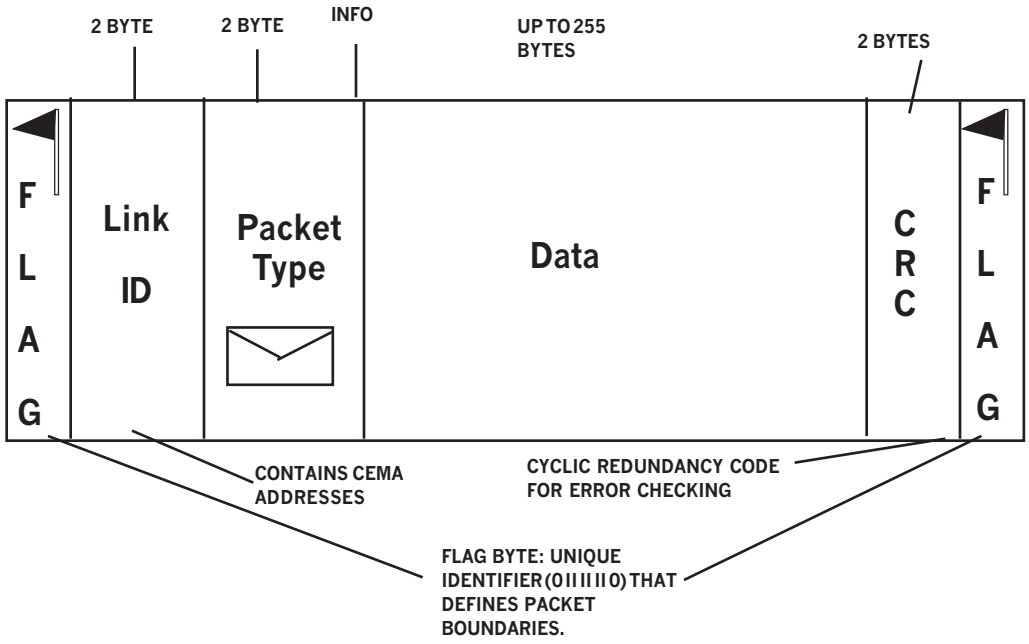
Network Startup Sequence

NETWORK ACTIVITY	RESULT
1. *ALOHA* exchange	Network synchronization established
2. Send *Initiate/Connect* packets	Node-to-node link is established
3. Send Locate/Here I AM packets	Port-to-port link is established
4. Send protocol startup information	Polling emulation begins (if applicable)
5. Send or receive *data* message	
6. Send *arbitration* packets (filler)	Maintains network synchronization

2.2 - Network Operation

Packets

The IRM uses packets to insure accurate transmission of user data. Data from the user Data Terminal Equipment (DTE) is bundled prior to transmission into units called packets. When the packet arrives at the destination IRM, it is verified for accuracy and sequence and is then unbundled to be passed on to the destination user DTE.



IRM Radio Packet Format

Packet Types

The following table lists all different CEMA packet types and describes how they are used.

2.2 - Network Operation

Message Type	Meaning
Arbitration	Used to pass network control from one node to another. Also called a "handoff" packet.
Broadcast	A class of messages destined for simultaneous transmission totwo or more nodes. CEMA messages LOCATE, HEREIAM, CHOKE, UNCHOKE, UNCHOKE_ACKNOWLEDGED and NODE_STATUS belong to this class.
Connect	The response to a CEMA initiate message, which is used to connect a pair of nodes to the network.
Data/Init Data	Message type used to pass non-broadcast "*user*" data from one node to another. *Init Data* packets are always sent as a first frame of a data transmission, while *Data* packets are always sent if there are subsequent frames in the same transmission.
Retransmission Delay	Used when a link partner fails to respond to arbitration transmission.
Initiate	This is a connection request to a partner node (or nodes). If the partner is functional, it will send a *connect* message in response to the *initiate,* causing the two nodes to logically link up.
Unknown	Displayed by Network Manager when it receives a unrecognized message type. This message type is never intentionally transmitted over the network.
Aloha Init/Aloha Response	The message types sent when an IRM powers up, and, after listening for 15 seconds, determines that there is no active network. The IRM will send an "Aloha Init" and expects its partner to send an Aloha response. If this occurs, the two IRMs will begin the standard *Initiate/connect* sequence.
Management Service	Used to send information messages to the Network Manager. This class will also be used to send messages from the network manager to one or more nodes. "Broadcast" Messages are a subclass of this type.
Network Controls	Used to send a disconnection notice - some node is being disconnected because of its failure to respond (or to take control of the network).
Reconnect/Recover/ Reinit	Message types used to reestablish communications with a partner. In some cases (typically when reception has been blocked for only a few seconds) a full session *Initiate/Connect* is not necessary to reestablish a connection; one of these message types is used instead.

2.2 - Network Operation

Message Type	Meaning
SNAC Packet	The acknowledgment to a Data/Data Init message. CEMA guarantees delivery of every data packet by sending an acknowledgment of the receipt of each packet back to the sender. If that acknowledgment cannot be "piggybacked" onto a return data packet, it is sent in a SNAC packet instead.
User Controls	Used by different protocol emulations to send commands (rather than data) across the network. This message type is typically used to send flow control and mode changing commands. It is used only by CEMA 1.7 nodes.
Transport Controls	Used by Async protocol for flow and modem control.
Version Packet	This is an "idle" packet. It is sent by a node when that node has nothing else to transmit.
DataLink Controls	Used to send CEMA link-level commands to a partner node. Currently, none are defined.

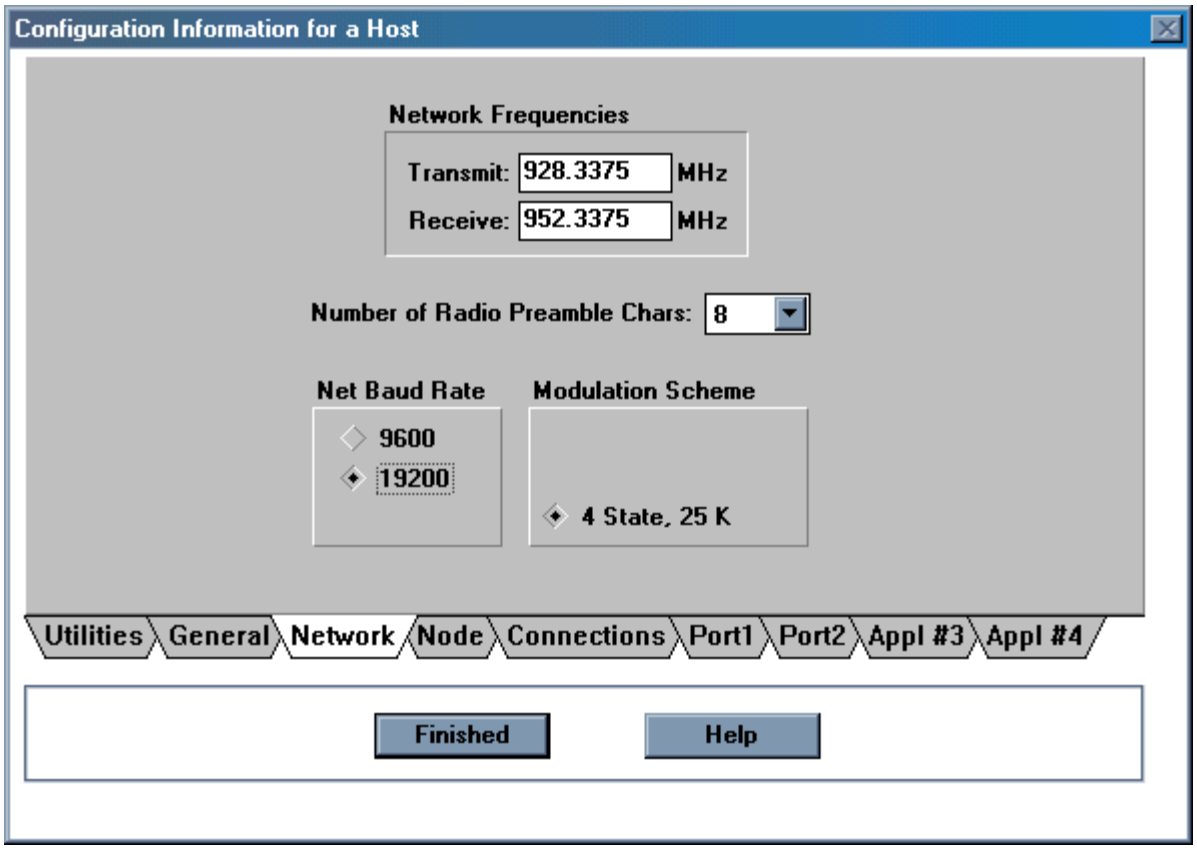
3.1 - Network Design

Designing a CEMA Network

Because the IRM is a relatively complex combination of hardware and software subsystems, it is important to follow an orderly procedure by which the unit is powered up, configured and connected to the network. This manual assumes that the IRM hardware subsystems have been assembled and properly configured, and that the CEMA System III EPROMs have been installed on the IRM CPU card.

NOTE
CEMA System III EPROMs are not compatible with the CPU boards that execute CEMA 1.7 software. A CEMA System III digital CPU board must be used with CEMA 2.0 EPROMs.

Once the software is installed and the IRM is powered up, configure your network using the Network Manager. From the *Network* window:



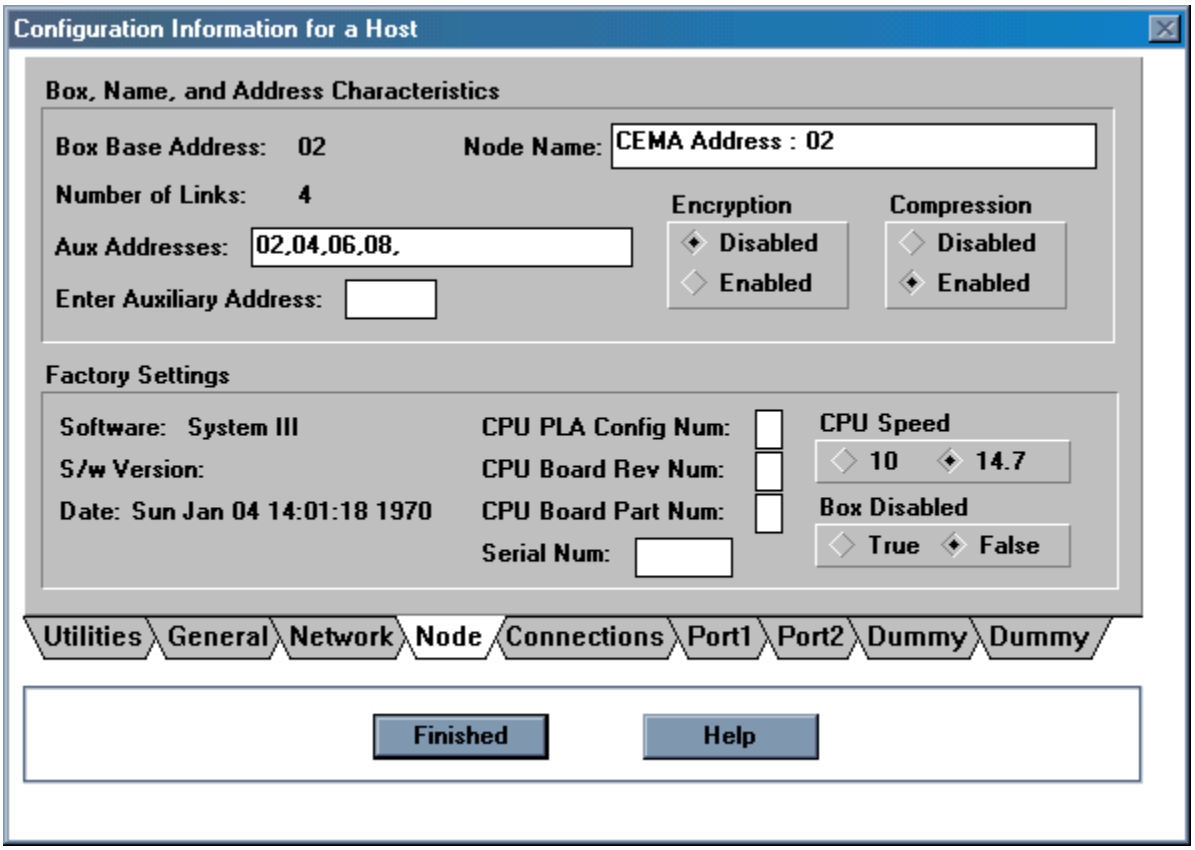
FROM THE MAIN CONFIGURATION MENU, CLICK ON NETWORK TAB TO CALL UP THE NETWORK CONFIGURATION PAGE .

1. Specify the radio transmit and receive frequencies.

3.1 - Network Design

2. Specify port and node addresses for each unit on the network

3. Specify the individual port



3.1 - Network Design

parameters. These depend on the chosen user protocol (i.e: IBM, SDLC, X.25).
This will is discussed in the Network Manager (Book #4) Reference Manual.

There are two methods of configuration:

• Local - PC connects directly to the IRM
• Remote - modifications are made over the radio network

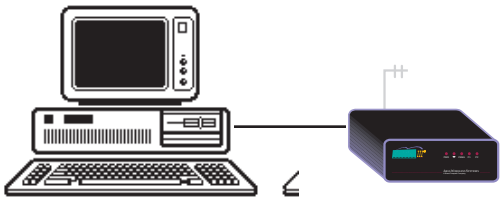
Local is recommended for initial installation or when a change is necessary and the CEMA network is not up.

Remote configuration is for minor modification on an operational unit. It has the advantage of saving a trip to the remote site. Performing a Configuration:

Configuring a Port

Local - physically connecting the COM port of the Network Manager PC, to an IRM port. This method is recommended for installation.
Remote - configurations are transmitted through RF on an operating CEMA network. Use remote configuration for minor changes, not installation.

Configure only those ports that are actually going to be used; the other ports should be set to *disabled* (this will be discussed later in the manual). Alternatively, if spare ports are available, one can be configured as a diagnostic message port, and one can be configured as a Network Manager output port - this will aid field engineering and troubleshooting, should problems arise.



LOCAL CONFIGURATION - DIRECT CONNECTION BETWEEN PC AND IRM.

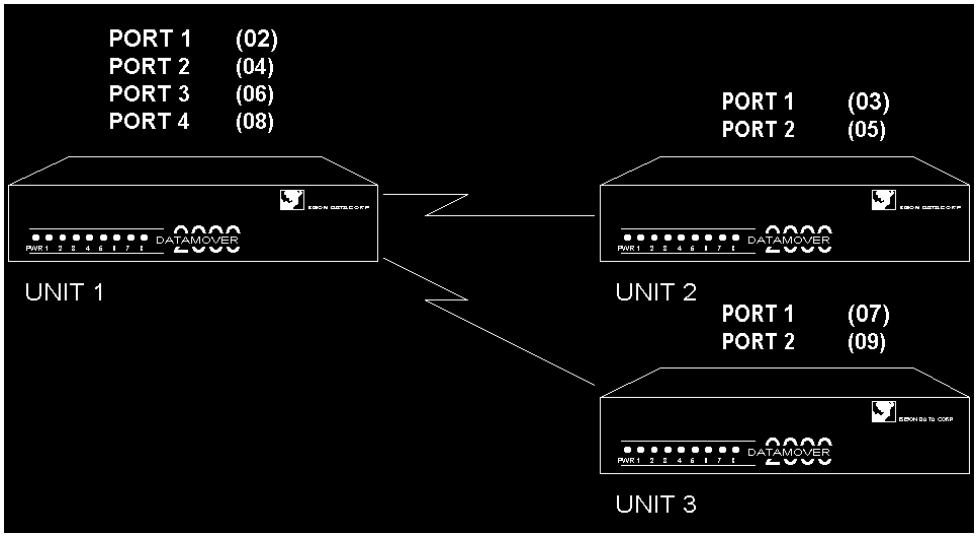
3.2 - CEMA Addressing

CEMA Addressing

CEMA allows for a maximum of 254 addresses. However, instead of using a pair of CEMA addresses to connect one port to its partner port (as does CEMA 1.7), CEMA System III uses a pair of addresses to connect one unit to a partner unit. The distinction here is that CEMA 1.7 would take 4 pairs of addresses (8 total) to multidrop a single port on a single DataMover to 4 ports on some other DataMover. Using CEMA System III, only one pair of addresses (2 total) are required.

In the following example, Figure 1 represents the addressing scheme used by CEMA 1.7. Each port is identified by a unique CEMA address. Figure 1 shows unit 1 on the left (the host) connected to units 2 and 3 on the right (the remotes); port 1 of the host connects to ports 1 and 2 of the first remote and to ports 1 and 2 of the second remote. CEMA 1.7 requires that 4 pairs of addresses be used: Address 02 is linked to address 03, address 04 is linked to address 05, and so on.

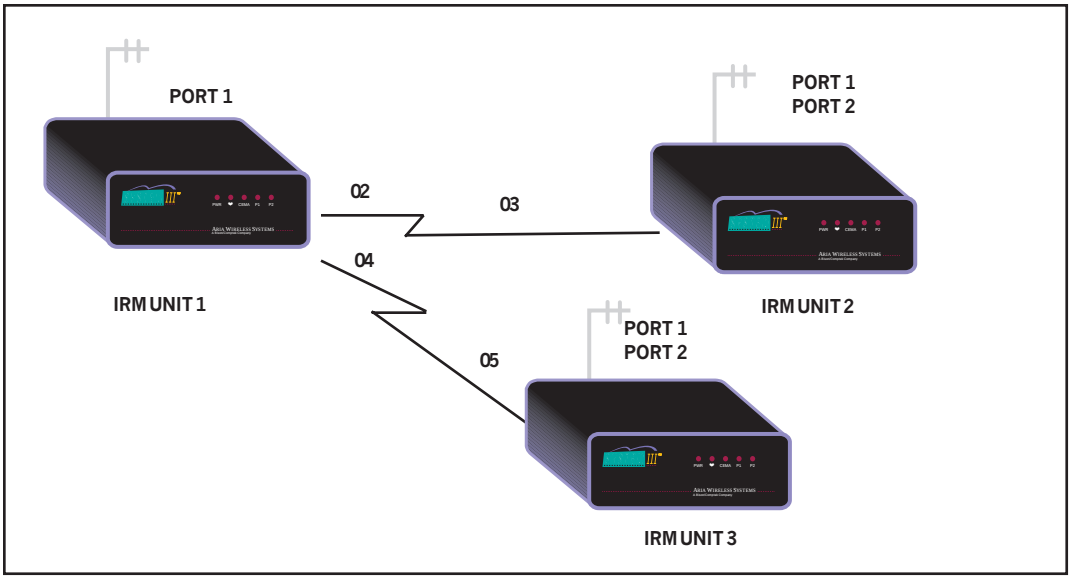
Figure 1: CEMA 1.7 Addressing



3.2 - CEMA Addressing

Now look at Figure 2. Since CEMA System III connects nodes to nodes (not ports to ports), only two pairs of addresses are needed: Address 02 is paired with address 03 (connecting node 02 to node 03) and Address 04 is paired with address 05 (connecting node 04 to 05). Unit 1 utilizes two CEMA addresses (02 and 04), while units 2 and 3 utilize one CEMA address each.

Figure 2 : CEMA System III Addressing



3.3 - Port to Port Addressing

Port to Port Addressing

So how are port-to-port connections made using CEMA System III? In addition to CEMA-level addressing, individual ports must be assigned unique “source” and “target” names. The “source” name is the name that you assign to each specific port on the IRM. The “target” name is the name that you assign to the other end of the connection. These names can be any combination of printable characters up to 3 characters in length. When a IRM is powered up (or reset), the names given to each port are broadcast over the network. Each “source” name is specified with one or more “target” names to which it wants to connect. As individual IRMs receive them, the port names are examined to determine if the receiving IRM contains a matching name and if so, then the source and target ports are logically connected.

The source and target names are assigned automatically by the Network Manager. It uses the convention of "llp" for the port name where:

ll = CEMA Node/Link number
p = port number

For example, host server node 02, PORT 1 would have source mode "021".

In summary, port-to-port addressing is now a two-step process in CEMA System III. First, nodes are paired by unique, consecutive numeric address. Then ports are paired by unique name.

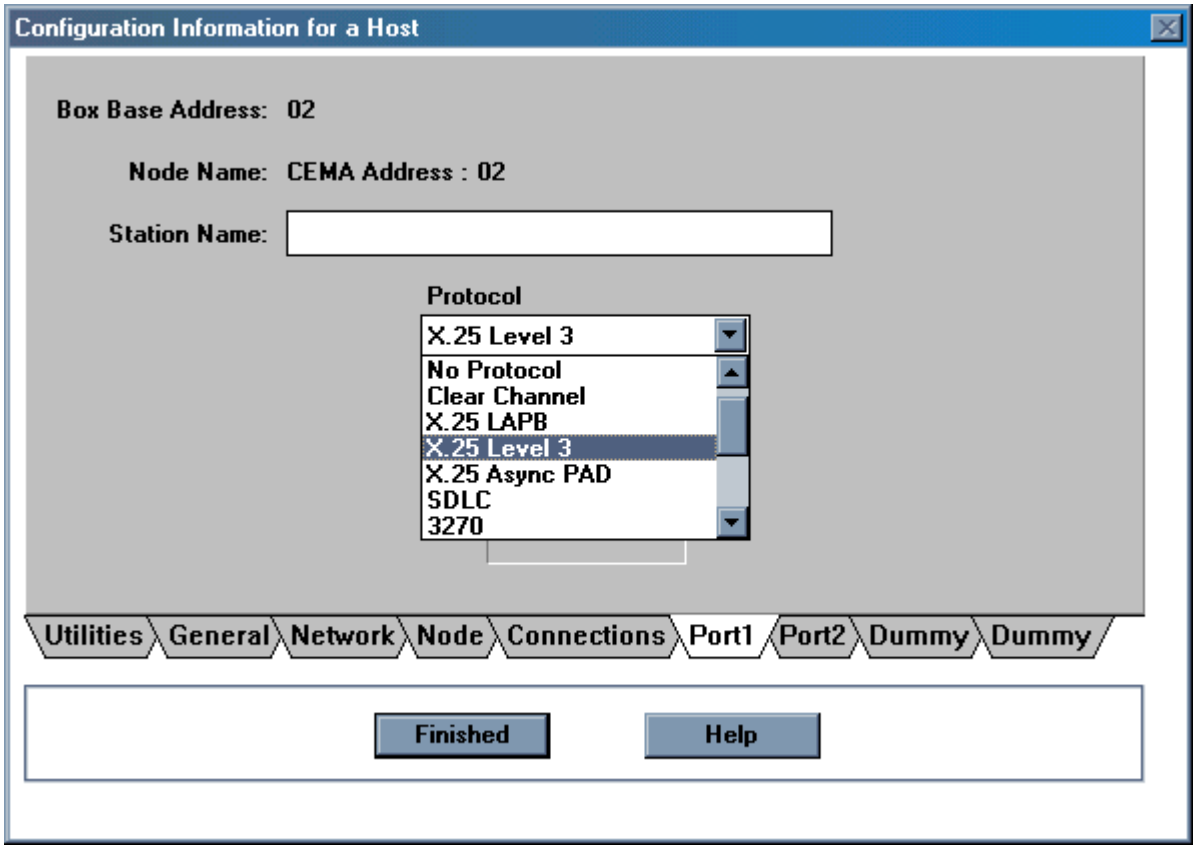
Multicast Capability

Beginning with CEMA System III, multicast transmission capability can be utilized on the IRM network. Multicasting gives an IRM the ability to send (broadcast) a single message that can be addressed to more than one node. Prior to CEMA System III, multicasting was emulated by retransmitting a multicast message to each individual node in the multicast group. This led to computational and memory loading problems and made for inefficient use of the network.

Although not used by any of the currently-supported protocols, multicasting will be used by multidrop protocols such as IBM 3270 and SDLC, when they become available on the CEMA System III baseline.

3.4 - Protocol Selection

Protocol Selected per port



3.5- Compression

Data Compression

Data compression can now be configured on a port-by-port basis. The IRM's compression algorithm is a simple repeating character compression (called run-length encoding); strings of four or more repeating characters are replaced by a three-byte code. This significantly reduces the size of data packets feeding display terminals and printers, which tend to contain strings of blanks and nulls, respectively. We also observe a small reduction in the size of a typical financial transaction packet, since such packets generally contain short strings of blanks or zeroes.

Depending on the size of the data frame, it may take from 0.7 to 30 milliseconds to perform data compression. We recommend that data compression be used, since it helps conserve radio network bandwidth (albeit at the CPU's expense).

3.6 - Encryption

Data Encryption

Like data compression, data encryption can now be configured on a port-by-port basis. The IRM's encryption algorithm converts the data received from customer terminals into an encrypted character stream (ciphertext) prior to transmission over the radio network. This feature effectively provides IRM users with privacy and security for their sensitive financial transactions and textual data.

The encryption scheme utilizes a symmetric private key technique based on a method originally described in 1918 by AT&T Bell Laboratories engineer Dr. Gilbert S. Vernam[1]. The algorithm was further refined in 1949 by AT&T scientist Claude Shannon[2]. Vernam's method utilizes the simple algorithm:

> Ciphertext = Random Cipher XOR Data Stream where the same algorithm is used to both encrypt and decrypt the data stream.

Vernam proved that the Exclusive OR (XOR) of a random character stream and a fixed data stream is also a random character stream, hence denying useful information to the casual observer of the encrypted data. The method also removes from the ciphertext all of the frequency information, inter-symbol correlation and periodicity which experienced code breakers use to decipher encrypted data encoded with fixed keys. To insure the continued random nature of successively transmitted data, the random cipher is continually updated throughout the duration of a session between a given terminal and host computer port.

Encoding and Decoding Messages

The IRM employs the Vernam algorithm to both encode and decode messages. In order to successfully decrypt the received messages, the receiver must utilize the same randomly varying key as used to encrypt the data stream. To accomplish this key synchronization, each IRM employs identical pseudo-random number generators to generate the random cipher bits. Provided it is initialized with the same seed, each pseudo-random number generator will generate the same pseudo randomly varying key values. Thus to maintain data protection the random number generator seed must be passed in a secure manner between transmitter and receiver.

Random Numbers

At the beginning of a session between two IRMs, identical random number generator seeds are independently derived by the IRMs at each end of the link. Using random parameters unique to each IRM, different initialization keys are generated by the receiver and transmitter. Then using a secure transfer method, a derivative of the key is exchanged between each IRM. Following this exchange, each IRM independently calculates the seed from which the initial random cipher is derived.

By employing the Vernam cipher together with the secure initial key passing technique, a robust, difficult to break data protection is obtained. The algorithm is estimated to require in excess of 2^{112} (10^{33}) attempts to randomly break the code. Further information about the Vernam and other encryption techniques can be found in a 1979 article by Gustavas Simmons[3].

[1] VERNAM, G.S. "Cipher Printing Telegraph System for Secret Wire and Radio Telegraphic Communications", J. AIEE 45, Feb 1926, pp 109-115

[2] SHANNON, C.E. "Communications Theory of Secrecy systems", Bell Systems Technical Journal, October 1949, pp 623-656.

[3] Simmons, G.S. "Symmetric and Asymmetric Encryption", ACM Computer Surveys, December 1979, pp 305-330.

3.6 - Encryption

Synchronization

Data encryption requires synchronization between the sending and receiving IRMs. Should synchronization be lost (because of either hardware or software failure), the IRMs will logically disconnect from each other and reconnect, forcing resynchronization. Under normal operating conditions you will not observe synchronization problems, but under extreme conditions (poor radio reception, extremely high data rates) it is anticipated that some synchronization problems could occur.

Depending on the size of the data frame, it may take from 0.7 to 30 milliseconds to perform data encryption. This additional processing load on the CPU must be considered before enabling encryption, although noticeable system degradation will occur only in the most extreme loading conditions.

3.7 - Network Tuning Parameters

Network Tuning Parameters

There are several parameters that can be changed to optimize the CEMA network performance.

> **NOTE**
> These parameters can severely effect network operation. They should not be changed without consulting the factory first!

The following table lists each network parameter and its meaning. These can be changed only via a special purpose Network Manager window.

Description	Meaning
Flow Control Timeout	The amount of time (in seconds) that a flow control condition is allowed to persist at the CEMA level before the box is reset. Chronic flow control conditions typically arise when the IRM starts running out of memory. For example, if the IRM cannot complete a buffer-releasing operation because some transaction has not yet completed, yet that transaction needs to receive more data frames before it can complete, a chronic flow control condition will arise if there is not enough memory left to receive the data frames. This timeout is used as a last resort to prevent the IRM from locking up. The default value is 60 seconds.
Stalled Port Timeout	Once a port transmission or reception has been started, a timer is maintained to determine if subsequent bytes are being written to or read from the port. If the port stalls for any reason, the port (not the IRM) will be reset after this timeout expires. The default value is 10 seconds.
Locate Message Tries	The number of times a LOCATE message is broadcast over the CEMA network. LOCATE messages are sent by each IRM as part of the algorithm used to logically connect two ports. Since these messages are broadcast, there is no guarantee that they will be delivered. To provide an extremely high probability that all nodes receive the LOCATE message, this parameter is used to determine the number of times that the message will be transmitted. The default value is 3. On CEMA networks with poor radio reception, it may be necessary to raise this value.

3.7 - Network Tuning Parameters

Description	Meaning
Locate Message Timeout	The minimum period (in seconds) between LOCATE message transmissions. The default value is 8 seconds.
HEREIAM Message Tries	The number of times a HEREIAM message is broadcast over the CEMA network. HEREIAM messages are sent in response to a LOCATE message (and also whenever the IRM is powered up or reset) as part of the algorithm used to logically connect two ports. These messages are broadcast over the network. This parameter is used to determine the number of times that the message will be transmitted. The default value is 2.
HEREIAM Message Timeout	The minimum period (in seconds) between HEREIAM message transmissions. The default value is 2 seconds.
Choke Message Tries	The number of times a CEMA-level CHOKE message is broadcast over the CEMA network. Sending this message a number of times provides a high degree of certainty that the CHOKE (flow control) will be received by all nodes. The default value is 2.
Choke Message Timeout	The minimum period (in seconds) between CHOKE message transmissions. The default value is 2 seconds.
Unchoke Message Tries	The number of times a CEMA-level UNCHOKE message is broadcast over the CEMA network. Sending this message a number of times provides a high degree of certainty that an UNCHOKE (flow control disable) will be received by all nodes. The default value is 2.
Unchoke Message Timeout	The minimum period (in seconds) between UNCHOKE message transmissions. The default value is 2 seconds.
Node Status Max Timeout	The maximum period during which an IRM may idle without transmitting a message on the network. If the IRM has not transmitted anything for this period, the NODE STATUS message will be transmitted. The node's "health" can be determined by observing this message on the Network Manager. The default is 900 seconds (15 minutes).

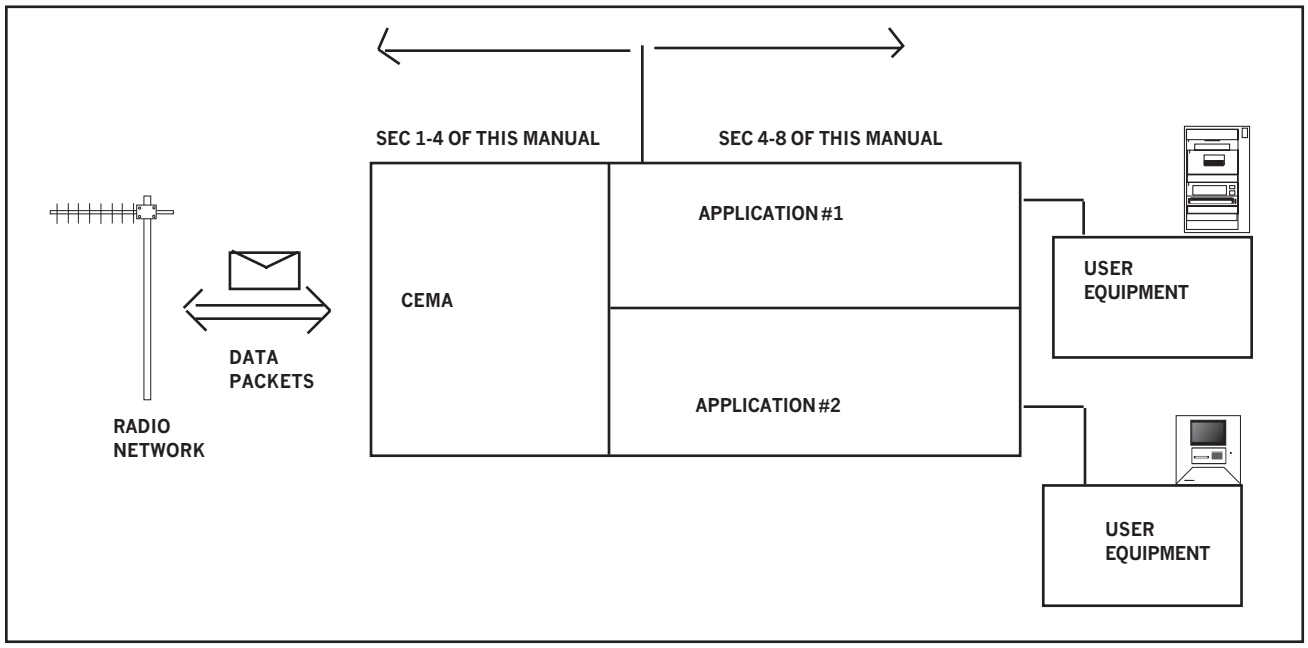
3.7 - Network Tuning Parameters

Description	Meaning
Max Chars/ Encryption Attempt	This parameter specifies the maximum number of bytes in a data frame that will be encrypted during a single pass through the encryption algorithm. Specifying a small number of bytes spreads the encryption effort out over time, which minimizes CPU overhead but takes the encryption longer to complete. Specifying a larger number of bytes allows encryption to complete rapidly, but takes considerable CPU overhead during that period (and may cause other critical events to be delayed or missed). The default value of 28 will cause a typical 100-byte data packet to be encrypted over 4 passes, with roughly 10 msec between passes (total delay: 40 msec). For those applications where encryption is required and the processing load is light, it is possible to raise this value (the maximum is 99).
Max Chars/ Compression Attempt	This parameter specifies the maximum number of bytes in a data frame over which compression will take place during a single pass through the compression algorithm. The default is 28 bytes. For those applications where the processing load is light, it is possible to raise this value to a maximum of 99.
Maximum Broadcast Delay	The average delay period (in seconds) between broadcasts. Many broadcasted messages are in response to another broadcast; to prevent these broadcasts from occurring simultaneously across all nodes (and overloading the network) each broadcast is delayed a random amount of time between 0 and the Maximum Broadcast Delay. The default value is 3 seconds.

4.1 User Applications - Introduction

Introduction to the User Applications Section

CEMA software as it applies to the *user* will be addressed in the following sections (SEC 4 through SEC 8). CEMA software allows multiple *application modules* to run as interfaces to the specific equipment. Two *application modules* are provided to interface to specific System III components: The Network Manager and the Diagnostic Monitor.



The application module designed to interface with user equipment is sometimes called a *user protocol*. These interface modules provide protocol emulation or some other intelligent means to:

- Provide a seamless connection of user equipment to the system III network.
- Reduce data traffic on the radio network by compressing the data, eliminating polling and acknowledgments.
- Maintain flow control and re-transmit data on errors.

Any port on an IRM can be configured to run any *application module*.

4.1- UserApplications Introduction

Each Application module is explained in the following sections:

Section	Application
4	Network Manager Application - provides the interface between the PC-based Network Manager utility and the System III radio network; and Diagnostic Monitor - provides insight to the inner workings of the software.
5	X.25 - CCITT compliant emulation software for the internationally standard packet switching system.
6	ISO Poll/Select - provides polling emulation for a variety of poll/ select protocols, including Burroughs Poll/Select and 3201.
7	3270 Bisync - provides the polling emulation for older IBM Bisync equipment.

4.2 - Network Manager

Network Manager Application

Prior to CEMA System III, the Network Manager application was available only as a separate set of EPROMS requiring a dedicated IRM. Network Manager can now be configured onto any spare port of a CEMA System III IRM.

Network Manager gives you the capability to observe all radio network activity. All received radio packets are formatted and transmitted out the selected port. When received by the PC-based Network Manager program (via the PC's COM port), these packets can be displayed and analyzed to determine network performance.

The Program

The PC-based Network Manager program is a separate program used to capture and display network messages received from the IRM's Network Manager protocol. A complete description of this program's operation and capabilities can be found in Book #4, Network Manager Reference Manual.

The Protocol

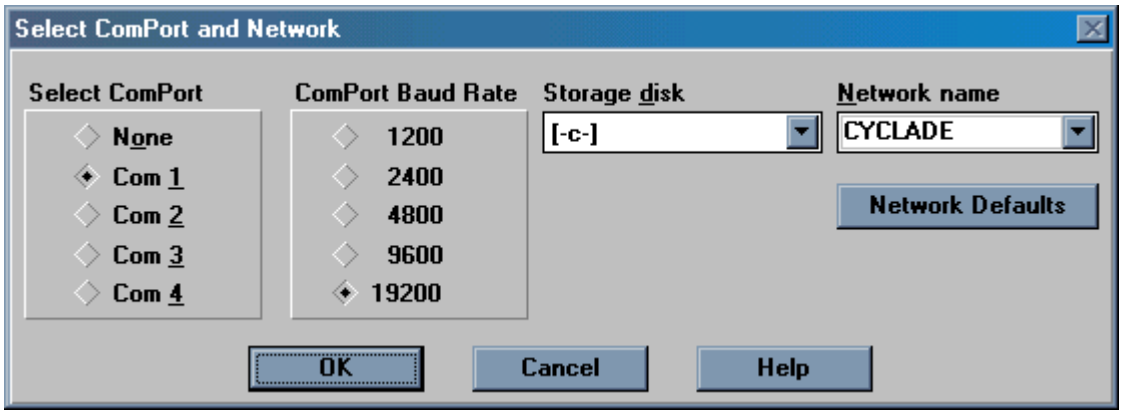
The Network Manager Application can be configured to output a subset of the available network packet types. For example, "idle" packets (such as the Version and Arbitration packet types) do not normally provide information about network performance; output of these packet types can be disabled in order to reduce both IRM processing overhead and the data traffic between the IRM and PC. Any or all packet types can be disabled or enabled.

Selectable Port Baud Rate

Port baud rate is selectable, so that Network Manager can be connected directly to a PC's COM port (at high baud rates 19,200) or to a modem (at low baud rates up to down to 1200) for remote Network Managing. When selecting a port baud rate less than the network baud rate, you will be forced to output only a subset of all network messages (otherwise, the IRM will simply buffer them until it runs out of memory and then it drops messages). For these situations we recommendedusing message filters.

4.2 - Network Manager

Network Manager Protocol Parameters Menu



SETUP WINDOW

LED Display

When the Network Manager Application is selected for a particular port, that port's LED will flash at a 2Hz rate, or at twice the CPU LED rate. When a port LED has this indication, it means the port is ready to accept Network Manager commands and send Net Activity Messages.

4.3 Diagnostic Monitor

Purpose of the Diagnostic Monitor

The purpose of the Diagnostic Monitor is to provide field service engineering with information regarding the internal operation of the IRM. Many internal error conditions can arise that are caused by either hardware or software anomalies. Some of these will cause the unit to be reset (in the hopes of clearing the problem) while others are simply noted in order to allow processing to continue as best as possible. Still other conditions arise that are not necessarily errors but may indicate that the IRM is not performing as expected.

IRM Configuration

The Diagnostic Monitor can be configured onto any spare IRM port; it will output any diagnostic messages to this port, to be received by any terminal connected to it. In the lab, we connect the Diagnostic Monitor to a PC running a standard communications program such as ProComm®, so that we can capture the information, save it to disk and analyze it should we observe any errors.

Once a minute (this is the default time period, which is configurable) the Diagnostic Monitor outputs a line of text consisting mostly of numbers, that looks like this:

aaa:bb MEM: cema|ccc appl*ddd*|*eee* rsys (L)*fff*|(S)*ggg*

The meaning of these numbers (moving from left to right) is on the following table.

Diagnostic Monitor Periodic Output

Parameter	Description
aaa:bb	Elapsed time (in hours:minutes) since the IRM was last powered up or reset.
cema|*ccc*	The number of available CEMA Network-level buffers. These buffers are used only by CEMA.
appl*ddd*|*eee*	First Item: The number of protocol-level memory packets available to all protocols. One packet is used per message, regardless of the protocol. Second Item: The number of protocol-level memory buffers available to all protocols. A buffer has room for 28 bytes of data. One or more buffers are used per message (depending on message size), regardless of protocol. The buffers are used by all protocols.
rsys (L)*fff*|(s)*ggg*	The number of available buffers in the ring buffer system. This is used in the X.25 and SDLC type protocols only. *fff* is the number of large buffers available and *ggg* is the number of small buffers.

4.3 - Diagnostic Monitor

Other diagnostic messages are displayed as an error or anomaly occurs. A complete list of all general diagnostic messages can be found on the following pages of this section. Diagnostic message descriptions for the specific protocols are found in the individual protocol sections.

Diagnostics will change as IRM protocol software is modified and as new protocols are added to CEMA System III.

Diagnostic Error Messages

There are about 300 diagnostic messages that have been added to System III in order to provide the service technicians with some information when internal problems arise. While we strive to offer a perfect product, it is unreasonable not to expect some programming errors. If and when they do occur, the diagnostic messages provide us a window into the software and give us clues as to the cause of the problem. This, in turn, helps us to more quickly correct the problem.

Diagnostic messages are sent to any IRM port configured with the Diagnostic protocol. The default output from this port is 9600 baud asynchronous, 8 bits no parity, 1 stop bit. Any terminal that conforms to VT100 emulation can be used to display the output. A PC running a communications package such as ProComm can also be used (although you will have to configure ProComm to force CR/LF, and translate LF characters (10 hex) to CR characters (13 hex).

You are not required to reserve a port for the diagnostic monitor. However, if one is available, it is useful to configure it as a diagnostic port, since this will aid field engineering should a problem arise later.

Fatal Error Messages - Known Causes

The following table describes fatal error messages (from a known cause) that are sent to the diagnostic port. These messages are also sent over the network so that they can be displayed using the Network Manager.

Non-Fatal Error Messages

Most of the messages that are displayed on the diagnostic monitor are non-fatal. However, they may be symptomatic of some underlying problem that eventually results in a catastrophic failure. For this reason, we usually output, whenever possible, a diagnostic message at the first sign of trouble. Many of these messages simply indicate that a scheduled operation could not be performed (because the network was down, IRM memory was unavailable, and so on), while others indicate that an unresolvable problem occurred and that the IRM will try to continue in spite of it.

Because of the sheer volume of the messages and the limited amount of ROM available, most messages are very brief (and often cryptic). The following table lists all non-fatal diagnostic error messages and offers a brief explanation of what they mean.

4.3 - Diagnostic Monitor

Fatal Error Messages Sent to the Diagnostic Port

Message	Description
Chronic Applications Choke	Protocol emulation software was in a persistent flow control position caused by some internal problem (typically, the IRM has run out of available memory. When this condition persists for a long period of time (about 90 seconds), the IRM is reset.
Chronic CEMA Choke	The CEMA software was in a persistent flow control position caused by some internal problem (typically, the IRM has run out of available memory. When this condition persists for a long period of time (about (about 90 seconds), IRM is reset.
I_BMON:Out of Memory IX25_Initialize DOPEALLOC Failure 1 DOPEALLOC Failure 2 I_FRMLVL INIT Failure FRINITIALIZE T_CREATE: OUT OF MEMORY DOPE VECTORS R_INIT: OUT OF MEMORY	The X.25 Protocol has signalled one of several fatal errors, all due to lack of available memory at initialization. As a temporary solution, reduce the number of ports running X.25 and see if the problem disappears.
***CRASH: [Followed by a screen of information]	A fatal error has occurred and the IRM has been reset. The "crash dump" provides information about the state of the hardware and software at the time of the crash. If a persistent fatal error occurs, we recommend using PROCOMM or some other terminal emulation program to capture the screen image to disk and send it to ARIA Wireless Systems for review.

4.3 Diagnostic Monitor

Non-Fatal Error Messages Sent to the Diagnostic Port

Message	Description
APP_MSG Error # 1 *nn* (On this and subsequent messages, the value*nn* is a status further detailing the error)	The IRM was unable to append data to a message being broadcast to the network. Most likely cause: out of memory.
APP_MSG Error #2*nn*	The IRM could not broadcast a LOCATE message to the network. Most likely cause: network is down or choked.
APP_MSG Error #4*nn*	The IRM could not broadcast a LOCATE message to the broadcast queue. Most likely cause: programming error. This error indicates that the broadcast queue is probably corrupted.
APP_MSG Error #5*nn*	Could not find the handle to a timer being used to periodically send LOCATE messages. Most likely cause: no more timers available.
APP_MSG Error #6*nn*	Could not broadcast a timed message. Most likely cause: network is down or choked. An attempt will be made to broadcast the message at some later time.
APP_MSG Error #7*nn*	Number of bytes in received LOCATE message does not match the expected number of bytes. Most likely cause: version mismatch between paired IRMs.
APP_MSG Error #10*nn*	Could not broadcast HEREIAM message. Most likely cause: network is down or choked.
APP_MSG Error #13*nn*	Could not add a HEREIAM message to the broadcast queue. Most likely cause: programming error. This error indicates that the broadcast queue is probably corrupted.
APP_MSG Error #14*nn*	Could not find the handle to a timer being used to periodically send HEREIAM messages. Most likely cause: no more timers available.
APP_MSG Error #16*nn*	Number of bytes in received HEREIAM message does not match the expected number of bytes. Most likely cause: version mismatch between paired IRMs.

4.3 Diagnostic Monitor

Non-Fatal Error Messages Sent to the Diagnostic Port

Message	Description
APP_MSG Error #22*nn*	Could not broadcast CHOKE message. Most likely cause: network is down.
APP_MSG Error #26*nn*	Error while trying to send a message to the network. Most likely cause: network is down.
APP_MSG Error #29*nn*	Could not broadcast UNCHOKE message. Most likely cause: network is down or choked.
APP_MSG Error #30*nn*	Could not broadcast a timed UNCHOKE message. Most likely cause: network is down or choked. An attempt will be made to broadcast the messages at some later time.
APP_MSG Error #36*nn* APP_MSG Error #39*nn*	Could not broadcast NODE STATUS message. Most likely cause: network is down or choked.
APP Error # 1 *nn aaaaaa*	Unknown message type received from the network and put on the general applications queue. Most likely cause: version mismatch between paired IRMs.
APP Error # 2 *nn nn aaaaaa*	Unable to close packet that was removed from the general applications queue. Most likely cause: programming error.
APP Error # 3 *nn nn*	Could not read message from general applications queue Most likely cause: version mismatch between paired IRMs.
APP Error # 4 *nn nn*	Invalid message handle found on general applications queue. Most likely cause: programming error - previous memory management operation was not handled properly, resulting in a cascaded error here.
APP Error # 5 *nn nn nn*	Mismatched application numbers. The application expected to receive the current message is not the same as the actual application. Most likely cause: programming error.
Missing*nn* packets	The IRM packet utilization count does not match the actual count of packets in use. Most likely cause: programming error - previous memory management operation was not handled properly, resulting in a lost (or double-linked) packet.

4.3 Diagnostic Monitor

Non-Fatal Error Messages Sent to the Diagnostic Port - (Continued)

Message	Description
APP_QUE Error 1 *nn*	An indecipherable message was received on an inbound (from the network) queue. Most likely cause: version mismatch between paired IRMs.
Decryption Failure ...resynchronizing	The encryption engines used by two linked *IRM*s have gotten out of sync, resulting in an encrypted message than can no longer be decrypted. The message will be passed on to the higher layers in the hopes that some action can be taken to retransmit the message. Most likely cause: erratic network behavior causing one *IRM* (but not the other) to undergo a state change.
Output Queue Port*nn*, (stalled port?)...resetting	Could not append a message to the network broadcast queue. Most likely cause: network is down or choked.
NET MSG # 1 *nn*	Handle attached to message being sent to network is invalid. Most likely cause: programming error.
Network Manager has disabled this node	The Network Manager program has shut down transmissions by this node. This capability will be available to network managers to prevent illegal use of the network by non-subscribing customers.
Aloha lock...	The *IRM* has lost contact with the network and is now in "aloha" mode, waiting for a network startup command.
Aloha unlock!	The *IRM* has timed out waiting for a network startup command and has successfully initiated the network itself.
In Circuit INIT	The *IRM* has transitioned from an "aloha" mode to CEMA mode, hearing and responding to network commands. This is not an error but rather an indication that normal network operations have resumed.
RING= *nn*	The X.25 task scheduler has reached its queue limit, and subsequent requests for X.25 processing will not be honored until the queue size has decreased. Most likely cause: X.25 is being saturated by many small frames from two or more ports. A temporary solution would be to decrease the number of ports running X.25, and/or to reduce the port baud rate.

4.3 Diagnostic Monitor

Non-Fatal Error Messages Sent to the Diagnostic Port - (Continued)

Message	Description
nwl received reconnect for circuit that is down	A "reconnect" request was received by a *IRM* that had been previously disconnected. This is not logical (CEMA requires that an "initiate" or "aloha" request precede the "re-connect"). Most likely cause: programming error.
nwl forcing disconnect	The CEMA network layer is out of sync with its partner, and can recover. It will force a disconnect, followed by a reconnect, to get both *IRM*s back into sync. Most likely cause: programming error.
ACP:RX error on channel *nn* - Error in parity	The Asynchronous Comm Port module got a parity error while trying to receive asynchronous data from a port. Most likely cause: noise on a data line or a broken connection.
ACP:RX error on channel *nn* - Framing error	The Asynchronous Comm Port module got a byte framing error while trying to receive asynchronous data from a port. Most likely cause: noise on a data line or an incorrect port baud rate.
ACP:RX error on channel *nn* - Receiver overrun	The *IRM* could not keep up with an asynchronous input data stream. Most likely cause: the port's baud rate is too high to be supported along with all other *IRM* operations going on.
ACP:RX error on channel *nn* - UNKNOWN status interrupt	The Asynchronous Comm Port module got some kind of unknown error while reading asynchronous data.
ACP: break received from channel *nn*	An unexpected break signal was received by the Asynchronous COM Port module.
(!AVAILBUF !SOME)	CEMA requested a data buffer when none were available. Most likely cause: a programming error prior to the request for memory has locked up (or used up) available memory.
(AVAILBUF < SOME)	CEMA requested more data buffers than were available, and the request could not be honored. Most likely cause: the *IRM* cannot keep up with the network activity. If this happens, it is most likely to happen to a host *IRM* that is supporting several remote *IRM*s.

4.3 Diagnostic Monitor

Non-Fatal Error Messages Sent to the Diagnostic Port - (Continued)

Message	Description
_MTM_Start_Multi_Timer - Timer Value is *nn* in aaa (*nn*)	A timer was requested with an invalid time period. Most likely cause: programming error.
!*nnn*/[filename]:line	A diagnostic message preceded by an exclamation point always takes the form on the left, where nnn is the elapsed time (in sixteenths of a second) since the *IRM* was last reset; [filename] is the name of the submodule in which the error occurred; This diagnostic message type is used throughout the software, typically where critical tasks are running (examples would include I/O subsystem errors, like FCS or receiver overrun). The *IRM* will usually (but not always) fully recover from these types of errors. If an error like this persists, you should copy it down and notify Aria Wireless Systems. Line is the line number in the source code where the error occurred.

4.3 Diagnostic Monitor

Network Manager Error Messages

Where appropriate, some error messages are sent over the CEMA network to Network Manager, where they can be displayed (and logged) for subsequent analysis. These messages appear as text after the Network Manager descriptor for "Network Debug Message". See the Network Manager Manual for details.

5 - LAP-B Protocol Application

Protocol Emulation

The IRM LAP-B protocol emulation implements the 1984 CCITT (Blue Book) Link Access Procedure - Balanced (LAPB) standard. This gives the IRM the same point-to-point capability as an HDLC link, but with the addition of protocol emulation to minimize network traffic. The level 3 traffic is transparent to LAPB and is sent across the network as data or information frames (I-Frames). The IRM will perform both polling emulation and data acknowledgments locally, sending only I-Frames and control information across the network.

Supported LAP-B Frame Types

SABM/SABME	Set Asynchronous Balanced Mode/Set Asynchronous Balanced Mode Extended
RR/RNR/REJ	Receive Ready/Receive Not Ready/Reject
DISC	Disconnect
UA	Unnumbered Acknowledge
DM	Disconnect Mode
FRMR	Frame Reject
IFrame	Information Frame

The CCITT standard allows modifications to the values of several LAP-B parameters, in order to provide flexibility to developers of equipment. The following table lists these parameters, whether or not the IRM supports modifications to them, and the maximum and minimum values to which they can be set.

Standard LAP-B Parameters

LAP-B Parameter	Configurable?	Min Value	Max Value
Baud Rate	Yes	50	192000
Extended Control	Yes	normal (mod 8)	extended (mode 127)
T1 (Response Timeout)	Yes	0 msec	9,999,999 msec
T2 (Acknowledgment Delay)	Yes	0 msec	9,999,999 msec
T3 (Channel Timeout)	No	(IRM supplies its own timeout)	
N1 (Maximum Frame Length)	Yes	1	4096
N2 (Retransmission Tries)	Yes	1	99
k (Max acknowledged Frames	Yes	1	50/# LAP-B Ports
Multilink Operation	No	(Not Supported)	

5 - LAP-B Protocol Application

> NOTE
> LAP-B does not guarantee acceptable performance if the DCE and DTE aren't exactly matched.

LAP-B Physical Layer

An LAP-B terminal is usually wired to be Data Terminal Equipment (DTE), while the LAP-B network interface is usually wired to be Data Circuit-terminating Equipment (DCE). Electrically, an IRM is always DCE. This means that even if the IRM port is configured as a DCE Server (emulating a LAP-B DTE and connected directly to the LAP-B DCE), it is still a DCE at the RS-232 connection. If the customer equipment cannot be configured as a DCE (logically) and a DTE (physically), then a custom cable will be needed that swaps the data and clocking lines between the IRM and the LAP-B DCE.

Refer to the IRM Reference Manual, Sec 2.3, for connecting DCE to IRMs.

IRM LAP-B Capacities

The IRM has been tested running LAP-B on one, two, three and four ports simultaneously. At 9600 baud, four ports can be supported at moderate data rates. At 19200 baud, at least two ports (and possibly three) can be supported at moderate data rates. Bear in mind that the combined average port data rate cannot exceed the average radio network data rate for more than a brief period of time. The IRM will attempt to buffer data for those periods when input is occurring on two or more ports simultaneously; however, IRM memory is limited and data buffering can be sustained only for about 16 Kbytes of data. The IRM will attempt to flow control the user equipment (replying RNR to a poll or data) when data buffering nears its limit.

Memory limitations also force the IRM to limit the maximum number of unacknowledged IFrames that can be buffered. This limit is 50 per IRM, regardless of the number of LAP-B ports that have been configured. If the number of unacknowledged frames grows too large, the IRM will attempt to flow control the user equipment by sending RNRs. If the unacknowledged pool is filled, the IRM will send REJ frames to the user equipment until pool space is freed up. This limitation can be avoided by keeping the (configurable) LAP-B parameter *k* (Max Unacknowledged Frames) small. The default is 7.

The largest LAP-B IFrame that the IRM will support is 4096 bytes. The IRM can buffer up to 16K bytes of data; flow control will be applied when roughly 60% of the available buffering is utilized.

5 - LAP-B Protocol Application

Configuration

The user selectable parameters for LAP-B Protocol are grouped into three categories:

1. Active Session Parameters
2. Inactive Session Parameters
3. Physical Parameters

The distinction between "active" and "inactive" settings is related to parameters that affect operation while the session is established (i.e., after a SABM/UA has occurred) and parameters that affect operation while no session is established (i.e., after a DISC or DM has occurred). *There is no processing of X.25 Packet Layer (Layer 3) items, so there are no Packet Layer parameters.* The LAP-B only operate to level 2 (LAPB), so these are the only configurable parameters you need to set. Level 3 is completely transparent to the IRM.

Active Session Parameters

Frame Window Size

The maximum number of outstanding data frames (*"IFrames"*) allowed before an acknowledgment is required. The range is 1 to 7 (7 is the default value). Under most circumstances this parameter should not be modified. If it is set to a value less than what the user's equipment expects, the LAPB software will send frame rejects (FRMR) whenever it receives more unacknowledged packets than allowed. This will result in loss of session.

Min Receive Window Size

If the number of unacknowledged data frames is less than this parameter, then LAPB will automatically send a reply (RR) to the port without waiting for T2 (or a return Iframe) to expire. The range is 1 to *Frame Window Size* (the default is 2). The result of setting this parameter smaller than the *Frame Window Size* is that it speeds up data frame acknowledgments, leading to more efficient use of the port. Under most circumstances this parameter should not be modified.

Active Polling

This item controls the IRM's ability to poll the user equipment with RRs. Having the IRM actively poll will allow it to know if the user equipment goes down. If this is set to False, then the IRM will not do any polling, and only IFrames will be transmitted between the router and the IRM. In cases where the user equipment does not respond to polls, set Active Polling to False, because after N2 timeouts (see below) the IRM will disconnect the session because of a lack of activity on the router's part.

Server Type

The "Primary" side of the connection is usually associated with an X.25 router or switch, and is regarded as the LAP-B "network" side of the connection. The "Secondary" side of the connection is usually associated with an LAP-B terminal, but the terminal could also be another LAP-B router or switch. It is regarded as the LAP-B "terminal" side of the network.
What makes this confusing is that LAP-B is really a peer-to-peer link, and the names given to the devices can become arbitrary. In general, however, the following rules must apply when using IRMs as the access medium:

One LAP-B device **must** be configurable as a logical DCE, and the other **must** be configurable as a logical DTE.

The LAP-B emulation (the IRM) connected to the logical DCE must be configured as the Primary Server while the emulation connected to the logical DTE must be configured as the Secondary Server.

5 - LAP-B Protocol Application

NOTE
It makes no difference which Node Type (Host or Terminal) is associated with a Primary or Secondary Server.

Maximum Frame Length

Normally, the LAP-B session layer arbitrates the maximum size of the data packets that can be sent from unit to unit. The IRM emulation has an upper limit of 4096 bytes (the default) but can be set lower to provide an additional source of error checking. Under most circumstances this parameter does not need to be modified.

T1 Timer

The T1 Timer (also called the Response Timeout or Retry Timeout) is the amount of time (in msec) that the LAP-B logic will wait for a response before retransmitting a frame. This parameter should be set identically to the value used by the customer's equipment.

T2 Timer

The amount of time that LAP-B will withhold emulated acknowledgments in the hopes of receiving a reply from the other end of the connection. Judicious use of this parameter allows more efficient use of the port, since fewer port transmissions will occur if a real reply (i.e., a data frame) is received prior to an emulated acknowledgment. However, because CEMA network delays tend to be the overriding factor in data throughput, trying to make the port connection more efficient has little real impact on performance.
This parameter is normally configured to be no more than 2/3 T1. Its default value is 200 msec. It is not allowed to be greater than T1; setting this value larger than T1 will cause the user equipment to retransmit frames whenever T1 expires and an acknowledgment has not been received.

Num N2 Timeouts

Sometimes called *N2* or *Retry Count*, this parameter determines the maximum number of times a frame will be transmitted before the LAP-B logic changes state. If N2 timeouts occur while attempting to transmit a data frame, LAP-B will force a disconnect sequence to occur. If N2 timeouts occur when already disconnected or trying to reconnect, a *Disconnect Mode* (DM) frame will be transmitted. This parameter should be set identically to the value used by the user equipment.

Inactive Session Parameters

These parameters are necessary to determine behavior while in a disconnected state. Some user equipment connections demand a very specific disconnect/connect sequence; if the disconnect/connect handshaking does not occur in exactly the correct order, one or both user units will fail to connect.

Should Auto Start [Connection]

This parameter, when set Yes, allows the LAP-B software to initiate a connect sequence whenever a session disconnect has occurred. It has the advantage of not relying solely on the user equipment to establish the session. The default for this value is Yes. If after a session disconnect the customer equipment has trouble reconnecting, then it may be advisable to set this parameter to No in order to minimize any interference from the LAP-B emulation.

5 - LAP-B Protocol Application

Here is an example of when it is a problem to have the Auto Start function enabled:

Host Router	Host Server	Term Server	Term Router
DISC->	(Send DISC to CEMA)->		
	<-UA	DISC->	
	<-SABM		
UA-->			<--UA
	<-Send SABM to CEMA	,-(send DISC to CEMA)	
	<--DISC	UA-->	
UA-->			
DISC-->	(send DISC to CEMA) -->		
(and everything	repeates like this	forever !!)	

If this condition occurs, disable Auto Start.

Use Explicit UA

If a unit has sent a disconnect notification to the LAP-B emulation and LAP-B has acknowledged the disconnect, LAP-B will normally wait for a disconnect notification to come from the remote side of the connection before changing state. (Receipt of the remote disconnect indicates that both sides of the connection are in a disconnected state.) If this parameter is set to FALSE and the user equipment tries to start the connection prior to LAP-B's receipt of a remote disconnect, LAP-B will not acknowledge the connect and will instead send a connect of its own, expecting the user equipment to acknowledge. This behavior is consistent with the X.212 protocol standard.

However, some user equipment will not tolerate the lack of a reply to its connect request. If *Use Explicit UA* is set to TRUE, LAP-B will always acknowledge the user equipment's SABM. This will satisfy the user equipment but has the possible effect of getting the two sides of the connection out of sync with each other.

The default value for this parameter is FALSE, although careful analysis of the user equipment connection is required to determine if this value should be set to TRUE.

Setting this to True will force the IRM to respond UA to any SABM and to follow it with its own SABM, causing both sides to SABM/UA each other. If this is set to False, then when the IRM gets the router's SABM it will ignore sending a UA and instead send its own SABM, expecting a UA from the router. It looks like this:

"Use Explicit UA" set to FALSE

Active Disconnect

If set to TRUE (this is the default), then the LAP-B logic will initialize a connection by sending a disconnect request (DISC) prior to sending a connect request (SABM). If *Should Start Connection* is FALSE, then this parameter has no impact on LAP-B processing.

No Initial RR

If this parameter is set to TRUE (the default) then a SABM/UA is all that is needed for the LAP-B emulation to be considered active. If FALSE, then at least one poll or data acknowledgment must be received before the link is declared active.

From a connection point of view, it is safer to set this parameter to FALSE. However, some user

equipment may expect to be able to send data immediately after the SABM/UA handshake. If *No Initial RR* is FALSE, at least one poll will have to occur first before LAP-B accepts any data from the user equipment. This could lead to communications failure since the data will be ignored. For this reason, *No Initial RR* should normally be set to TRUE.

Disconnected Phase Timer

This parameter is used to prevent LAP-B from leaving the disconnected state until after the timer expires. It is meant to provide some time for user equipment to recover and reinitialize itself after a disconnect.
This parameter is normally disabled, which indicates to LAP-B that it should wait for the terminal to reconnect. A value of 0 msec indicates that LAP-B should try to reconnect immediately. The maximum legal value is 65.534 sec.

Physical Parameters

In addition to the standard RS-232 physical parameters (baud rate, CD and RTS control, etc.), there are a few important items that must be set.

Enable Clk Btwn Frames

Some user equipment may require that the idle period **between** frames be flag-filled (and not mark-filled). To do this, make sure this item is set to TRUE and the configuration item "IDLE Condition" is set to FLAGS.

Enable Active Idle [future]

Setting this parameter to TRUE will force the transmission of idle characters during the period between frame transmissions. Some user equipment requires this. The default value is TRUE. If set to FALSE, the I/O chip will transmit nothing (the "marking" state) during the period between frame transmissions.

Idle Character [future]

This parameter can set so that either flags (01111110) or marks (11111111) are transmitted during the idle period between frames. It is not relevant if the *Enable Active Idle* parameter is set to FALSE.
This parameter is dependent on the expectations of the customer equipment. Idle Flags is the default.

Example: Configuring LAP-B on Routers

Like other protocols, LAP-B requires a primary/secondary or host/terminal connection. Even though you're going to be hooking up two routers, one will effectively be set up as a logical DTE and the other will be a logical DCE. If the two routers were hooked directly together, they'd look like this at the physical and datalink levels:

(Unlike SDLC or 3270, LAP-B is actually a full-duplex peer-to-peer protocol. It therefore uses two logical addresses - 01 and 03 - to differentiate from commands/responses coming from both directions.)
When using IRMs for this link, use the following configuration:

A tail circuit cable may be needed on the host router if it is a physical DCE. Refer to section 2.3 of the IRM Reference Manual for details on how to interconnect two physical DCEs.

5 - LAP-B Protocol Application

Config Parameters - Physical Layer Settings

Carrier Detect:	Always On
Clear To Send:	Always On
CD Anded with Radio:	False
CTS Anded with Radio:	False
Data Encoding and Clock Source:	depends on user equipment settings
Frame Check:	CCITT_1
Enable Clk Btwn Frames:	True
Enable Active Idle:	True (default)
Idle Char:	Flags (default)

Config Parameters - Protocol Active Settings

Frame Window Size:	7
Min Rx Window:	2
Active Polling:	True
Server Type:	Primary for the host IRM, Secondary Remote IRM.
T1 Timer:	3.000 seconds
T2 Timer:	0.5 seconds
N2 Timeouts:	same as router's value
Max Frame Length:	512 or 1024

Config Parameters - Protocol Inactive Settings

Should Auto Start:	No
Use Explicit UA:	False

If you have trouble getting a session to reconnect after it has disconnected, this is probably the first parameter to change. "Use Explicit UA" set to True is not precisely compliant with the LAP-B spec, so it is recommended to leave it False unless you have session problems.

Active Disconnect:	True
No Initial RR:	True
Disconnected Phase Timer:	Disabled [65535]

Port LED Display

The port LED can be in one of four states:

LED State	Meaning
Off	This port has no radio link established. Protocol emulation is running, but no messages will be exchanged across the network.

5 - LAP-B Protocol Application

Network Messages

There are several network messages sent between IRMs to maintain the LAP-B session. These appear on the Network Manager's Realtime Display as User Control Packet or as Data Packet. Only the information contained in the IFrame is sent as a Data Packet, the rest are User Control Packets.

6 ISO Poll/SelectApplication

Protocol Features

The ISO Poll/Select application provides protocol emulation for several manufacturer's equipment that fallS under the general class of poll/select communications. The software conforms with the International Standards Organization (ISO) specification 1745 and the American National Standards Institute (ANSI) X3.28 procedures.

Within this general class, there are several specific protocol selections:

- IBM BiSync (3270): conforms with IBM spec GA27-3004, Binary Synchronous Communications
- Burroughs Poll/Select, Async: conforms with the Diebold spec 79-811-5. Diebold 9000 Series Terminal Poll/Select Protocol Manual
- Burroughs Poll/Select, Sync:
- Lottery 3201:

Each one operates according to its own specific manufacturer's rules, but the general operation and configurations are similar.

In this release, only the Burroughs Poll/Select Async is supported.

Burroughs Poll/Select Supported Feature

This protocol conforms with ANSI X3.28 Establishment and Termination Procedure Subcategory 2.5 and Message Transfer Subcategories A4 and B1. The following features are implemented:

- Standard Poll/Select
- Fast Select
- Group Select
- Broadcast Select
- ASCII character set
- Up to 32 terminals per multidropped line (Host Server port); up to 32 multidrop Terminal Servers per Host Server port.
- Full RS-232 control handshaking.
- Baud rates 300 to 19,200, each port.
- Up to 4 active ports per CPU.

Compatible Terminal Equipment:

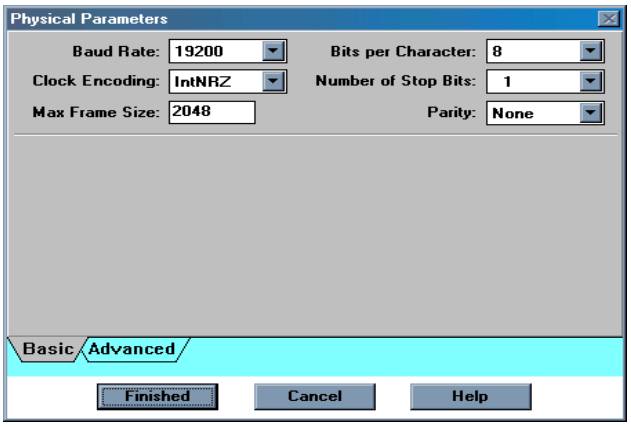
This protocol operates with the following equipment:

* Diebold serves 910 Automatic Teller Machines and Simulators.
* Computer Peripheral Systems Including Poll/Select, Host and Terminal Emulators.

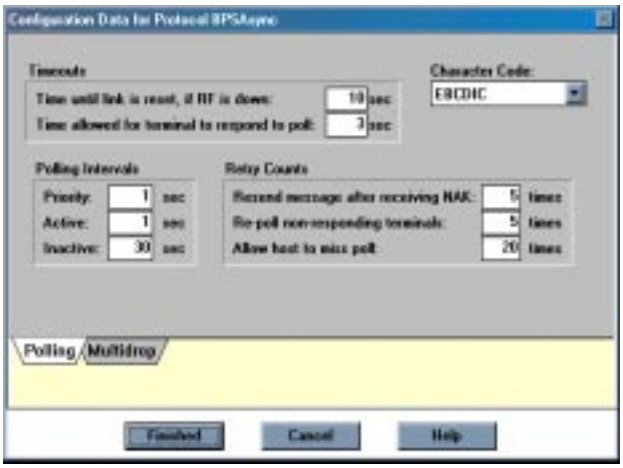
6 - ISO Pol/Select Application

How to Configure:
Use the Net manager, select the Port Tab.

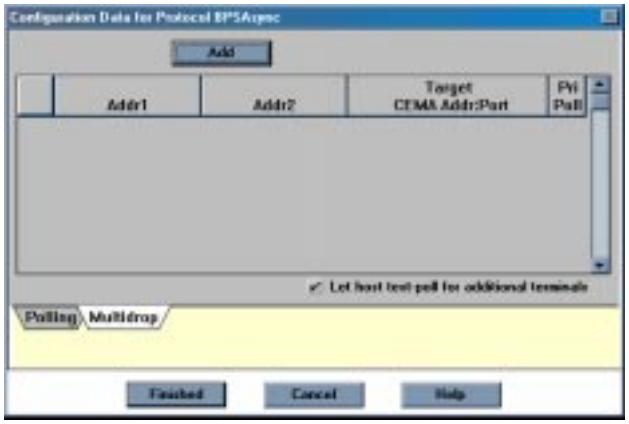
Select BPS AsyncPhysical Parameters, Depress Physical Button. This screen appears:



Set the port physical parameters as desired. The usual settings for Burroughs Poll/Select terminals are 7 bits per character and Even Parity. Usually the remaining parameters can be left as default. Click on OK, and then select the BPS Async Protocol button. This screen appears:



Again, these parameters can usually be left at their default values, but can be changed if needed. The table on pages 4-5 gives a precise definition of each.
The last step is Configuring the **Multidrop Terminal**. This **MUST** be done in the Host Server for all terminals that will be polled. Click on **Multidrop Terminals** and this screen will appear:



6 - ISO Poll/Select Application

Config Parameters Values

Parameter	Required?	Range	Default
Multidrop Terminals	Yes, on HS, optional on TS	ID: 2 character ASCII or 4 character Hex Target: any remote port Priority: yes or no	none none no
Polling Interval	No	0.1 to 100 secs	1 second
Priority Polling Interval	No	0.1 to 100 secs	1 second
No Response Timeout	No	0 .1 to 100 secs	3 seconds
Number of Polls to Inactive	No	1 to 255	5
Number of Retries to Nak Messages	No	1 to 255	5
Periodic Update Time	No	1 minute to 24 hours	10 minutes
Suspended Session Timeout	No	0.1 to 1000 seconds	10 seconds
Max Frame Size	No	1 to 8192 bytes	2048 bytes
Debug Enable	No	Yes or no	yes

6 - ISO Poll/Select Application

Config Parameter	Definition
Node Type	Selects whether this port is a Host Server or Terminal Server selected in the Utilities Menu. A Host Server behaves as a secondary device responding to poll and select commands. A Terminal Server behaves as a primary device initiating poll and select commands.
Multidrop Terminals	Selects which terminals will be emulated. Three fields: 1. Terminal ID - the terminal address, entered in ASCII of Hex 2. Terminal Server - select which terminal server will poll this device 3. Priority Polling - yes or no Must be configured at the Host Server side, optionally, can be configed at the Terminal Server side.
Active Polling Interval	The minimum time interval between polls to a terminal that is active, but not priority. The actual precise polling interval may become longer than this, if the processing load is high. Used in the Terminal Server side only.
Inactive Polling Interval	Same as in polling interval, but is the interval at which terminals marked as priority will be polled. Usually this interval is less than the standard interval, but it does not have to be.
No Response Timeout	Time a Terminal Server will wait for a response to a poll (in seconds).
Number of Polls to Inactive	The number of polls an active terminal (standard or high priority) does not respond to, in a row, before it is marked inactive. Used in the Terminal Server only.
Number of Retries to Nak Messages	The number of times the IRM will retry sending a message that has been Nak'd, before it will give up and discard the message. Used in both the Terminal Server and Host Server.
Periodic Update Time	Specifies the interval between the periodic update message that keeps the terminal tables in each unit in sync. Typical times are 5 to 15 minutes. Used in both Host Server and Terminal Server.
Suspended Session Timeout	Used in both HS and TS. The amount of time a protocol session will remain suspended waiting for the RF link to come back up. When this times out, all message queues are cleared and the polling mechanism is reset. Typical times are 10 -30 seconds.

6 - ISO Poll/SelectApplication

Config Parameter	Definition
Max Frame Size	The maximum size, in bytes of a legal data link frame, starting from the Start of Header (SOH) character up to (and including) the Block Check Sequence (BCC) character. Messages longer than this will be rejected. This limit prevents transmissions with missed End Of Text (ETX) characters from waiting forever for the end of a message.
Debug Enable	Used to enable the diagnostic text output to the designated diagnostic port. Useful when debugging a protocol interfacing problem.

Operation

Theory of Operation

The emulation process is based on an internal terminal (or device) table that is set with all the protocol parameters at configuration time. The table contains an entry for each terminal to be emulated.

> NOTE
> Polling emulation is performed only for terminals that are specified in the configuration. If commands or messages are for terminal addresses not listed in the configuration, they will be ignored.

At startup, after each node has established a CEMA network connection, the Host and Terminal Servers exchange Session Start messages. These make sure that the terminal tables in each node agree. The Host Server will update the Terminal Server with its portion of the master table if the two do not agree.

Polling emulation begins at the Host Server. The Host Server remains in an Idle state until it receives a poll or select command. If a poll/select command is received for one of the pre-configured terminals, the Host Server sends out a Device Status network message (or a complete Terminal Table network message containing the status for all devices), telling the Terminal Server to start polling.

The Terminal Server polls at the rate specified in the configuration, either the standard or priority interval, until a response is received. When a terminal responds, the Terminal Server sends back a Device Status network message to the Host Server, which causes the Host Server to begin responding to polls or selects.

When selected, the Host Server will send the message over the radio network to the Terminal Server connected to the specified device address. At the next opportunity, Terminal Server will then select the device and send it the message.

The Terminal Server constantly polls the terminals in its table at the operator-specified rate. When a terminal responds with a message, it is sent over the radio network to the Host Server where it is held until the next poll.

Both the Terminal and Host Servers contain sufficient memory to buffer many messages. The available buffer space depends on many factors, such as number of multidrop terminals and what is other applications are running. The remaining buffer space can be determine in the periodic diagnostic message (see section 4.3).

6 - ISO Poll/SelectApplication

Port LED Display

The port LED can be in one of four states:

LED State	Meaning
OFF:	This port has no radio link established. Protocol emulation will still run but messages will not go back and forth across the radio network.
SLOW Blink:	Radio link established for this port, but no port activity. •Host Server: not receiving polling for any configured terminals. •Terminal Server: not sending any polls, no terminals activated.
FAST Blink:	Radio link OK, with one-way port activity. •Host Server: receiving polls but not responding since it has not received an active terminal status message from the remote end . •Terminal Server: sending polls but not receiving any responses yet.
ON:	Radio link OK and two-way port activity. IRM has polling and responses for at least one terminal.

6 - ISO Poll/SelectApplication

Network Messages

There are several network messages that this protocol sends to maintain the emulation and exchange data and status. These will appear on the Network Manager's Realtime Activity display. Use this display when debugging terminal polling activity or message exchange problems.

Message Name	Description
Data	One or more messages sent for every data frame transferred at the port. Only the number of bytes sent over the radio network is displayed. This may be less than the actual number of bytes at the port because of compression.
Device Table	Only sent by Host Servers to Terminal Servers. First lists the number of devices (or terminals) specified for this Terminal Server and then for each device, lists the following information: • Device Address (in hex) • Device Existence: always Static • Device Status: Null (error), Active, Inactive, Wacked, Not Started, Tentative (not used), Starting, Excluded • Target Number: internal number specifying the index into the multidropped array • Polling Interval: (in seconds) • Number of Missed Polls: number of missed responses to a poll.
Device Update	Similar to device table, but only for one device.
Session Start	Contains the CEMA node address and port number of the sending station along with terminal table information: the number of terminals in the table and a checksum of pertinent data in the table. The receiving station can use this to verify that its terminal table agrees with the remote end. The Terminal Server always sends a Session Start message in response to a Session Start. The Host Server will respond only if the checksum does not match, in which case, it responds with a Device Table message.

6 - ISO Poll/SelectApplication

Diagnostics

Note that many software segments (CEMA network control or other applications) use the diagnostic port to report their progress. As such, diagnostic reports from different segments will be intermingled. Refer to the Diagnostic section of each individual application you have in your IRM if the diagnostic message cannot be found here.

Startup Diagnostics

Message Name	Description
Baud Rate	Identifies the port baud rate selected
Port x is P/S Host Server: # Terms: nn Addr: aaaa Target: llp	Identifies this port was configed as a Poll/Select Host Server, with nn terminals entered. Each configured terminal is listed with its address aaaa in hex and its target (the Terminal Server which will poll it) listed as CEMA link ll, port p.
Port x is P/S Terminal Server	Identifies that the application was configed as a Terminal Server.
SS Msg to Tar#	A Start Session message has been sent to target # [0 thru n]
Send_Session_Msg failed nn Put_Message failure.	Poll/Select application attempted to send one of the session coordination messages, and it failed. The numeric code is a memory manager return value that corresponds to the Put_Message failure. This message usually occurs when the radio link is down during a session establishment.
Rcvd SS Msg [delaying...]	Received a Start Session message. If delaying... appears, it means that the radio link is not fully up in both directions, so the responding Start Session message will not be sent immediately.
Connect_Change, port p, state s	A Change Connection Status event has just occurred for port p, indicating that the radio link has just gone up or down. State s is an internal state variable for the session control layer.

6 - ISO Poll/Select Application

Runtime Diagnostics

Message Name	Description
Nt Cntrl to Tar # x:	Indicates the Poll/Select software has sent a terminal table or device status type message (polling network control message). These messages occur at startup or whenever the polling state (active or inactive) changes. x indicates to which multidrop target node number (starting from 0) the message was sent. If the node is a Terminal Server, x is always zero.
Rcvd Nt Cntrl [bad]	Indicates the Poll/Select software has just received a terminal table or device status type message (polling network control message). These messages are expected at startup or whenever the polling state (active or inactive) changes. The word bad should never appear. It means the receiving unit could not decode the control message. Probable cause is incompatible versions between host and terminal server software.
Send_Net_Cntrl failed nn	Poll/Select application attempted to send one of the polling network control coordination messages and it failed. The numeric code is a memory manager return value that corresponds to the Put_Message failure. This message usually occurs when the radio link is down during a session establishment
RcvdPoll: aaaa	RcvdPoll: aaaa A poll for address aaaa (hex) was received in the port.
RcvdSel: aaaa	RcvdSel: aaaa A standard select for address aaaa (hex) was received in the port.
RcvdSpecSel: aaaa	A fast, broadcast or grouped select for address aaaa (hex) was received in the port.
Sending Msg	A message is being sent out the port, either in response to a poll (Host Server) or select (Terminal Server).
Sending EOT	Sending an EOT in response to a poll (no message ready).
ACKing Sel	Attempting to send an ACK out the port in response to a select
NAKing Sel	Attempting to send an NAK out the port in response to a select because the device is busy: the IRM's buffers are too full to accept anymore data.
RcvdEOT	Received an EOT in response to a poll (Terminal Server only).

6 - ISO Poll/Select Application

Message Name	Description
RcvdSOH	Received a message in response to a poll (Terminal Server only).
Poll Timed Out	No response to a poll was received within the timeout period.
Sending poll: aaaa	Sending poll to device aaaa (in hex).
Sending sel: aaaa	Sending select to device aaaa (in hex).
Sel timed out	No ACK was received for the select operation within the poll timeout period.
Rcvd Ack	ACK was received in response to a sent message.
Rcvd Nak	NAK was received in response to a sent message.
Rcvd Unk, NAKing	Unable to decipher the response to our sent message, sending a NAK in return.
SentMsg time out	No response was received to our sent message.
RcvdEOT after AckNak	Received the normal EOT response to our ACK or NAK transmission.
Bad Cksm	Block Check Character (BCC) of the received message did not match the calculated result, rejecting the message.
No ETX	Received message did not contain an ETX character at the end, rejecting the message.
Rcvd Msg hhhhhh	Received a message with header hhhhhh (in ASCII).
Sent Ack	Sent an ACK is response to a received message.
Sent Nak	Sent a NAK is response to a received message.
Rcvd Nonsense	Could not decipher response, or unexpected response for a given state.