

Lucidata Diplomat jr
Model JRN-ASV
Network Asynchronous Server

Lucidata House
Selwyn Close
Great Shelford
CAMBRIDGE CB2 5HA
England

tel: +44(0)1223 846100
fax: +44(0)1223 846200
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 846200
email: info@lucidata.com**

Diplomat[®] is a registered trademark of Lucidata Limited.
© Lucidata Limited 1991-2001

No part of this publication may be reproduced, transmitted, transcribed, stored in any retrieval system or translated into any human or computer language without the prior written permission of Lucidata Limited.

Diplomat jrN-ASV User Guide Issue Number 2 (04/98)

Revision Details

Issue	First Published	Revised	Pages
2	4/98	11/98	3,5,9,10,11,14-22,24
		04/99	2,3,29
		07/99	2,13
		04/00	2,3,7,12,13,15,17-19,25,29
		07/00	2,3,4,13,18,19,20,29
		08/00	2,3,28,29,30
		09/00	2,4
		03/01	2,3,9,10,13,18-32

Introduction	Page	5
Getting Started Quickly	Page	6
Port A	Page	6
Port B	Page	6
Power	Page	6
Configuration	Page	9
Port A Hardware Options	Page	9
Data Rate	Page	9
DTR	Page	9
Configuration Cable	Page	9
Control Characters	Page	10
Main Menu	Page	10
Configuration Bytes	Page	11
Remote Configuration	Page	18
Operation	Page	20
Normal Operation	Page	20
UDP Client/Server	Page	21
TCP Client/Server	Page	21
Closing TCP Sessions	Page	22
Status Reporting	Page	22
Telnet Port Operation	Page	22
Controlling the Flow of Data	Page	23
Transparent Mode	Page	24
LED Indicators	Page	24
Trouble Shooting and Error Messages	Page	25
Basic Error Conditions	Page	25
Statistics Display	Page	26
Network Trouble Shooting	Page	27
Network Monitor	Page	28
Error Messages	Page	29
Technical Specification	Page	30
Asynchronous Port A	Page	30
Network Interface Port B	Page	31
Product Details	Page	32
Technical Data	Page	32

Warranty



FM 13348 BS EN ISO 9001:1994

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 via any of the addresses given on page ii. 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 ii.

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 jrN is one of a family of simple connectivity solutions built around Lucidata's popular Diplomat jr product. The jrN 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.

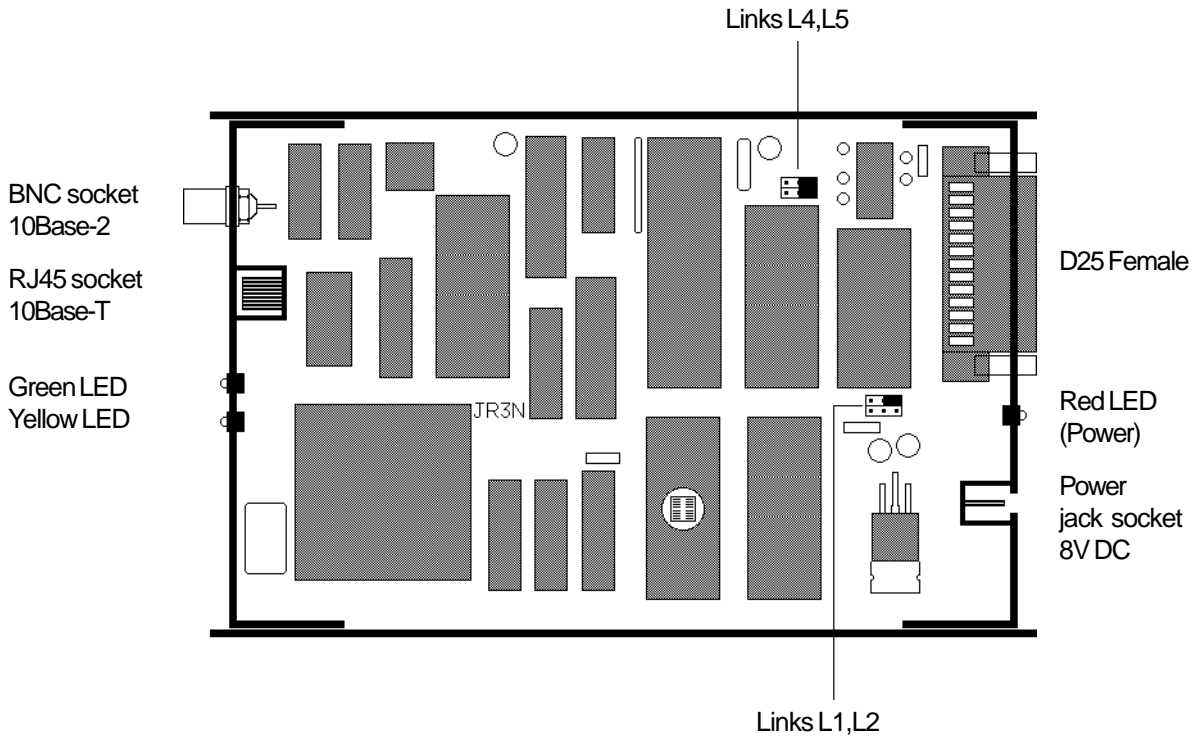
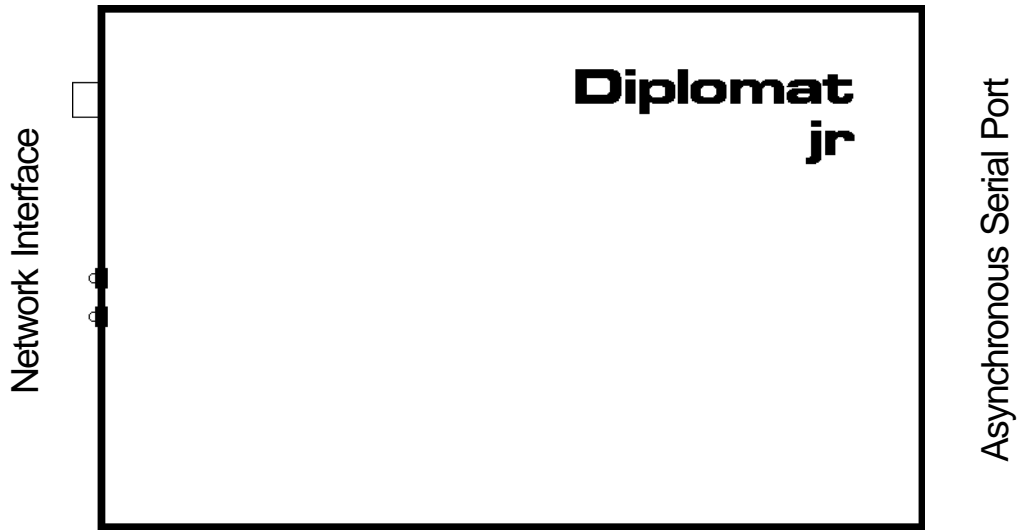
The model jrN runs the jrN-ASV firmware as standard and supports interconnectivity between Ethernet and simple asynchronous serial devices over an RS232 interface. It also has brothers and sisters that offer RS422 (jrNV), synchronous (jrNS) and parallel (jrNP) interfaces which run a variety of communications protocols

This manual is structured to require the minimum of reading to effectively operate the *Diplomat jrN*. 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 jrN* then Chapter 4, Operation, is where we tell of all the things that the jrN 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 jrN* 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



When you hold the *Diplomat jrN* 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 Asynchronous DCE and any cable that was designed to connect a terminal type device to a modem using a 25 pin male D type connector will be suitable to connect your 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.

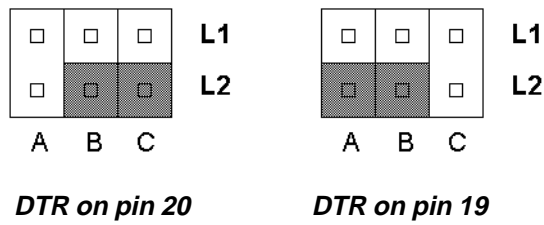
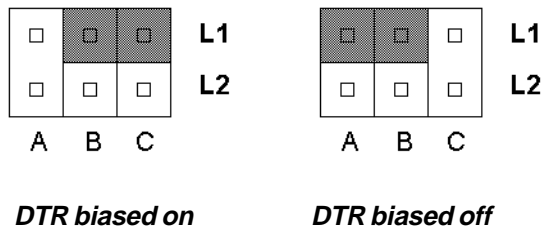
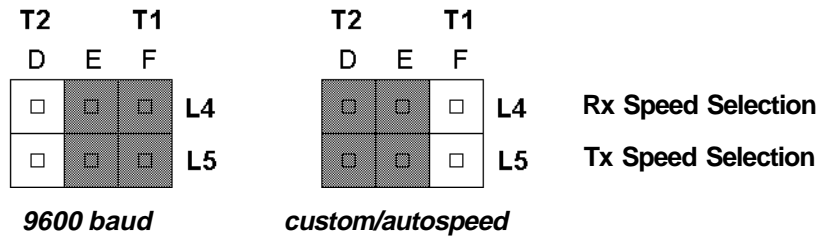
Power

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 jrN 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 jrN 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 sending a single character to Port A will cause the jrN to attempt to make a connection to the remote server defined in its configuration.



Changing Data Rate and DTR Signal on Links inside the Diplomat jrN

Port A Hardware Options

Most configuration of the jrN is performed by interacting with the Menu screens presented through Port A but there are two sets of hardware jumpers that determine some properties of Port A. Reference should be made to the diagram on pages 6 and 8 when making any changes to the jumpers.

Data Rate

The data rate of Port A is selected by choosing the position of the jumpers on links L4 and L5. The default speeds are 9600 and 19200bps but the clocks T1 and T2 may be configured differently by setting the Configuration Byte D (See later section). The receive speed is selected by link L4 and the transmit speed by link L5. If a jumper is on the right most two pins (E-F) of a link then 9600 bps is selected. If a jumper is on the left most two pins (D-E) of a link then the custom speed is selected (by default 19200 bps).

Character Format

The default character format used by Port A is eight data bits, no parity bit and one stop bit (8N1). This can be configured differently by setting the Configuration Byte C. (See later section)

DTR

The state of the internal DTR signal on Port A will always determine whether Port A will be able to transmit and it is not necessary for an external connection to be made to pin 20. Some printers provide a READY signal on pin 19. If external control is required, and it usually is, a jumper between the right most pins (B-C) of link L2 will select pin 20 for DTR control. A jumper between the left most pins (A-B) of link L2 will select pin 19 for DTR control.

In addition the selected pin may be gently biased towards either ON or OFF by jumpering link L1. Some devices will still hold DTR high enough to appear ON even when they are powered off so by gently biasing the pin OFF when the device is powered down DTR is correctly sensed. Equally it may be desirable to keep Port A enabled all the time in which case no links would be used on L2 and the DTR level would be determined solely by L1. If a jumper is on the right most two pins (B-C) of L1, DTR is biased ON and if the jumper is on the left most two pins (A-B) of L1, DTR is biased OFF.

The DTR signal can have significant effects depending on other configuration options which are described later so it is important to have it properly configured. The default factory setting is DTR biased ON and connected to pin 20 of Port A.

Configuration Cable

If *Transparent Mode* has been selected the jrN will ignore all control characters. (see next paragraph). This would make it difficult to re-configure the unit so the Diplomat looks for a link between Pin 8 (or 6) and Pin 20. If it detects a link it will interpret control characters for 15 seconds before entering *Transparent Mode*. It is important that link L2 is between pins B and C and that nothing is connected to pin 20 that will prevent it being driven high and low by pin 8.

Note: The link must NOT be present for normal operation so a specially labelled Configuration Cable should be made for the purpose.

Configuration

Control Characters

Throughout this manual reference is made to ASCII control characters that have special significance. They are identified variously as a key combination eg CTRL/P, standard mnemonic eg DLE or by the ASCII value. To make for easier reading, all referenced control characters are defined here.

Mnemonic	Key Combination	Decimal Value
DLE	CTRL/P	16
ENQ	CTRL/E	5
DC2	CTRL/R	18
DC1(XON)	CTRL/Q	17
DC3(XOFF)	CTRL/S	19
CR	RETURN	13
SUB	CTRL/Z	26
NUL	CTRL/@	0
BEL	CTRL/G	7

Main Menu

All other configuration is done by invoking the Main Menu. Under most circumstances, the exceptions will be described later, typing CTRL/P (that is holding down the CTRL key and typing P) will cause the Main Menu to be displayed. CTRL/P is ASCII value 16 decimal. The interaction with the menu system might be considered rather old fashioned in this Windows World but there is a good reason why it was designed this way. Basically it makes it easy to configure the jrN from a program running on any computer by simply sending a string of significant characters to Port A without waiting for any response. In fact if the computer first sends a DC3 character (ASCII value 19 decimal) then no responses will be returned to the computer at all. When the *Diplomat* has finished interpreting the commands it will perform a soft start and clear the flow control blocking flag.

```
Lucidata Diplomat C 1995-2001
Model JRN-ASV rev 3.35:1048

Terminal Profile is <Local Port>
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 (CAUTION)
<D> Set Data Rate Configuration Byte (CAUTION)
<S> Enter Statistics Menu
<N> Enter Network Control Menu
<R> Reset Diplomat Softly

Select <>
```

Configuration Bytes

The current generation of *Diplomat jrS* 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 jrN 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 jrN* there are four sets of Silicon Switches associated with four Configuration Bytes.

Configuration Byte A controls the major characteristics of Port A and Configuration Port B controls the major characteristics of Port B. Changing Configuration Bytes C and D should only be attempted after careful consideration of the consequences as once altered Port A will expect data coming in to comply with the newly specified speed and character format. Having said that Configuration Byte D used in conjunction with Clock Links L4 and L5 can provide very versatile speed options including split speed.

Selecting A, B, C or D 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

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

Bit	Name of Switch	Description
0	BHWPNG	[0] - Ignore ICMP ECHO notifications. [1] - If an ICMP ECHO message is received on Port B and Configuration Byte B BEXREP=1 then output a BEL character on Port A. If BHWDIS=1 then also drop pin 6(DSR) and pin 8(DCD) on Port A for 1 second. A TTL logic level 1 is also asserted on pin 12 of Port A for 1 second.
1	BHWDIS	[0] - Disable Hardware Disconnect [1] - Enable Hardware Disconnect. If DTR drops then any OPEN TCP session is CLOSED. If an OPEN TCP session is CLOSED from the remote side then drop pin 6(DSR) and pin 8(DCD) on Port A for 1 second. A TTL logic level 1 is also asserted on pin 12 of Port A for 1 second.
2	BCNTR	[0] - Only action defined Control Characters, DLE, ENQ, DC2 during the first 15 seconds after power up, if configuration cable detected, otherwise treat data stream completely transparently. [1] - Always action defined Control Characters
3	BXON	[0] - Treat DC1 and DC3 characters as data. Note: If the connected device issues either of these characters and BECHO=1 then a feedback loop is established and the network could be flooded with packets of DC1/DC3 characters. [1] - Use DC1 and DC3 characters for local XON/XOFF flow control
4	BCRLF	[0] - Do not append a LF character to echoed CR characters [1] - Append LF character to each CR character echoed
5	BECHO	[0] - Do not Echo input characters [1] - Echo all input characters
6	BSCHAR	[0] - Only send data to Network on a terminator character or input buffer full condition [1] - Offer each character input for immediate transmission over the Network. Characters may naturally accumulate and there is no guarantee that a TCP segment will only contain a single character.
7	BEXREP	[0] - Do not output Error Message Texts to Port A [1] - Output human readable Error Message Texts to Port A

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

Bit	Name of Switch	Description
0	BPEER	[0] - Enforce Client/Server relationship in TCP [1] - Allow Client/Client sessions in TCP
1	BTCPU	[0] - Use the TCP protocol [1] - Use the UDP protocol
2	BSEXY	[0] - New Session(SYN) attempts must come from the same Host as the current TCP session and Resets (RST) must come from the same Host AND Port as the current TCP session. [1] - New Session (SYN) attempts can come from any Host but Resets (RST) must come from the same Host as the current TCP session [0] - Insist on 'Interactive' behaviour when in UDP Server mode. ie Do not accept a new Client until a response sent to old Client. [1] - Accept packets from anyone as long as they are addressed to us in UDP Server mode.
3	BCLIENT	[0] - Client initiates a TCP session on DTR high [1] - Client initiates a TCP session on Data appearing
4	BSERV	[0] - Behave as a Client Device i.e. initiate sessions [1] - Behave as a Server Device i.e. listen and wait for contact
5	BSEND	[0] - Disable Auto Send [1] - Enable automatic sending of buffered data to the network after 50mS has expired since last character input on Port A
6	BMONIT	[0] - Normal Operation, respond to packets addressed to unit [1] - Produce a formatted dump on Port A of the first 64 bytes of every packet detected on the Network. The first 4 bytes are internal status bytes and not Network data.
7	BEXREP	[0] - Do not forward Network Error Message Texts to Port A [1] - Output local translation of Network Errors in human readable form and pass on ICMP Echoes.

Note: If the Firewall feature is enabled the bit BSEXY has no effect.

Configuration

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

Data Bits	Parity Bits	Stop Bits	Bit 3	Bit 2	Bit 1	Bit 0
8	N	2	0	0	0	0
8	N	1	0	0	0	1
8	E	1	0	0	1	0
8	O	1	0	0	1	1
7	N	2	0	1	0	0
7	E	2	0	1	0	1
7	O	2	0	1	1	0
7	M	2	0	1	1	1
7	S	2	1	0	0	0
7	E	1	1	0	0	1
7	O	1	1	0	1	0
7	M	1	1	0	1	1
7	S	1	1	1	0	0

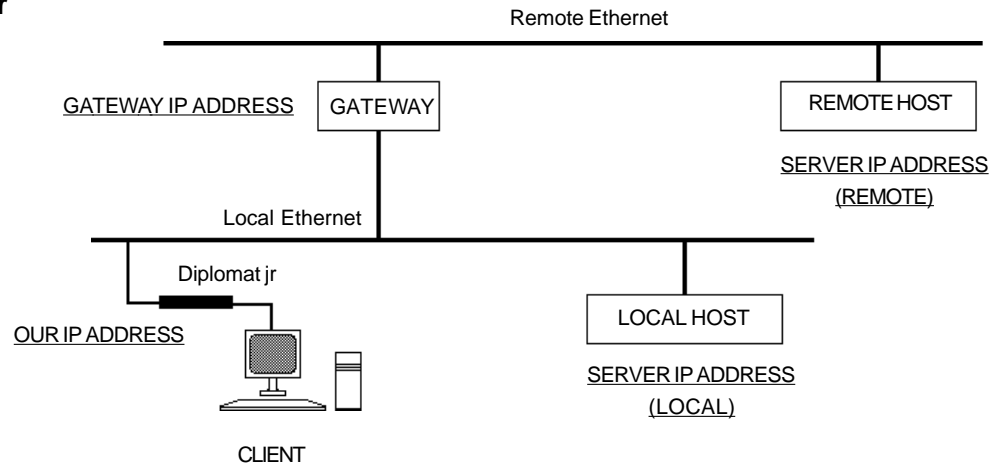
Where the Parity Bit Codes mean None, Even, Odd, Mark, Space

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
 Clock 2 (T2) is controlled by bits 4 to 7

Speed (bps)	Bit 3 or 7	Bit 2 or 6	Bit 1 or 5	Bit 0 or 4
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
19200	1	0	0	1
19200	1	0	1	0
19200	1	0	1	1
19200	1	1	0	0
19200	1	1	0	1
19200	1	1	1	0
19200	1	1	1	1

Network Parameter Configuration



Now that the basic configuration of the *Diplomat jrN* 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 - FFFFFFF0
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.

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 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 'P' 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 jrN*.

The Port value 12346 should not be used as it invokes a special filter.

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
```

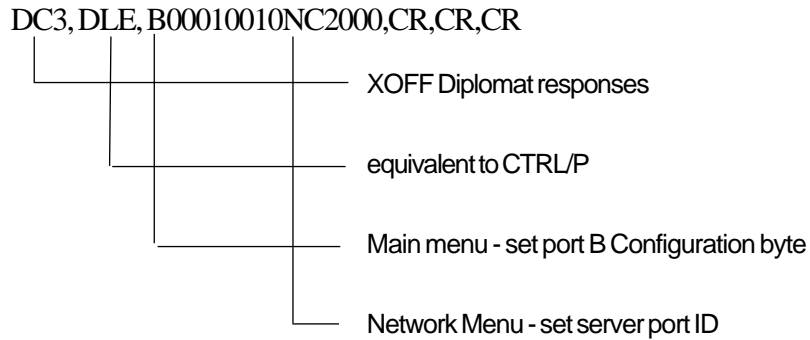
```
<A> Add an entry, <D> Delete an entry, <E> Edit an entry
```

```
<CR> Returns to Previous Menu
```

The feature only has effect if the *Diplomat jrN* 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 type CTRL/P, N to see the Network Control Screen and then return to the active session by typing Return twice, once to get back to the Main Menu and once to get back to the session.

As we mentioned earlier, the design of the menu system enables automatic configuration changes under the control of a local computer system very simply. For example suppose that the configuration change required was to make the *Diplomat jrN* a UDP Server on port 2000 just for the day. The string that would be sent from the computer (ignoring commas) would be:



Remote Configuration

The *Diplomat jrN* can be configured remotely using a program or another *Diplomat jrN*. This becomes essential in the case of the jrN(S) and jrN(P) variants which do not have an asynchronous RS232 port. It will be easier to describe the process from the point of view of the *Diplomat jrN* which is being used to do the remote configuration. We will call this the Host jrN.

The Host jrN should first be configured as a UDP Client with full Error Reporting using the following values for configuration byte 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 Server IP address and the Remote Service 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".

For all intents and purposes the Local Terminal is connected to the remote jrN. All menu driving commands work in the usual way with the exception that no control characters are sent to the remote jrN. Make very sure of the changes that are made because they will be remembered by the remote jrN when the Main Menu is left and if the IP address has been changed erroneously you may not be able to contact the jrN again.

The remote jrN 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 Host jrN Main Menu. The remote jrN 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 jrN was doing at the time. If no configuration values are changed because you only viewed the statistics or got the remote jrN to Ping its Server then that will not force a restart and any existing TCP session will be preserved.

Normal Operation

As long as the *Diplomat jrN* 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 jrN* to change its IP address to the value contained in the RARP reply.

When the *Diplomat jrN* 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 jrN* 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 jrN* 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 jrN* does not issue any automatic ARP requests.

If switches BHPNG of Configuration byte A and BEXREP of Configuration byte B are both set then whenever the *Diplomat jrN* receives an ICMP echo request (PING) from a remote host a BEL character is transmitted from Port A. If in addition switch BHWDIS is set then the DSR (pin 6) and DCD (pin 8) signals on Port A will be dropped for 1 second. A TTL logic level 1 is also asserted on pin 12 of Port A for 1 second.

The *Diplomat jrN* 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 jrN* 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 jrN* cannot send any data over the network until it has received a packet containing a Source Port address for it to use as a return address.

If a UDP packet arrives from another host before the *Diplomat jrN* has sent a reply to the previous host, the new packet will be ignored unless switch BSEXY of Configuration Byte B is set to 1. If BSEXY is set to 1 the new packet's Source IP and Port addresses become the new Destination addresses for any *Diplomat jrN* reply.

When the *Diplomat jrN* 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.

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 jrN* 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. The status of the connection can be monitored through Port A.(see later) Should a new attempt to initiate a TCP session be detected from the same IP address then the existing session is considered broken and the *Diplomat jrN* 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 jrN* terminates the current session and returns to the waiting state.

These rules are relaxed if switch BSEXY in Configuration Byte B is set to 1. If BSEXY is set to 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 BSEXY is set to 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.

The switch BSEXY has no effect if the Firewall feature is enabled as this alone will determine who is able to talk to the *Diplomat jrN*. New session requests or Reset commands from any Firewall qualified host/ports will be accepted and actioned as described above. The *Diplomat jrN* cannot initiate a TCP session when in Server mode.

When configured as a TCP Client the *Diplomat jrN* will attempt to initiate a TCP session with the Remote Server on the declared Server Port as soon as the first character is received on Port A. The very first character is consumed in the process. 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.

If switch BHWDIS in Configuration Byte A is set then the signals on DSR (pin 6) and DCD (pin 8) on Port A will be dropped for 1 second when the session is closed from the remote host.

The *Diplomat jrN* will respond to a CTRL/R character entered at Port A by closing down any open TCP session provided switch BCNTR in Configuration Byte A is set. In any event if switch BHWDIS in Configuration Byte A is set then dropping the DTR signal (pin 20) on Port A will have the same effect and close down the session.

Status Reporting

The *Diplomat jrN* will respond to a CTRL/E character entered at Port A by issuing the message:

Status = Number

Number will normally have the values of 0 meaning there are no open TCP sessions or 128 meaning there is an open TCP session. Various other values are possible if the *Diplomat jrN* has been unable to finish initiating or terminating a TCP session. The values will be made up of a combination of the following bit values.

Value	Meaning
0	TCP session fully CLOSED
1	Close Initiated by Remote
2	Local Close sent in response to remote
4	Close Initiated from Local
16	Server Waiting State
32	Session Initiated from Local
64	Session Initiated from Remote
128	TCP session fully OPEN

The TCP service guarantees correct delivery of the data streams in both directions while a TCP session is OPEN. Any Status other than 0 or 128 can be cleared by entering a single CTRL/R.

Telnet Port Operation

If a value of 23 is used for the Port Address the *Diplomat jrN* will perform basic Telnet functions. The main function is to insert a NUL character after any CR found in the input data stream before sending to the network. The *Diplomat jrN* will also recognise and reply to any Telnet options appended to the IP header.

Controlling the flow of data

The *Diplomat jrN* has been designed to be flexible so that it can be used in situations as yet unknown. It is therefore not practical to say how it should be set up because we do not know precisely what it will be used for. Therefore we will describe a simple application and then describe how various features are invoked and how they impact on the *Diplomat jrN*'s behaviour.

A simple requirement might be to gain access to a character based application running on a remote mainframe host using a terminal emulation on a PC or even a dumb terminal. The things that are important here are that the user probably wants to see what he has been typing and the device he is using wants to exercise flow control on data coming from the network. He also wants each new line he types to start on a new line and wants to be able to access the menu.

It should be clear from Chapter 3 that Configuration Byte A should have switches BCNTR, BXON, BCRLF, and BECHO set and all the rest clear. If he also wants to receive all locally generated messages he needs to set BEXREP also. All the data he enters from the terminal is stored up until he hits RETURN or CTRL/Z. The difference between these two characters is that the RETURN key terminates the data with a CR character which is sent with the data to the remote host while the CTRL/Z only serves as a terminator and causes all the data up to but not including itself to be sent.

It could happen that the remote host wants to see each character as it is typed and to decide whether to echo the character itself or not. Typically passwords are 'hidden' in this way. If this is the case BECHO and BCRLF would be cleared and BSCHAR must be set so that characters are sent immediately to the remote host as they are typed in.

If instead of a human user we connect a machine of some kind; computer, cash register, process controller etc. the requirements change significantly. We almost certainly do not want characters echoed back so we need to clear BECHO and BCRLF. It is quite likely that the data will be binary or quasi-binary which has additional implications.

If the use of CR and CTRL/Z is consistent with the data format used then the data can still be blocked in the interests of network efficiency. If not switch BSCHAR must be set so that data is sent as it comes in and no special meaning is associated with CR or CTRL/Z.

The third way to cause data to be sent over the network is to enable Automatic Sending by setting switch BSEND in Configuration Byte B. With Automatic Sending if any data remains in the input buffer after 50msecs has elapsed since the last character was input, the buffer data is automatically sent.

Most important is to make sure the setting of switch BXON correctly reflects the way DC1 and DC3 characters are handled by the system. If switch BXON is cleared and the connected device uses XON/XOFF flow control then any DC1 or DC3 characters sent to the *Diplomat jrN* intended for flow control will be sent to the remote host which is probably not what was intended. Similarly if the system is treating DC1 and DC3 as just another binary value then we do not want the *Diplomat jrN* stripping them out and stopping and starting the data stream.

Transparent Mode

If it is required to send full eight bit binary data that is incompatible with the *Diplomat jrN*'s use of CTRL/P, CTRL/R and CTRL/E then switch BCNTR must be clear. This means that the menu can never be accessed once the *Diplomat jrN* has been configured in this mode without the use of the special *Configuration Cable*, described earlier.

The other implication of switch BCNTR being clear is that the only way for the *Diplomat jrN* to close a TCP session is by making use of the DTR signal on Port A so switch BHWDIS must be set.

LED Indicators

The *Diplomat jrN* 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 jrN* 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 Menu up in response to CTRL/P immediately after power-up

- i) Check position of links L4 and L5 and set-up of terminal
- ii) Check position of links L1 and L2 and that pin 19/20 is high
- iii) Check cable to Port A, data should be arriving at unit on pin 2.
- iv) Check if configuration link was required

Return unit and adaptor to supplier (see page 4)

Trouble Shooting and Error Messages

Statistics Display

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
Count of Bad Asynch Inputs -               0
Asynch.DTR - Hi

<CR> Returns to Previous Menu
```

Any significant counts in the Hardware Exceptions, Aborted Transmissions or Bad Asynch inputs 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

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 - FFFFFFF0
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 jrN* is trying to work with is actually reachable. It is best to have all the low level switches set so that all error messages are displayed and so that BEL characters can be sent to the terminal to give an audible 'ping'.

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 jrN* 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 jrN* and the destination.

Trouble Shooting and Error Messages

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 jrN* will display a transit time and produce a beep at the terminal. If another host is trying to test the reachability of the *Diplomat jrN* by sending an ICMP echo request the *Diplomat jrN* will produce a beep at the terminal when it receives the request.

The BOOTP option remains undefined.

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

Network Monitor

There is a low level monitor feature that can be useful under some circumstances. If the switch BMONIT is set in Configuration Byte B then the first 60 bytes of every packet detected on the network is displayed in hex dump format on the terminal. The true packet starts at the fifth byte as the first four bytes are internal status and pointer information relevant to the packet. On a busy network the asynchronous port can be easily saturated.

Error Messages

There are three types of messages, those originating from error conditions detected by the *Diplomat jrN* 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 is controlled by switch BEXREP in Configuration Byte A and the display of remote messages 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

Technical Specification

Asynchronous Port A

The table below shows the pin connections to this port connector. This port is normally connected to a terminal or other asynchronous peripheral and is a female 25 pin D-type configured as a serial asynchronous DCE.

PINNO. **RS232 SIGNAL**

1	G	Protective Ground connects to chassis and power supply ground
2	TX	Asynchronous Transmitted Data going into the Diplomat
3	RX	Asynchronous Received Data from the Diplomat
4	RTS	Connected to pin 5
5	CTS	Connected to pin 4
6	DSR	Data Set Ready held high if Diplomat ready to receive
7	SG	Common signal return is connected to power supply ground
8	DCD	Data Carrier Detect held high if Diplomat ready to receive
12	O/I	TTL level is inversion of pin 6 and 8
19	RDY	see links L1 and L2
20	DTR	see links L1 and L2

The Diplomat jrN Model V is supplied with an RS422 interface. In this case the female 25 pin D-Type is configured as follows:

PINNO. **RS422 SIGNAL**

1	Shield	Connects to chassis and power supply ground
2	T(A)	Asynchronous Transmitted Data going into the Diplomat
3	C(A)	Control Signal going into Diplomat
4	R(A)	Received Data from Diplomat
5	I(A)	Indication Signal from Diplomat
8	SG	Signal Ground
14	T(B)	Transmitted Data going into Diplomat
15	C(B)	Control Signal going into Diplomat
16	R(B)	Received Data from Diplomat
17	I(B)	Indication Signal from Diplomat

The Control Signal is used by the Diplomat jrNV in place of the DTR signal used by the jrN. The Indication Signal is generated by the Diplomat jrNV in place of the DSR and DCD signals generated by the Diplomat jrN.

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

10Base-T Connection

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

Illuminates when the link is enabled (UTP only)

Product Details

Product Details

Product name	Diplomat™ jr
Model	jrN
Serial Number	
Configuration Code	
Firmware Reference	JRN-ASV Rev. 3.36
Issue Date	26/03/01
Special features/notes	

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 Volts AC 50-60 Hz

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 female D-type RS232 or (optionally) RS422

External Indicators

Red LED indicating +8Volts present

Green LED indicating UTP link enabled

Yellow LED indicating packet transmitted or received

Configuration

Menu driven, either locally or remotely

Data Rates

Asynchronous up to 19.2Kbps

Network 10Mbps Half Duplex