Lucidata Diplomat jr

Model jrNS-CDF

Network Synchronous Server

Lucidata House
Selwyn Close
Great Shelford
CAMBRIDGE CB22 5HA
England

tel: +44(0)1223 846100
fax: +44(0)1223 846100
email: info@lucidata.com

Publication Details

All possible care has been taken in the preparation of this publication, but Lucidata accepts no liability for any inaccuracies that may be found.

Lucidata reserves the right to make changes without notice to both this publication and to the product which it describes.

If you find any errors in this publication or would like to make suggestions for improvement, please write to the Company at the address below.

Lucidata House
Selwyn Close
Great Shelford
CAMBRIDGE
CB2 5HA
England

tel: +44(0)1223 846100
fax: +44(0)1223 846100
email: info@lucidata.com

Diplomat jrNS-CDF User Guide Issue Number 1 (10/03)

Revision Details

Issue	First Published	Revised	Pages
1	10/03	11/03	9
		02/04	8
		06/05	2
		08/07	1,2,3,9,10,11,20,21,22,23,28

All Lucidata products are designed, developed and tested under the control of its ISO9000 compliant Quality Management System. The high quality of our products is thus assured. Should any issues on the quality of our products arise please address them to the Quality Manager at the address given on page 2. This User Guide contains all the necessary information for the proper installation and configuration of the product to ensure the highest level of performance.

Warranty

Lucidata warrants that the products described in this User Guide are free from defects in manufacture and that they meet the specifications and functionality described in this User Guide. Lucidata will replace parts and repair defects in manufacture, on a return to factory basis, for a period of 12 months from the date of our original invoice provided that the product has only been used in the manner and for the purpose described in this User Guide. Lucidata does not warrant that the products described in this User Guide are suitable for any specific application and the purchaser must satisfy him/herself of the suitability of the product for the intended application as best known to him/herself. Lucidata does not accept any contingent liability for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages arising from the use of its equipment. Lucidata assumes that if its equipment is used in a business critical or any other essential application, then the system design should incorporate sufficient resilience to ensure that a single failure would not have disproportionate consequences.

Service and Support

If a unit fails, and you have bought it from a Lucidata appointed dealer, you should contact that dealer. If bought from the manufacturer, return the unit in its original packing to the address on page 2.

You should telephone or fax Lucidata prior to returning the unit to ascertain whether an apparent fault is due to mis-operation rather than to a technical fault within the unit and to obtain a returns number.

Lucidata reserves the right to charge for any investigation of an apparent fault that is found to be due to incorrect operation, or for the repair of a fault that is due to the unit not being used in accordance with the instructions in this User Guide.

Maintenance

Faults that occur outside the warranty period and are not covered by a separate maintenance contract, will be repaired on a time-and-materials basis. Please telephone Lucidata prior to returning your unit. You will be given an estimate of the repair costs.

Introduction

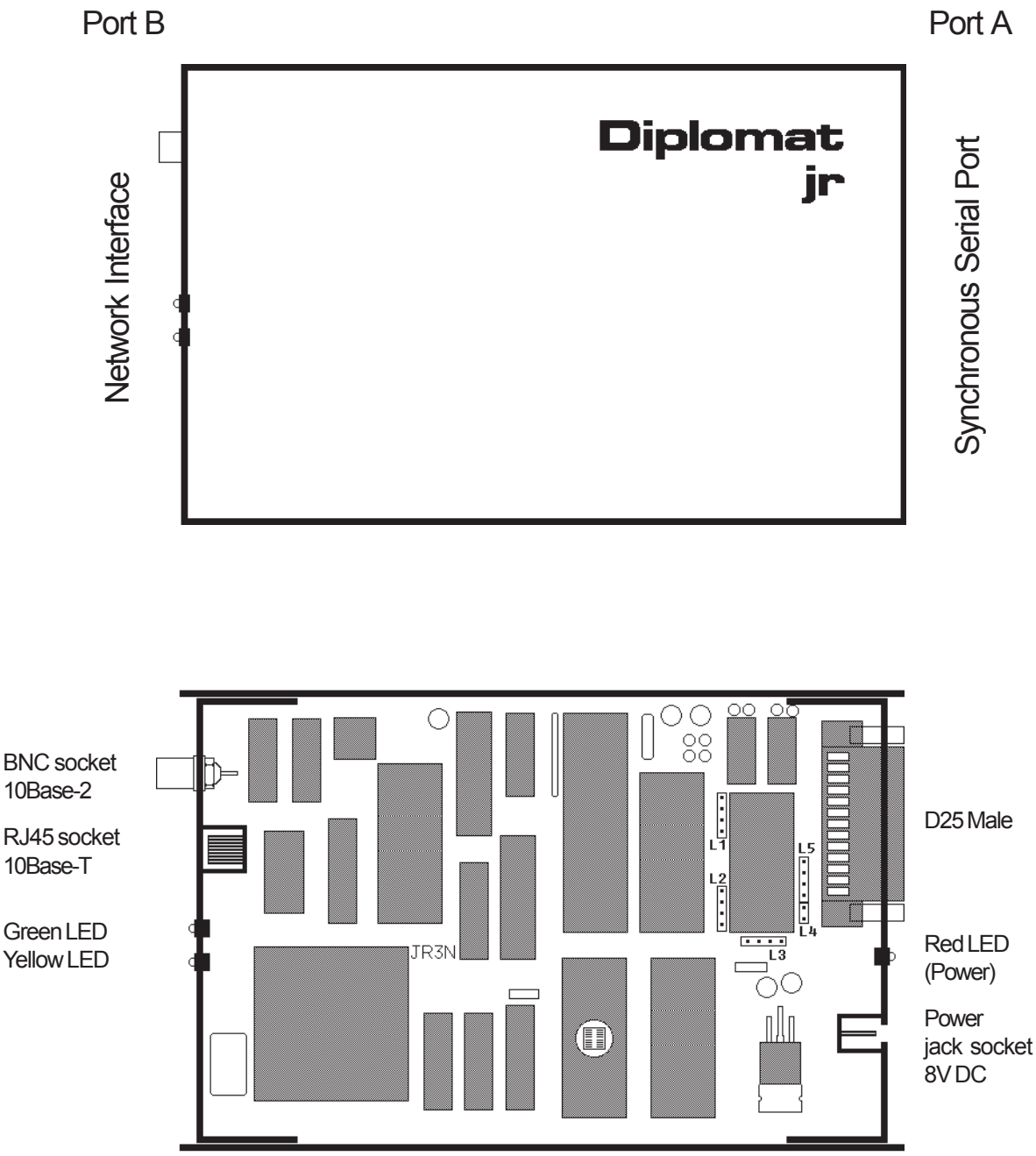
The Lucidata *Diplomat* model *jrNS* is one of a family of simple connectivity solutions built around Lucidata's popular Diplomat jr product. The *jrNS* model has been designed specifically to interface to the most common local area network (LAN) media utilising Ethernet technology and employing the TCP/IP transport level protocols. Despite network technology being rather complex, Lucidata has always sought to make its products easy to use and user friendly. We believe that our products should just be connected up and left to do their job with little or no intervention necessary from the user.

To this end most Lucidata products are supplied with simple menu driven configuration screens that can be accessed with any simple local terminal or emulation. Remote configuration over the network is also possible but due to the inherent security implications of such a method it is not the default method.

The *Diplomat jrNS* is the member of the Diplomat jr family that enables interconnectivity between an Ethernet/IP network and devices running legacy frame synchronous protocols using serial RS232 communications. The protocol supported by a particular model is determined by the firmware installed in the EPROM. The JRNS-CDF supports the transport of a character delimited synchronous serial data stream over a TCP/UDP/IP network using UTP Ethernet.

This manual is structured to require the minimum of reading to effectively operate the *Diplomat jrNS*. If, as is our usual policy, Lucidata has configured your unit for you, you will only need to read Chapter 2, *Getting Started Quickly*, to discover what plugs into where and you will be on the air.

If your unit is not configured yet you will need to read Chapter 3 on *Configuration* to discover what information you need to get your hands on before starting that process. If you are wondering why you bought a *Diplomat jrNS* then Chapter 4, *Operation*, is where we tell of all the things that the *jrNS* can do and how to drive it. You will probably want to read this chapter anyway. Networks can be complex things and problems can and do arise which may generate many and varied error messages, some coming from within the *Diplomat jrNS* and others from outside but reported to the interface. Chapter 5, *Trouble Shooting and Error Messages*, documents these and gives probable explanations and recommended courses of action. Finally Chapter 6, *Technical Specification*, contains the dry detail of the hardware so you know what pins to use.


Port B
Port A
Diplomat
jr
Network Interface
Synchronous Serial Port
BNC socket
10Base-2
RJ45 socket
10Base-T
Green LED
Yellow LED
JR3N
L1
L2
L3
L4
L5
D25 Male
Red LED
(Power)
Power
jack socket
8V DC

When you hold the *Diplomat jrNS* in your hand so that the Diplomat jr logo is oriented in the normal reading orientation, the Network end is to the left and the Serial interface is to the right. For documentation purposes we refer to the Serial interface as Port A and the selected network interface as Port B.

Port A

Port A is wired as a Serial Synchronous DTE and any cable that was designed to connect a terminal type device to a modem using a 25 pin female D type connector will be suitable to connect your DCE device to Port A.

Port B

Port B has a 10Base-T RJ45 connector and optionally a 10Base-2 BNC connector. If both are present connection should be made to only one of these connectors otherwise the Auto Media Sensing will get confused and probably choose 10Base-2. The Auto Media Sensing only operates at power-up time so changing the connector during operation will not have the desired effect. The 10Base-T connector is wired for direct connection to a hub using UTP cable.

Power

The power lead from the mains adaptor is plugged into the socket on the Port A end. When power is applied to the adaptor the Red LED by the power connector should light. If it does not you probably have a dead mains socket but refer to Chapter 5, *Trouble Shooting* and *Error Messages* to discover what to do.

If you have selected the 10Base-T connector the Green LED by the RJ45 socket should be illuminated to indicate a good link to the hub. If not consult Chapter 5.

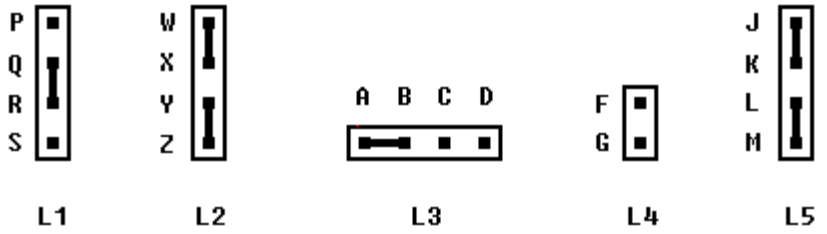
The *Diplomat jrNS* is now operational and should be doing what was expected. If there is traffic on the network then the Yellow LED by the RJ45 connector will be flashing.

If the *Diplomat jrNS* has been configured as a Server then it will just wait until someone makes a connection over the network. If it is configured as a Client then the *Diplomat jrNS* will attempt to make a connection to the remote server defined in its configuration when the configured initialisation condition occurs.

Pinouts and Links

Because the Synchronous Serial interface of the *Diplomat jrNS* has been designed to be general purpose some of the 25 pins on the D25 male plug have a variable function. It is therefore essential that connection is only made to those signals that are needed for a particular application and to no others.

The following table lists all the pins and shows how they are assigned for some standard applications. The default jumpers shown are for the *Diplomat jrNS* to supply the clocks.

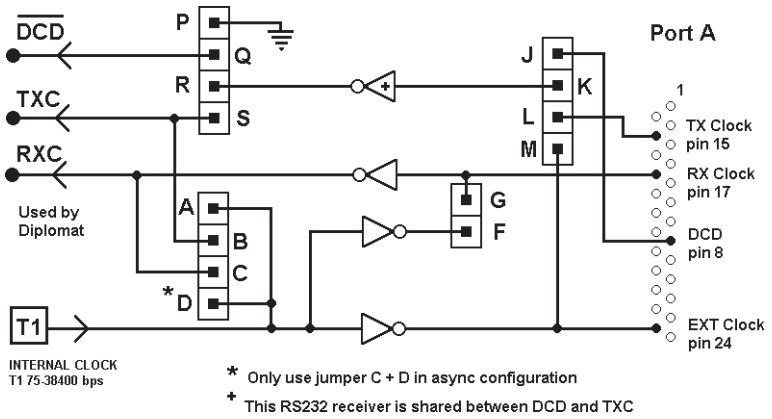


Pin No.	Name	Link L1	Link L3	Link L4	Link L5	Function
1	Screen					Connected to groundplane
2	TXD					jrNS Transmits Data
3	RXD					jrNS Receives Data
4	RTS					jrNS Signals Ready to Send
5	CTS					External Cleared to Send
6	DSR					N/C
7	Common					Signal Return
8	DCD	Q+R P+Q	- -	- -	J+K -	Uses DCD Signal from DCE Held High Internally
15	TXC	R+S - -	- B+C A+B A+B	- - - -	K+L - - L+M	Uses External TX Clock from DCE Uses External RX Clock from DCE Uses Internal Clock Outputs Internal Clock on pin 15
17	RXC	- - -	- - C+D	- F+G -	- - -	Uses External RX Clock from DCE Outputs Internal Clock on pin 17 Uses Internal Clock iff IC20 removed.
20	DTR					Held High by Diplomat
24	EXC					Outputs Internal Clock always

Desired Interface	IC2	IC20	Link L2
Serial Synchronous	MC6852	MAX232	W+X,Y+Z
Serial Asynchronous	MC6850	Remove	X+Y

NOTE: L1 MUST have either P+Q or Q+R with J+K. This is because DCD must not be left floating

The following diagram shows the realationship between the various clock and DCD selection links



Remote Configuration

All *Diplomat jrNx* can be configured remotely using one of two programs or a local *Diplomat jrNA*. It is necessary in the case of the *Diplomat jrNS* and *Diplomat jrNP* variants as they do not have an asynchronous RS232 port.

JrConfig Program

The JrConfig program runs on a standard Windows PC and is self documenting. It will assume it is on a Class C network and determine the broadcast address for its subnet. When the Search Button is pressed JrConfig will find all Diplomats present on the subnet. The selected Diplomat is then available for configuring.

JRemote Program

The JRemote program aims to give a similar presentation as would be observed if a local connection had been made to a Diplomat fitted with an asynchronous RS232 interface. It enables control as well as configuration of the remote Diplomat. All that is required to initialise the program is to fill in the IP address of the Diplomat it is desired to configure, Tab to the Command text box and enter characters just as described in the following section using a *Diplomat jrNA*. The displays invoked by the *Diplomat jrNA* will appear in the large window of the program.

Local Diplomat jrNA

The *Diplomat jrNA* should first be configured as a UDP Client with Error Reporting using the following values for configuration bytes A and B.

A=11001100
B=10101010

In the Network Menu, the IP address of the remote jrN to be configured should be substituted for the Remote IP address and the Server port should be set to 12345. This is the reserved UDP port number that all Diplomats use for configuration. Ensure that the Default Gateway is the one required to obtain a route to the remote jrN. Send a few Pings to the remote jrN using the "E" command to verify it is contactable. Then on hitting the Return key three times a new Main Menu display should appear. This Menu is coming from the remote jrN as is shown by the Terminal Profile now showing "Remote Control" instead of "Local Port".

Factory Settings

Should the configuration of the *Diplomat jrNS* become corrupted for any reason so that it no longer responds to the IP address that was assigned to it, it can be reset to the factory configuration. To do this make a D25 female socket with a link between pin 4(RTS) and pin 8(DCD) and plug it into Port A. Power the unit up, wait 5 seconds, and power it down. Remove the special socket and the unit will be reset to the factory defaults.

Main Menu

```
Lucidata Diplomat C 1995-2007
Model JRNS-CDF rev 1.02:5005

Terminal Profile is <Remote Control>
Type Single Digit to Select, <CR> to Exit

<A> Set Port A Configuration Byte
<B> Set Port B Configuration Byte
<C> Set Character Configuration Byte
<D> Set Data Rate Configuration Byte
<F> Set First Frame Byte
<L> Set Last Frame Byte
<I> Set Line Idle Byte
<S> Enter Statistics Menu
<N> Enter Network Control Menu
<R> Reset Diplomat Softly

Select < >
```

For all intents and purposes the Local Terminal is connected to the remote *Diplomat jrNS*. All menu driving commands work in the usual way with the exception that no control characters are sent to the remote *Diplomat jrNS*. Make very sure of the changes that are made because they will be remembered by the remote *Diplomat jrNS* when the Main Menu is left and if the IP address has been changed erroneously you may not be able to contact the *Diplomat jrNS* again without following the reset procedure described earlier.

The remote *Diplomat jrNS* will also perform a soft restart after saving the new configuration and any existing TCP connection will be lost.

It must be emphasized that typing Return when in the remote Main Menu is necessary for new configuration values to be stored, but typing CTRL/P at any time will return to the local *Diplomat jrNA* Main Menu if one is being used. The remote *Diplomat jrNS* will be left in whatever state it was in. Although the remote menu displays look the same as if the configuration was being done locally they are actually performed in parallel with whatever the remote *Diplomat jrNS* was doing at the time. If no configuration values are changed because you only viewed the statistics or got the remote *Diplomat jrNS* to Ping its Server then that will not force a restart and any existing TCP session will be preserved.

Configuration Bytes

The current generation of *Diplomat jr*s grew from a generation that had lots of configuration switches on the PCB to set up options. This required taking the lid off the box to make changes and in addition the switches occupied valuable PCB space that could be better utilised for extra functionality. The *Diplomat jrNx* has non-volatile memory so it can remember any configuration details that it is given. For simplicity we have introduced the concept of 'Silicon Switches' to select low level options. They are directly analogous to ordinary switches but only exist in the Diplomat's memory.

In the *Diplomat jrNS* there are four sets of Silicon Switches associated with four Configuration Bytes. Configuration Byte A controls the major characteristics of Port A and Configuration Byte B controls the major characteristics of Port B. Configuration Byte C allows specification of the character format to be used on Port A and Configuration Byte D determines the internal serial clock rate. There are also three application level switches F,L and I for specifying framing characters.

Selecting A, B, C, D, F, L or I from the Main Menu will cause the appropriate Configuration Byte to be displayed and the cursor will be positioned under the first bit. At this stage the following characters can be typed in to change the configuration byte:

CR - Return to Main Menu with the value of the configuration byte set to the displayed value.

Space - move cursor to the right without changing the byte.

BS - move the cursor to the left without changing the byte.

0 - Change the 'Switch' above the cursor to 0 and move cursor right.

1 - Change the 'Switch' above the cursor to 1 and move cursor right.

Note - if any operation moves the cursor off either end the system returns to the Main Menu.

Because the configuration bytes set low level properties of the Diplomat they should be set up prior to attempting to configure the Network parameters.

By convention the switches or bits of a configuration byte are numbered as follows

7	6	5	4	3	2	1	0

Configuration Byte A Specifies Protocol on Port A

Bit	Name of Switch	Description
2,0	BMBLK	[111] - Mask to extract blocking size [000] - Do not use blocking [001] - Forward when 1 byte collected [010] - Forward when 10 bytes collected [011] - Forward when 50 bytes collected [100] - Forward when 100 bytes collected [101] - Forward when 200 bytes collected [110] - Forward when 500 bytes collected [111] - Forward when 1000 bytes collected
3	BCRTSF	[0] - RTS is asserted when the unit has data to send [1] - RTS is kept high while unit is powered up
4	BCDCD	[0] - DCD is asserted when data is sent to the unit [1] - DCD is kept high while the DCE is powered up.
5	BFFST	[0] - Do not forward First Framing byte to the Network [1] - Forward the First Framing byte to the Network
6	BFLST	[0] - Do not forward Last Framing byte to the Network [1] - Forward Last Framing byte to the Network
7	BFIDL	[0] - Do not forward received idle bytes to the Network [1] - Forward received idle bytes to the Network

Note (i) These bits determine the criteria for forwarding data from Port A onto the Network

Configuration Byte F defines the First Framing Byte

Configuration Byte L defines the Last Framing Byte

Configuration Byte I defines the Idle Byte.

Configuration Byte B defines Protocol on Port B

Bit	Name of Switch	Description
0	BRSTAH	[0] - Only allow current Host to Reset current TCP session [1] - Allow any Host to Reset a current TCP session
1	BRSTAP	[0] - Only allow current Port on current Host to Reset current TCP session [1] - Allow any Port on current Host to Reset current session
2	BPEER	[0] - Only allow Client/Server relationships [1] - Allow Client/Client relationships
3	BSTART	[0] - Wait for Port data before starting TCP session [1] - Start TCP as soon as powered up
4	BSERVR	[0] - Behave as a Client device [1] - Behave as a Server device
5	BDCDF	[0] - Ignore DCD dropping on Port A [1] - Close any open TCP session if DCD drops
6	BTCPUD	[0] - Use TCP protocol [1] - Use UDP protocol
7	BEXREP	[0] - Do not report network originated errors [1] - Report ICMP network messages in text form to Port A

Note (i) If BPEER=1 the unit will allow a remote host to establish a TCP session with it if, and only if, the IP address and the Port address of the remote host are the same as those declared in the Network Menu for Remote IP Address and Remote TCP Server Port.

Note (ii) BEXREP must be set to zero in model DCF

The meaning of the bits in Configuration Byte C are given in the following table.

Data Bits	Parity Bits	Bit 5	Bit 4	Bit 3
6	E	0	0	0
6	O	0	0	1
7	N	0	1	0
8	N	0	1	1
7	E	1	0	0
7	O	1	0	1
8	E	1	1	0
8	O	1	1	1

Where the Parity Bit Codes mean None, Even or Odd

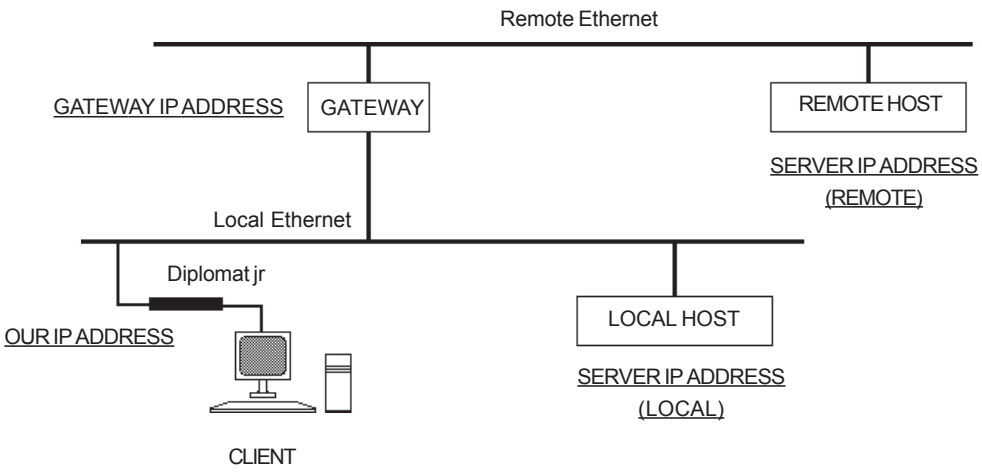
The meaning of the bits in Configuration Byte D are given in the following tables.

Clock 1 (T1) is controlled by bits 0 to 3

Speed (bps)	Bit 3	Bit 2	Bit 1	Bit 0
75	0	0	0	0
150	0	0	0	1
300	0	0	1	0
600	0	0	1	1
1200	0	1	0	0
2400	0	1	0	1
4800	0	1	1	0
9600	0	1	1	1
19200	1	0	0	0
38400	1	0	0	1
14400	1	0	1	0
28800	1	0	1	1
38400	1	1	0	0
38400	1	1	0	0
38400	1	1	0	1
38400	1	1	1	0
38400	1	1	1	1

Note Clock 1 only controls the Transmit Clock (TXC) in model CDF

Network Parameter Configuration



Now that the basic configuration of the *Diplomat jrNS* has been performed we can safely move on to setting up the Network Parameters.

Typing 'N' at the Main Menu will bring up the Network Control Menu.

```
Network Control Menu  -
Diplomat is configured as a TCP Server

Our Ethernet Address is  - 00 A0 EF 00 00 0C
Our Diplomat IP Address is  - 128.18.18.12
Default Remote  IP Address  - 128.18.18.255
Default Gateway IP Address  - 128.18.18.255
Default Sub-Net Address Mask  - FFFFFF00
Default TCP/UDP  Service Port Id.  -   7000
Status of TCP Session  - CLOSED

  <O> Set Our IP Address
  <S> Set Remote/Server IP Address
  <G> Set Gateway IP Address
  <M> Set Sub-Address Mask
  <P> Set Server Port Id.
  <C> Set Client Port Id.
  <F> Firewall Definition Menu
  <A> Broadcast ARP Request
  <B> Broadcast BOOTP Request
  <R> Broadcast RARP Request
  <E> Send ECHO Request to Remote

<CR> Returns to Previous Menu
```

In the above screen the Diplomat has been configured as a Server. In a later screen the slight differences when it is configured as a Client will be obvious.

The Ethernet Address is unique to the unit and cannot be changed. It is displayed for information only.

The three IP Addresses are all changed in the same way. First a key letter is selected:

'O' to set the Local IP Address of the Diplomat itself, 'S' for the Remote host and 'G' for the local Gateway. If there is no local gateway then the gateway address should be set to the same as the remote host. The following is a typical prompt:

```
Enter New IP address in Decimal Dot Notation
Address of this Diplomat (Client/Server) -
```

If the Return key is entered no changes are made and the screen refreshes to show the current values. Fields may be skipped by typing a '.' until the field you want to change is reached and then simply typing the new decimal value and hitting Return will update the value.

At this point, contact will be lost with the remote *Diplomat jrNS*. The Host jrN should now be re-configured so that it uses the new Remote IP address to re-establish contact with the remote *jrNS*.

Whether you are using Sub-Networking on your network or not the Sub-Net mask should be such that when applied (perform a bitwise AND operation) to both the Local IP Address and the Remote IP Address the masked values match. If a local gateway is used then the masked Gateway IP Address should match the masked Local IP Address. ie communicating devices must be on the same conceptual sub-net.

Typing 'M' will invoke the following response:

```
Enter Sub-Address Mask in hex
```

You should now enter the full eight hex characters to specify the 32 bit mask.

The TCP/UDP Local Service Port is the port number that a Client host will use to make a connection to the Diplomat when it is acting as a Server. The Diplomat will not respond to attempts to communicate with any other port number.

Typing 'C' will invoke the following response:

```
Enter TCP Port Address in Decimal -
```

Care should be taken to ensure that the value chosen is within the range allowed by the remote host TCP/IP stack. Some systems impose restricted ranges ie.2000 to 4000.

When the Diplomat is configured as a Client there are two port addresses required. This time the Service Port is the Server Port number that the Diplomat will try to establish a connection with on the Server and the Client Port number is the Diplomat's own local port ID.

If the value of 23 is chosen for the Service Port the Diplomat will perform Telnet control character processing by adding or removing NUL characters after CR characters.

The Port value 12345 should not be used as it is reserved for remote interrogation of the *Diplomat jrNS*.

Typing 'F' will invoke the Firewall Definition Menu

```
Firewall Definition Menu - feature activated by non-zero
values

Acceptable Hosts and Ports

1.   0.0.0.0 :      0
2.   0.0.0.0 :      0
3.   0.0.0.0 :      0
4.   0.0.0.0 :      0
5.   0.0.0.0 :      0
6.   0.0.0.0 :      0
7.   0.0.0.0 :      0
8.   0.0.0.0 :      0


<C> Clear All entries, Disable feature
<A> Add an entry, <D> Delete an entry, <E> Edit an entry

<CR> Returns to Previous Menu
```

The feature only has effect if the *Diplomat jrNS* has been configured as a Server or Peer. The Firewall is activated by defining a non-zero IP address. When activated the remote host IP address defined in the Network Control Menu is ignored and only those hosts defined in the firewall list will be able to start up a TCP session or enter into a UDP exchange. IP and port values are entered in exactly the same manner as described for the previous menu.

The Status of the TCP session is shown for information purposes and will be unaffected provided that no changes are made to the network parameters. Therefore it is possible, during an active session, to interrogate the Network Control Screen without causing any damage to the active session.

Normal Network Operation

As long as the *Diplomat jrNS* is properly configured and is not in Network Monitor mode it is in the Normal Mode of operation. It will process the following Ethernet message types:

ARP messages addressed to the local IP address
RARP messages containing the local Ethernet address
ICMP messages addressed to the local IP address
UDP messages addressed to the local IP address and the local port or the configuration port
UDP messages addressed to the Broadcast IP address and the local port or the configuration port
TCP messages addressed to the local IP address and the local port

Responses to ARP, RARP and ICMP are performed automatically and the user will in general be unaware of the activity. ARPs have no effect other than providing or giving essential information about Ethernet and IP addresses but a RARP request can cause the *Diplomat jrNS* to change its IP address to the value contained in the RARP reply.

When the *Diplomat jrNS* is configured as a Client it checks to see if it has a good Ethernet address for either the Default Gateway or Remote Server and issues an ARP if it does not. If the *Diplomat jrNS* determines that the Remote Server Address is on a different Sub-Network to itself it will address the ARP to the Default Gateway. The Ethernet address contained in the ARP reply will be used subsequently to address packets to the Remote Server. This process is repeated every 2 seconds until a valid reply has been received.

The *Diplomat jrNS* cannot send data until it has a valid ARP entry in its tables. For this reason an entry is preset into the ARP table for the Sub-Network broadcast IP address (host address of all ones) together with an Ethernet address of all ones. This is to enable a UDP client to generate UDP broadcasts if the Remote Server IP Address is set equal to the Sub-Network broadcast IP address. In this case the *Diplomat jrNS* does not issue any automatic ARP requests.

The *Diplomat jrNS* may be set up as a UDP Client or Server, or a TCP Client or Server. The following paragraphs describe the properties of each set up.

UDP Client/Server

When configured as a UDP Server the *Diplomat jrNS* will wait until a UDP packet is received from a remote host which is addressed to the local IP address and Server Port held in the jrN. The *Diplomat jrNS* cannot send any data over the network until it has received a packet containing a Source Port and IP address for it to use as a return address.

If a UDP packet arrives from another host before the *Diplomat jrNS* has sent a reply to the previous host, the new packet will be ignored unless switch BRSTAH = 1. If BRSTAH = 1 the new packet's Source IP and Port addresses become the new Destination addresses for any *Diplomat jrNS* reply.

When the *Diplomat jrNS* is configured as a UDP Client it will transmit a UDP packet over the network as soon as it has some qualified data to send. It will use the Remote Host address and Server Port address held in its tables to address the packet and will use its own Client Port address for the Source Port address field in the transmitted packet.

If switch BPEER=1 then the *Diplomat jrNS* will accept an initial contact as if it were configured as a Server, provided that the packet came from the Remote IP address and Server Port held in its tables.

The UDP service is a connectionless service with no guarantee of delivery. Only data contained in UDP packets whose header checksums are correct are passed on transparently to Port A.

TCP Client/Server

When configured as a TCP Server the *Diplomat jrNS* will wait until a remote host attempts to establish a TCP Session with it. This requires a proper three way handshake and matching Destination IP and Port Addresses to those held within the jrN. The Source Port address and IP address of the remote host are stored locally for use as a return address. Should a new attempt to initiate a TCP session be detected from the same IP address and port, then the existing session is considered broken and the *Diplomat jrNS* returns to its initial waiting state after first issuing a Reset to the old session. Similarly if the remote host sends a Reset or Close command then the *Diplomat jrNS* terminates the current session and returns to the waiting state.

These rules are relaxed if switch BRSTAH = 1. If BRSTAH = 1 any new host attempting to initiate a TCP session will cause the current session to issue a Reset to the old session and close down. The second attempt by the new host will be successful. In addition if BRSTAP = 1 any Reset packet received will be actioned if it comes from the current host IP address but need not be from the same port.

Neither switch has any effect if the Firewall feature is enabled as this alone will determine who is able to talk to the *Diplomat jrNS*. New session requests or Reset commands from any Firewall qualified host/ports will be accepted and actioned as described above. The *Diplomat jrNS* cannot initiate a TCP session when in Server mode.

Opening TCP Sessions

When configured as a TCP Client the *Diplomat jrNS* will attempt to initiate a TCP session with the Remote Server on the declared Server Port as soon as it has qualified data to send. Only packets from the Remote Server IP address and Port address will be processed.

Closing TCP Sessions

In both modes the user has control over the closing of active TCP sessions.

Normal Serial Port Operation

The model CDF uses Character Delimited Framing to handle the data flow on the synchronous port. In its idle mode - that is when there is no data available from the network - the synchronous port asserts pin 4 (RTS) OFF if bit BCRTS=0 or permanently ON if BCRTS=1. The internal clock is always available on pin 24 and as a Transmit Clock (TXC) on pin 15. If BCRTS=0 the idle Transmit Data (TXD), pin 2, is held in the MARKING state but if BCRTS=1 the transmitter keeps sending the Idle character defined by Configuration Byte I. An idle condition from the connected DCE is sensed when pin 8 (DCD) is OFF and the Received Data (RXD), pin 3, is MARKING. If bit BCDCD=1 then the DCE may be transmitting idle characters but unless the Diplomat's receiver has been previously synchronized they will not be seen.

Data flow Port A to Port B

The Receiver remains unsynchronized until a character which matches the FIRST character defined by Configuration Byte F appears on the line. If bit BFFST=1 it is copied to the network buffer otherwise it is discarded. Consecutive bytes are copied to the network buffer until a character matching the LAST character defined by Configuration Byte L is encountered. If bit BFLST=1 this character is copied to the network buffer and the network application notified there is a packet to send over the network. If the field defined by BMBLK is non-zero then the byte count determined by that field will control when a packet is sent over the network. The network buffer will always be flushed to the network when DCD drops or the maximum TCP segment size (1460) has been accumulated. The tests controlling forwarding are always performed in the following order.

i) Has DCD dropped?
ii) Has the maximum TCP segment size been reached?
iii) Is a forwarding block size defined and has it been reached?
iv) Have we been notified of a completed packet?

If BCDCD=1 the Diplomat will continue to receive idle characters and if bit BFIDL=1 they will be forwarded to the network buffer. If BCDCD=0 or BFIDL=0 the synchronization of the receiver is cleared so that no more data is forwarded until the occurrence of another FIRST character.

Data flow Port B to Port A

When data arrives from the network the complete packet is copied to the port buffer. If the Transmitter is already transmitting the data is just appended to the current stream. If the Transmitter is idle the first character of the new data is compared to the FIRST character. If it matches FIRST it and all following characters are transmitted over the line. If the first character does not match FIRST and bit BFFST=0 a FIRST character is output ahead of the new data stream. When the data stream from the network runs out the last character is examined and if it does not match LAST and bit BFLST=0 then a LAST character is sent out as a final character.

Byte data is shifted in and out on the synchronous lines Least Significant Bit (LSB) first.

Special Cases HDLC Data Stream

If both the FIRST and LAST characters are equal to $7E, the HDLC Flag character, the Diplomat will provide the following support. The data flow from Port A is assumed to be framed by Flag characters and to have been "bit stuffed". The data stream is "unstuffed" and if the special characters $7E and $7D are found within the data field they are converted to the character pairs $7D $5E and $7D $5D respectively.

The data flow from Port B is assumed to be framed by Flag characters and that any $7E or $7D data characters will have been converted to $7D $5E and $7D $5D pairs respectively. These are converted back to $7E and $7D before "bit stuffing" and being transmitted out on Port A.

CRC16 Terminated Data Stream

If the LAST character is set the same as the IDLE character then the frame termination condition is considered to occur when two consecutive IDLE characters have appeared. This case is common when the protocol being used places a 16 bit CRC after the termination character that would otherwise be used as a terminator. The data stream from Port B should start with one or more FIRST characters followed by the data frame and be terminated with two or more IDLE characters. It follows that the data stream must not contain two consecutive IDLE characters unless they are suitably escaped.

LED Indicators

The *Diplomat jrNS* has three LED indicators to provide basic operational status. The red LED by the power socket indicates that +5 volts is available internally. The other two LEDs are by the network connectors.

The green LED illuminates if a good 10Base-T connection has been made.

The yellow LED blinks whenever a packet is received from the network. If 10Base-2 is selected then it also blinks when a packet is transmitted.

Basic Error Conditions

There is very little that can fail on the *Diplomat jrNS* that will not result in complete unit failure necessitating return of the unit to the factory for repair. Most trouble shooting will revolve round the units relationship with the network it is connected to. Extensive tools have been provided to assist in the tracking down of network problems. However we will first of all deal with the identification of the cause of a units failure to operate.

a) Red LED is not illuminated - no volts

i) Check mains power by plugging in another device eg. desk lamp
ii) Check volts at end of power lead.
If <+7volts DC power adaptor is dead
Return unit and adaptor to supplier (see page 4)

b) Green LED is not illuminated when using UTP cable

i) Try different port or hub, power-up unit
ii) Try different cable, power-up unit
iii) Try 10Base-2 port if possible, power-up unit
Return unit and adaptor to supplier (see page 4)

c) Cannot get Remote Menu up

i) Check that the configuring *Diplomat jrNA* or program is able to reach the default declared IP address of the *Diplomat jrNS*.
ii) Reset the Diplomat to default settings and try again. (See Page 9)

Return unit and adaptor to supplier (see page

Statistics Display Port B

The Statistics display is accessible using all three remote configuration methods. Typing 'S' from the Main Menu will produce a list of statistics which can give a clue as to where the problem could be coming from.

```
Diagnostic Display of Monitored Counters

All counters except the clock are now reset

Number of Seconds since last initialisation - 19

Number of Packets for this unit  -          0
Number of Multicast Packets seen -          0
Number of Broadcast Packets seen -          0
Number of Transmitted Packets    -          0

Count of Unknown Ethernet Types  -      0
Count of Bad IP Datagrams -      0
Count of Bad TCP Segments -      0

Count of Receive Buffer Overruns -      0
Count of Failed DMA Transfers    -      0
Count of Aborted Transmissions   -      0
Count of Hardware Exceptions     -      0
Number of Free Buffers -   16
Lowest number of buffers - 14
Count of Software Ints. - 0
No Current TCP Session

<CR> Returns to Previous Menu
```

Any significant counts in the Hardware Exceptions or Aborted Transmissions could be an indication that the unit was beginning to fail.

Counts of Bad IP Datagrams, TCP Segments and Unknown Ethernet types is an indication of a failing network which could also generate some of the other counts already mentioned.

If the number of free buffers ever reaches zero then there is a serious internal problem.

Network Trouble Shooting

Trouble Shooting can only be performed using a *Diplomat jrNA* or the program JRemote.Typing 'N' at the Main Menu brings up the Network Control Menu which we have seen before.

```
Network Control Menu  -
Diplomat is configured as a TCP Server

Our Ethernet Address is  - 00 A0 EF 00 00 0C
Our Diplomat IP Address is  - 128.18.18.12
Default Remote  IP Address  - 128.18.18.255
Default Gateway IP Address  - 128.18.18.255
Default Sub-Net Address Mask  - FFFFFF00
Default TCP/UDP  Service Port Id.  -   7000
Status of TCP Session  - CLOSED

<O> Set Our IP Address
<S> Set Remote/Server IP Address
<G> Set Gateway IP Address
<M> Set Sub-Address Mask
<P> Set Server Port Id.
<C> Set Client Port Id.
<F> Firewall Definition Menu
<A> Broadcast ARP Request
<B> Broadcast BOOTP Request
<R> Broadcast RARP Request
<E> Send ECHO Request to Remote

<CR> Returns to Previous Menu
```

There are two commands that are most useful in probing the network to find out if the Remote Host that the *Diplomat jrNS* is trying to work with is actually reachable.

If the Remote Host is on another network segment and it is necessary to go via the Default Gateway then the link to the Gateway should be tested first. To do this it is necessary to temporarily change the Remote Server IP address to be the same as the Default Gateway. When the path to the Default Gateway has been verified then the Remote Host IP Address can be entered into the Remote Server IP address again to test its reachability.

Typing 'A' causes the *Diplomat jrNS* to send an ARP packet to the Remote Server Address. The time it takes to receive a reply is displayed in microseconds but is only accurate to ten microseconds. If no reply is forthcoming and no error messages have appeared (see later) then either the IP address was wrong or the network has failed between the *Diplomat jrNS* and the destination.

Depending on the amount of knowledge that is available about the topology of the network other IP addresses can be used to test various segments of a longer path.

If a reply is received this shows that at least the low level drivers at the Remote Host are functioning. To test that there is an IP stack loaded on the remote host and that it is alive type ‘E’. This sends an ICMP echo request (ping) to the Remote Host and if there is a reply the *Diplomat jrNS* will display a transit time.

The BOOTP option remains undefined.

Typing 'R' causes the *Diplomat jrNS* to broadcast a RARP request. If a RARP server exists on the network and if it responds with an IP address for the *Diplomat jrNS*, then that address will be used as the *Diplomat jrNS's* IP address.

Error Messages

There are three types of messages, those originating from error conditions detected by the *Diplomat jrNS* itself and those that are reported by the network and are translated into a readable text for the user. Internal error messages are bracketed by three asterisks and remote messages by three plusses. Simple informative messages are not bracketed.

The display of local and informative messages and the display of remote messages is controlled by switch BEXREP in Configuration Byte B.

The following table lists all messages which should explain themselves.

Informative Messages
Coax Cable detected
UTP Cable detected
Establishing TCP Connection - Please Wait
Local Error Messages * message*****
No Destination IP on local Subnet
Trying to Contact IP Address
Cannot Initiate in Server Mode
Failed to Open a link
Run out of buffers
Could not send Option (Telnet)
No TCP Session Established
Failed to Send Data
Failed OPEN
Remote Error Messages +++message+++
Network Unreachable
Host Unreachable
Protocol Unreachable
Port Unreachable
Fragmentation Needed
Source Route Failed
Destination Unreachable

Note: There is no defined method of delivering these text messages in Model CDF/ DCF. Both BEXPEP bits should be set equal to zero.

Synchronous Port A

The table below shows the pin connections to this port connector. This port is normally connected to a modem or other synchronous peripheral and is a male 25 pin D-type configured as a serial synchronous DTE.

PIN NO.	**RS232 SIGNAL**	
1	G	Protective Ground connects to chassis and power supply ground
2	TX	Diplomat Transmits serial synchronous data on this line
3	RX	Diplomat Receives serial synchronous data on this line
4	RTS	Diplomat asserts RTS when it wants to transmit data
5	CTS	Must be high to enable Diplomat to Transmit
7	SG	Signal Ground is connected to power supply ground
8	DCD	Must be held high before data is received by the Diplomat
15	TXC	Transmit clock internal/external determined by links
17	RXC	Receive clock internal/external determined by links
20	DTR	Held high by Diplomat when powered up
24	EXC	Internal clock always available

The use of screened cable is recommended with the screen being connected to the metal shell of the connector at both ends. It should also be verified that the screen is connected to the pin 1 conductor at least at one end of the cable. On installation it is good practice to verify that the case of the Diplomat is at the same nominal potential as the rack in which it is mounted.

The mating connector must be fixed to the mounting pillars provided to avoid accidental removal and to provide ground continuity for the screen. The above measures are important to minimize susceptibility to electrical noise and radiated RF interference.

The DTR signal from the Diplomat has a source impedance of 1Kohm to +5VDC. This means that it can drive one standard RS232/V28 input (>3Kohm) with a safety margin of 0.75V over the 3V minimum. If it is used to drive two inputs there is zero margin and if the load presented to the pin is less than 1.5Kohm the state of the pin will be indeterminate. It is recommended therefore that all the Port A outputs on the Diplomat jrNS be used to drive a single RS232/V28 input only.

Network Interface Port B

Optional 10 Base-2 Coax Connector

10Base-T UTP Connector

Green LED

Yellow LED

Flashes for every packet transmitted or received

Illuminates when the link is enabled (UTP only)

10Base-T Connection

Pin 1	Tx+
Pin 2	Tx-
Pin 3	Rx+
Pin 6	Rx-

Product Details

Product name	Diplomat™ jr
Model	jrNS
Serial Number	
Configuration Code	
Firmware Reference	JRNS-CDF Rev. 1.02
Issue Date	30/08/07
Special features/notes	
Default IP Address	. . .

Technical Data

Weight & Dimensions

Height x width x depth	25mm x 175mm x 110mm
Weight	350g

Electrical Requirements

Power to Diplomat jr	8±1 Volt DC 500mA
Power to adaptor	220-240 VAC 50Hz or 90-120VAC 60Hz

Operating Environment

Temperature	0-50˚C
Humidity	0-90% non-condensing

External connectors

Power	3.2mm jack socket positive tip
Network	10Base-T UTP or (optionally) 10Base-2 Coax
Serial Port	25 pin male D-type RS232

External Indicators

Red LED	indicating +8Volts present
Greed LED	indicating UTP link enabled
Yellow LED	indicating packet transmitted or received

Configuration

Menu driven, remotely

Data Rates

Synchronous up to 38.4 Kbps
Network 10Mbps Half Duplex