Using the KAD/ETH/101

TEC/NOT/054

The KAD/ETH/101 is a full-duplex, fast Ethernet module. It can be used to program an Acra KAM-500 chassis or transmit data from an Acra KAM-500 chassis. This technical note describes how to set up the KAD/ETH/101 for programming and decommutating using a PC and is divided into the following sections:

29.1 Introducing the KAD/ETH/101

The KAD/ETH/101 is a full-duplex, 100BaseTX Ethernet Acra KAM-500 programmer and packet generator.

29.1.1 Programmer

The Acra KAM-500 chassis is programmed via proprietary protocol over UDP. The KAD/ETH/101 module has a factory-programmed, unique MAC (Media Access Control) address. The IP address for the module must be manually assigned (see "29.5.4 Assigning the KAD/ETH/101 IP address" on page 7 for details).

29.1.2 Packet generator

The KAD/ETH/101 generates data in IENA packets. The IENA format is a published standard and consists of an IENA application layer, consisting of a header and payload, transported over UDP as shown in the following figure. For more information on IENA data header fields, see "29.6.2.1 IENA data header" on page 11.

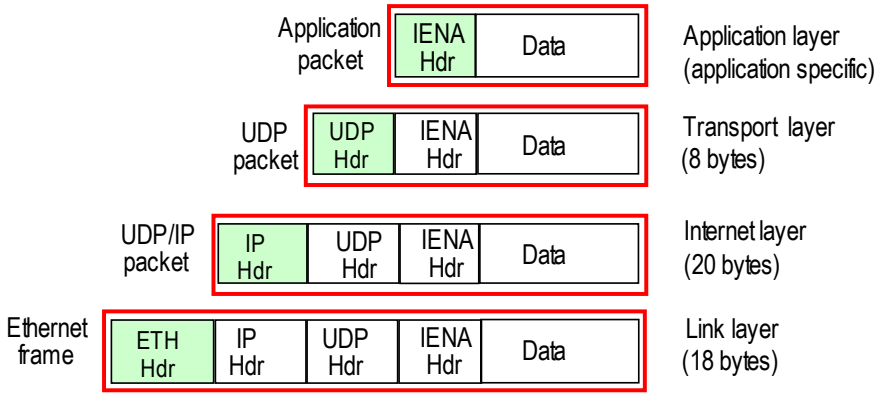


Figure 29-1: Packet encapsulation

The packet generator can transmit packets at varying rates as well as transmit packets of different sizes to different destinations, such as multicast and/or unicast and/or broadcast. When all parameter values in an IENA packet are present in the Current Value Table (CVT), the IENA packet is transmitted.

29.2 Wiring the KAD/ETH/101

You must wire the following elements on every KAD/ETH/101 module:

- The Ethernet interface (both Tx± and Rx± lines)
- The KAD/ETH/101 to KAD/BCU/101 programming interface (if Acra KAM-500 system programming via Ethernet is required)

NOTE: If the PC being used has auto-MDIX functionality, the KAD/ETH/101 may be connected to the PC through an ACC/ASY/023/C or ACC/ASY/024 cable, by using a straight-through or cross-over cable. Without this functionality, a cross-over cable or a straight-through cable with hub is required. Alternatively, the connection may be made as per the wiring guide (see the following table).

Table 29-1: KAD/ETH/101 to PC port RJ-45 wiring (cross-over)

KAD/ETH/101 pin	PC port RJ45 pin
1 (RX_A+)	1 (Tx+)
2 (RX_A-)	2 (Tx-)
18 (TX_A+)	3 (Rx+)
19 (TX_A-)	6 (Rx-)

29.2.1 KAD/ETH/101 to KAD/BCU/101

The KAD/ETH/101 transfers data to the KAD/BCU/101 via its programming lines. There are two programming busses designated, that is, bus A and bus B. Bus A is for all chassis whose chassis ID is 31 or less. Bus B is for all chassis whose chassis ID is 32 or greater.

The chassis ID is determined by pins 4-7, 37, and 38 on the KAD/BCU/101. When using a single chassis in stand-alone mode, these pins should be left open circuit, resulting in a chassis ID of 0. This is programmed via bus A.

For a single chassis, bus B can be ignored. The corresponding connections are outlined in the following table.

Table 29-2: Module connections

KAD/ETH/101		KAD/BCU/101	
Pin		**Pin**	
6	PROG_A+	25	PROG_DATA+
7	PROG_A-	26	PROG_DATA-

The programming bus should have 120Ω terminations at each end. The programming lines are internally terminated in the KAD/ETH/101. The 120Ω resistor on the KAD/BCU/101 (see the following figure) can be used to terminate the bus; this resistor is permanently connected to PROG_DATA+ internally. To connect to PROG_DATA-, connect pin 27 (PROG_DATA_TRM+) to pin 26 (PROG_DATA-).

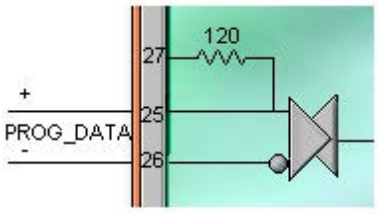


Figure 29-2: Termination resistor on the KAD/BCU/101

29.3 Connecting the Acra KAM-500 chassis to a PC

The Acra KAM-500 chassis may be connected directly to a PC using a cross-over cable, or may be connected to a hub using a straight-through cable. The goal is to create a network in which the programming PC is one node and the Acra KAM-500 chassis is another node.

29.4 Connecting the PC and the Acra KAM-500 chassis to a network

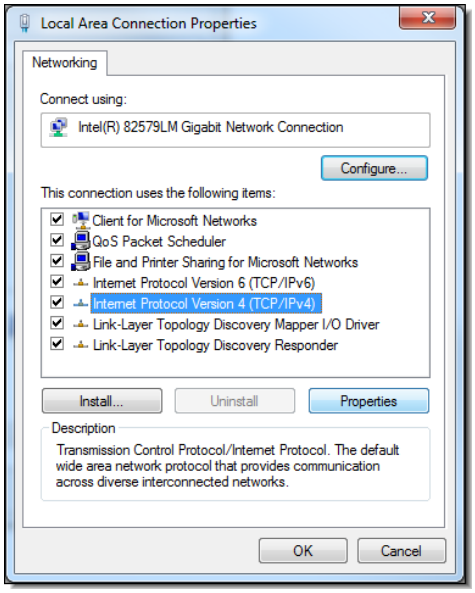
For a PC to recognize the Acra KAM-500 chassis, the PC must be on the same network as the chassis. Not only must they be physically connected, but they must share the same network address section of their IP address.

You can manually configure the IP address of the PC through Windows. For details on configuring the IP address for the KAD/ETH/101, see “29.5.4 Assigning the KAD/ETH/101 IP address” on page 7.

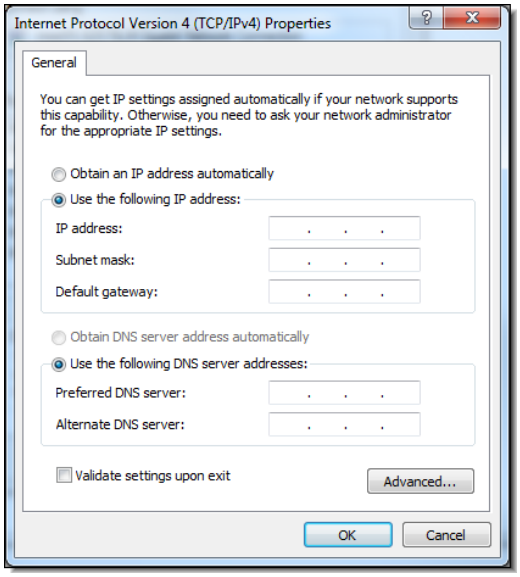
NOTE: The following procedure assumes your operating system is Windows 7.

To set up the network, do the following:

1. Click **Start**, **Control Panel**.
2. Click **Network and Sharing Center**.
3. Double-click the **Local Area Connection** that the Acra KAM-500 is connected to.
4. Click **Properties**.
   The Local Area Connection Properties window opens.



5. Select **Internet Protocol Version 4 (TCP/IPv4)** and then click **Properties**.
   The Internet Protocol **Version 4** (TCP/IPv4) Properties dialogue box displays.



6. Select the **Use the following IP address:** radio button.

7. In the **IP address:** field, insert the appropriate IP address.
   This IP address must have the same network address as the Acra KAM-500 chassis. Typically, the network address is determined by the first two or three bytes of the IP address. For example, if the chassis IP address was set to 192.168.0.3, then the network address for this might be 192.168.0. The node address—the one or two bytes that are not the network address—must be unique. So in this example we could set the PC address to 192.168.0.2.
8. In the **Subnet mask** field, insert details for the network address.
   If only the first two bytes are the network address, then the mask would be 255.255.0.0. If the first three are the network address then the mask would be 255.255.255.0.
9. Click **OK**.
   If required, re-boot the PC.

29.5 Using KSM-500 to configure the KAD/ETH/101

To operate the KAD/ETH/101, an IENA STANDARD packet must be created containing appropriate parameters and destination details. The module must be configured to communicate over a network by assigning it an IP address and establishing communication paths between it and the specified destinations of each packet.

When unicast packets are being used, it is important to correctly configure the target device MAC address when creating the IENA packet. This is because most switches use the MAC address rather than the IP address to determine how they route packets between ports. If an invalid target MAC address is used by the KAD/ETH/101, the switch may dump (delete) the packet or broadcast it to all ports.

When multicast packets are being used, KSM-500 software automatically assigns the corresponding destination MAC address for the IENA packets.

To configure the KAD/ETH/101, kSetup and kProgram software are required. kSetup and kProgram are included in the KSM-500 suite of tools.

29.5.1 Defining packets

You can add or remove IENA STANDARD packets on the Packets tab. You can also edit Packet Names, Packets per Acquisition Cycle, Destination IP Address, Destination Port and Mac Address fields for any packet.

Packet Name	Packet Type	Packets per Acquisition Cycle	Destination IP Address	Destination Port	MAC Address
TC_PACKET	IENA STANDARD	1	192.168.1.28	51000	00-1C-7E-2F-CA-B0
PT100_PACKET	IENA STANDARD	10	238.0.0.100	50001	01-00-5E-00-00-64
WING_PACKET	IENA STANDARD	16	238.0.0.101	50001	01-00-5E-00-00-65
ACCEL_PACKETS	IENA STANDARD	512	192.168.1.29	52001	AA-23-45-71-43-AF

Figure 29-3: IENA STANDARD packets

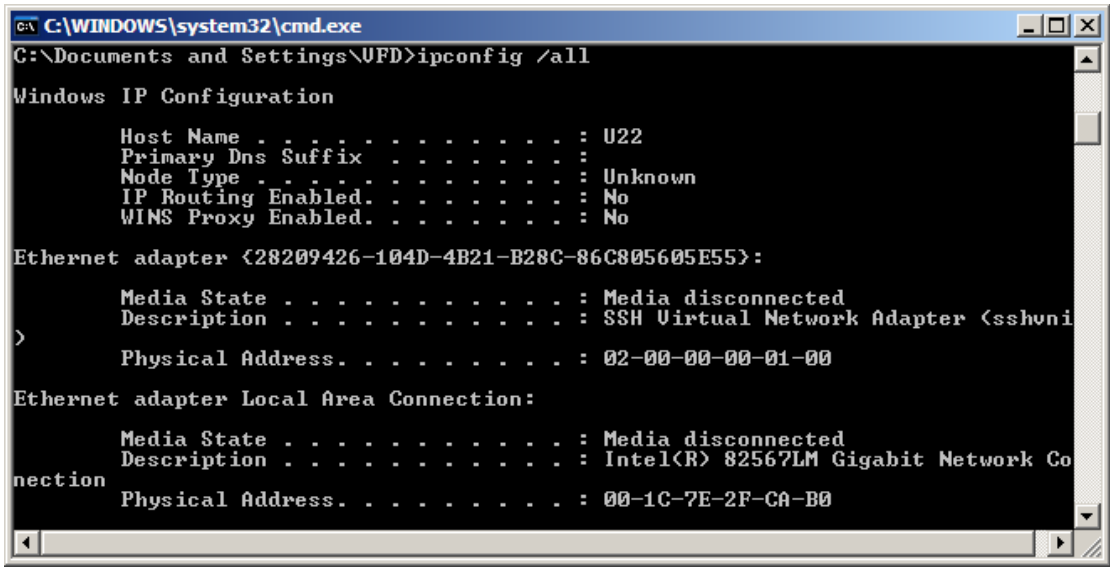
To add a packet, right-click on the spreadsheet, select Add Packet then select IENA STANDARD and complete the fields described in the following table.

Table 29-3: Adding/removing packets

Field name	Description
Packet Name	Name which identifies packet being transmitted.
Packet Type	IENA STANDARD is the only packet type supported; click IENA STANDARD to open the packet setup definition.
Packets per Acquisition Cycle	The number of packets per acquisition cycle; this number drives the sampling rate for the parameters transmitted into this packet (the sampling rate of a given parameter is calculated by multiplying the number of occurrences of that parameter within a packet, by the number of packets per acquisition cycle, by the frequency of the acquisition cycle).
Destination IP Address	The destination IP address can be unicast, broadcast, or multicast.
Destination Port	The destination port can be any value between 0 to 65535 except what is specified in RFC 1700 known as the well known ports (see “29.6.1 Appendix 1: Well known ports” on page 10); ensure your decommutation PC fire wall allows UDP packets to be received on this port.
MAC Address	The destination MAC address; when a multicast IP address is used, this field is automatically generated by the software and is read-only.

NOTE: Always create a packet with an instance of one for Packets per Acquisition Cycle. XidML doesn’t include the concept of acquisition cycle. For example, if you create a packet with 512 for packets per acquisition cycle, after closing kSetup, the number of acquisition cycles is multiplied to 512 and the packets per acquisition cycle changes to one.

NOTE: To know the MAC Address used by your PC, type IPConfig /all under a DOS CMD window. IPConfig refers to it as Physical address. In the example below, the MAC Address is 00-1C-7E-2F-CA-B0.



29.5.2 Configuring IENA packets

You can configure IENA packets on the Packets tab (see the following figure). For details of the IENA packet description, see “29.6.2 Appendix 2: IENA specification” on page 11“. To configure an IENA packet, double-click an IENA STANDARD cell in the Packet Type column on the Packets tab.

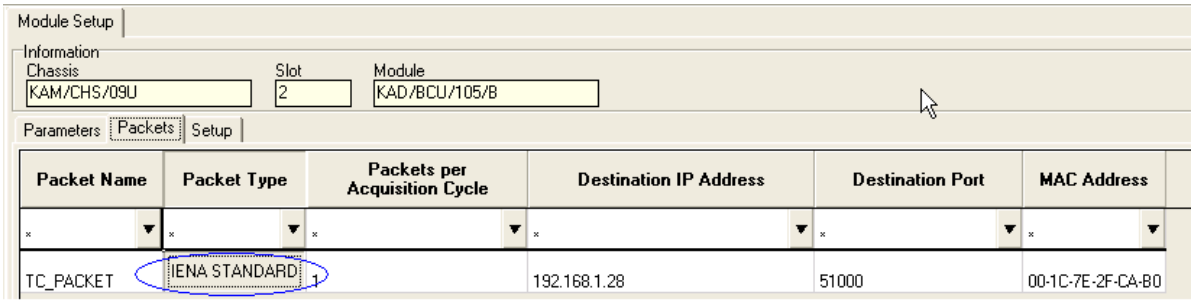


Figure 29-4: Configuring IENA packets

29.5.2.1 Editing IENA keys

To edit the IENA Key or IENA End key, double-click the Key cell or the End cell (see the following figure).

Figure 29-5: Editing IENA keys

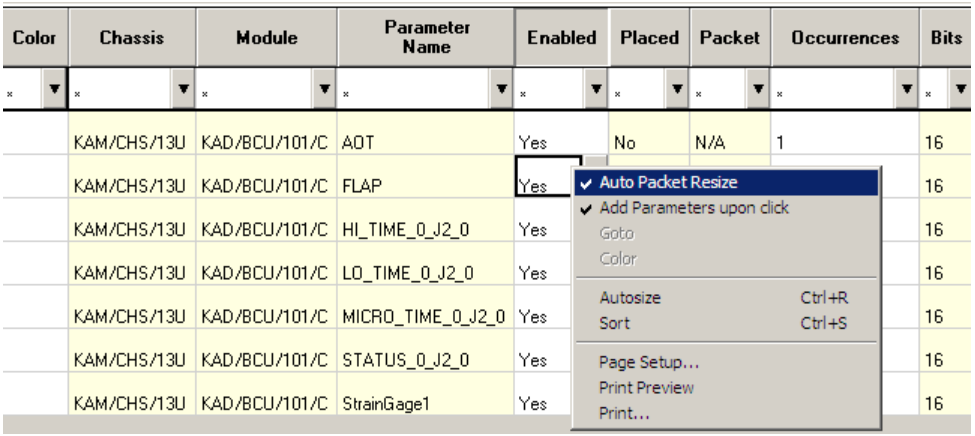
NOTE: To modify the IENA Key or the IENA End key, ensure Add Parameters upon click is not checked (see the previous figure).
The IENA key must be unique in a network distributed system.
The IENA End key has the same value for all the packets coming from the module.

29.5.2.2 Placing parameters in packets

You can manually place parameters in a packet if you want to specify the position of that parameter in the packet. For subsequent placements, each additional parameter is placed to the right of its predecessor.

To manually place a parameter, do the following:

1. On the Packet Setup tab, right-click and ensure Auto Packet resize and Add Parameters upon click are checked.



2. For the packet concerned, click on the spreadsheet to select a parameter.
3. Click on the byte to the right of the location you wish to place the parameter.
4. Complete the fields described in the following table.

Table 29-4: IENA packet settings

Field name	Description
Color	Not available.
Chassis	Chassis label from where the parameter comes from; read-only field.
Module	Module label from where the parameter comes from; read-only field.
Parameter Name	Name of the parameter; read-only field.
Enabled	Set to No prevents the user from placing the parameter in the packet.
Placed	Set to Yes when the parameter is placed into a packet.
Packet	Packet label where the parameter is placed.
Occurrences	Number of occurrences of the parameter in the packet; this number drives the parameter sampling rate; the same number of occurrences is recommended for all the parameters within the same packet.
Bits	Number of source bits for the parameter.

29.5.3 Setting up the KAD/ETH/101

After IENA packets have been configured, you can set up the KAD/ETH/101 to transmit the newly configured packets (for information on setting up IENA packets, see Figure 29-4 on page 6). When setting up the module, you must specify the Module IP address, Module Port and Time to live per packet.

On the Setup tab, complete the fields described in the following table.

Table 29-5: Module setup

Field name	Description
Module IP address	When set, the module can be pinged; for details of pinging the module, see “29.5.5 Testing the connection between PC and the KAD/ETH/101” on page 8.
Module Port	This can be any value between 0 and 65535. We recommend that well known ports as specified in RFC1700 are not used. Section “29.6.1 Appendix 1: Well known ports” on page 10 lists some of the more commonly used well known port numbers. Ensure that your logging device supports this port and that it is not blocked by any fire walls in the test system.
Time to live (s)	An advanced configuration field in the IP header, which determines how long a packet from the module *lives* in the network, in the event that it does not reach its destination. Each switch that a packet passes through as it travels through the network can decrement this field. A switch can dump a packet if its time to live is 0.

NOTE: The Module IP Address field does not assign the IP address for the KAD/ETH/101; this field is used only to program the chassis.

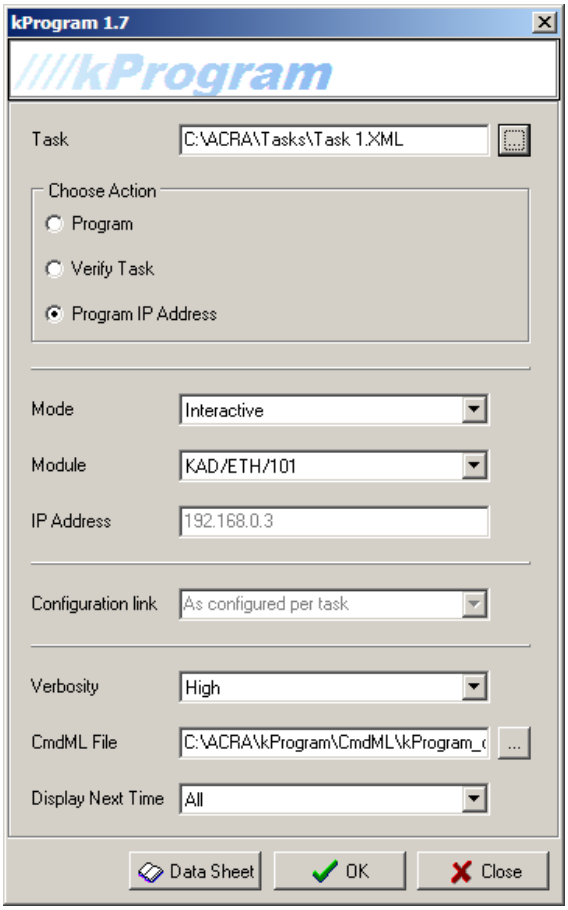
29.5.4 Assigning the KAD/ETH/101 IP address

If pin 39 is connected to GND, the KAD/ETH/101 assumes a default hard-wired IP address—224.0.0.3 is used, as it is an administratively scoped IP multicast address.

You must use kProgram to assign the IP into the module.

1. Launch kProgram.
2. In the **Task** field, browse for the task file required.
3. Select the **Program** IP address radio button.

4. In the CmdML File field, select the xidML file with the KAD/ETH/101 module IP address that you want to assign to. After the xidML file is selected, the IP Address field displays the IP address taken from the xidML file.



5. Click **OK** and follow the on-screen instructions.

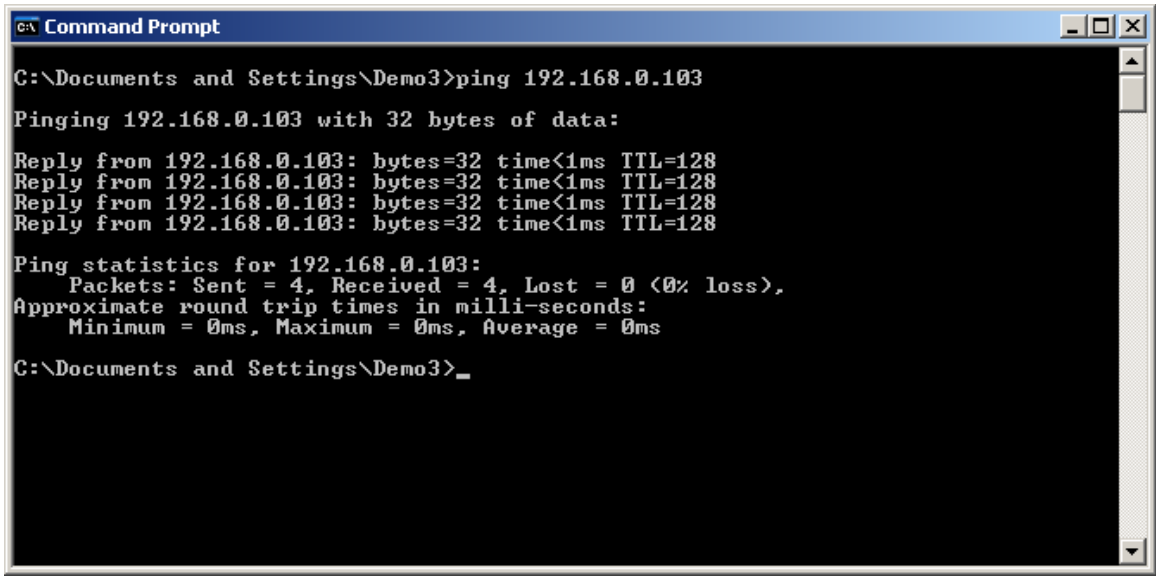
NOTE: Ensure the PC used to assign the KAD/ETH/101 uses the same subnet as the newly assigned KAD/ETH/101 module IP address. This is necessary should you want to use kProgram to perform a test on the IP address.

29.5.5 Testing the connection between PC and the KAD/ETH/101

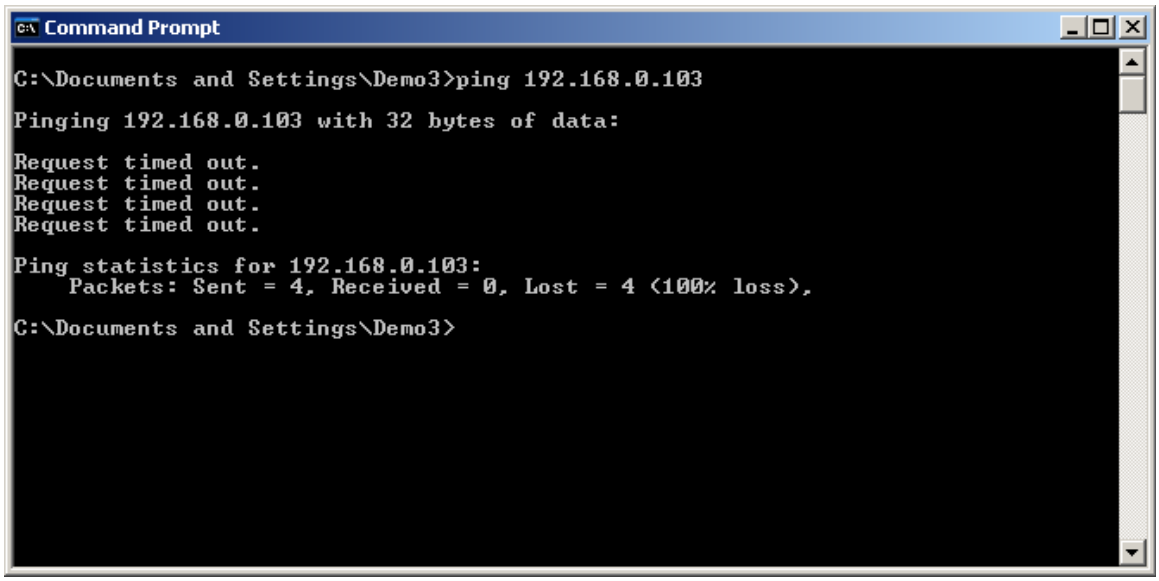
Before programming the unit, check the connection between the PC and the KAD/ETH/101. You can do this by pinging the module from the command prompt.

To ping the KAD/ETH/101, do the following:

1. Click **Start**, **Run**.
2. Type **cmd** and click **OK**.
3. At the C:\ prompt, type ping, space, followed by the IP address of the KAD/ETH/101.
   If the PC is able to connect to the KAD/ETH/101, you get a response similar to that displayed below.



If the ping determines that the PC can communicate with the KAD/ETH/101, the module has been successfully configured and is able to receive packets. If there is a problem and the PC is unable to communicate with the KAD/ETH/101, the response is similar to that shown in the following figure.



If a ping has not been successful, make the following checks:

- Check that the correct IP address was used in the ping command.
- Check that the pinging PC is on the same subnet as the KAD/ETH/101.
- Power down the Acra KAM-500 chassis and check the wiring and power to the chassis.

29.5.6 Programming the KAD/ETH/101

When pinging has determined that a connection between the PC and the KAD/ETH/101 is established, use kProgram to program the KAD/ETH/101.

To program the module, do the following:

1. Launch kProgram.
2. In the **Task** field, browse for the task file required.
3. Select the **Program** radio button.
4. Click **OK**.

For information on using kProgram, contact Curtiss-Wright support (acra-support@curtisswright.com).

29.6 Appendix

29.6.1 Appendix 1: Well known ports

The following table lists some well known port numbers and specifies the server process associated with its contact port. For a complete listing of well known ports refer to: http://www.iana.org/assignments/port-numbers

Table 29-6: Well known ports

Port Number	Description
1	TCP Port Service Multiplexer (TCPMUX).
5	Remote Job Entry (RJE).
7	ECHO.
18	Message Send Protocol (MSP).
20	FTP -- Data.
21	FTP -- Control.
22	SSH Remote Login Protocol.
23	Telnet.
25	Simple mail transfer table (SMTP).
29	MSG ICP.
37	Time.
42	Host Name Server (Nameserv).
43	WhoIs.
49	Login Host Protocol (Login).
53	Domain name system (DNS).
69	Trivial file transfer protocol (TFTP).
70	Gopher Services.
79	Finger.
80	HTTP.
103	X 400 Standard.
108	SNA Gateway Access Server.
109	POP2.
110	POP3.
115	Simple File Transfer Protocol (SFTP).
118	SQL Services.
119	Newsgroup (NNTP).
137	NetBios Name Service.
139	NetBIOS Datagram Service.
143	Interim Mail Access Protocol (IMAP).

Table 29-6: Well known ports (continued)

Port Number	Description
150	NetBIOS Session Service.
156	SQL server.
161	SNMP.
179	Border gateway protocol (BGP).
190	Gateway Access Control Protocol (GACP).
194	Internet Relay Chat (IRC).
197	Directory Location Service (DLS).
389	Lightweight directory access protocol (LDAP).
396	Novell Netware over IP.
443	HTPPS.
444	Simple Network Paging Protocol (SNPP).
445	Microsoft-DS.
458	Apple QuickTime.
546	DHCP Client.
547	DHCP Server.
563	SNEWS.
569	MSN.
1080	Socks.

29.6.2 Appendix 2: IENA specification

IENA has different types such as IENA STANDARD or messages. The KAD/ETH/101 supports only IENA STANDARD. The IENA STANDARD packet is the payload of a UDP packet.

29.6.2.1 IENA data header

The following table shows the IENA data header fields with corresponding size and description. You must define the Key value for each additional IENA STANDARD packet created.

Table 29-7: IENA data header fields

Field	Size	Description
Key	16 bits	Key in IENA standard indicates the type of data in the packet and how data is structured within that packet; this key is a user input.
Size	16 bits	Number of data words in the packet; automatically calculated by the module when packet is built.
Time	48 bits	Time of sampling of first data sample in packet in straight binary microseconds.
Status	16 bits	Reserved.

Table 29-7: IENA data header fields (continued)

Field	Size	Description
Seq	16 bits	Value that increments for each packet of a given key.

29.6.2.2 IENA data footer

The following table shows the IENA data footer end field and its size and description. Once the value is changed, the change applies to all IENA STANDARD packets defined.

Table 29-8: IENA data footer end field

Field	Size	Description
End	16 bits	This is a constant value; a typical value for this is 0xDEAD.

29.7 Glossary

IP address

The address of a device attached to an IP network (TCP/IP network). Every client, server and network device must have a unique IP address for each network connection. The format of an IP address is a 32-bit numeric address, written as four numbers separated by periods. Each number can be zero to 255. For example, 1.160.10.240 could be an IP address.

IP subnet addressing

Routers, or gateways, are used to separate networks. The router breaks the network into multiple subnets. This result may seem familiar as Class A, B, and C addresses have a self-encoded or default subnet mask built in; class A network address - 255.0.0.0: class B network address - 255.255.0.0: class C network address - 255.255.255.0.

MAC address

A hardware address which uniquely identifies each node of a network. In IEEE 802 networks, the Data Link Control (DLC) layer of the OSI reference model is divided into two sublayers—the Logical Link Control (LLC) layer and the Media Access Control (MAC) layer. The MAC layer interfaces directly with the network medium. Consequently, each different type of network medium requires a different MAC layer.

Port

A number used, in conjunction with the IP address, to indicate one end of an Ethernet conversation. Some port numbers are reserved for particular services. The port number identifies what type of port it is. For example, a server listening for HTTP traffic listens on port 80. Port numbers range from 0 to 65536, but only port numbers 0 to 1024 are reserved for privileged services and designated as well known ports. For more information, see http://www.iana.org/assignments/port-numbers.

Switch

A device that can route data only to the nodes (and links) for which the data is intended. Using a switch eliminates the possibility of collisions on a node link. Also, as long as the total bandwidth available to data leaving the switch is the same as, or greater than, the total bandwidth of data entering the switch, there is no data loss.

UDP

User Datagram Protocol. An unreliable connection-less transport protocol which doesn't provide a guarantee that packets arrive, or that they arrive in the order in which they were sent. UDP is widely used for streaming audio and video, voice over IP (VoIP) and video conferencing.