

JETSTREAM 4000, 8500 LANSTREAM 2000

Configuration Guide

5500024-17

Copyright statement

This document must not be reproduced in any way whatsoever, either printed or electronically, without the consent of:

Perle Systems Limited ,
60 Renfrew Drive

Markham, ON
Canada
L3R 0E1

Perle reserves the right to make changes without further notice, to any products to improve reliability, function or design.

Specialix, the Specialix logo, JETSTREAM, JETSTREAM4000, JETSTREAM8500 and LANSTREAM2000 are trademarks of Perle Systems Limited.

Microsoft, Windows 95, Windows 95, Windows NT Windows 2000 and Internet Explorer are trademarks of Microsoft Corporation.

Netscape is a trademark of Netscape Communications Corporation.

Solaris is a registered trademark of Sun Microsystems, Inc. in the USA and other countries.

Perle Systems Limited, Tuesday, May 13, 2003.

FCC Note The Specialix JETSTREAM 4000, JETSTREAM 8500 and LANSTREAM 2000 products have been found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions in this Guide, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his/her own expense.

EN 55022: 1998, Class A, Note

WARNING This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.



Caution: the JETSTREAM 4000, JETSTREAM 8500 and LANSTREAM 2000 are approved for commercial use only.

About this Guide

This guide describes how to configure the JETSTREAM 4000, 8500 or LANSTREAM 2000, using a text-based terminal or terminal emulator. It is intended for a network systems administrator, familiar with UNIX operating systems and Ethernet TCP/IP networks and, possibly, the RADIUS protocol.

Please note this Guide describes menu functions in the text-based menuing system (also named 'Full Screen Menus' or 'fsm'), thus:

SLIP line 1			
Local IP	[]	Remote IP	[]
Address		address	
Subnet Mask	[]		[]
Max TX unit	[]	Suppress ICMP	[]
Interactive	[]	VJ_comp	[]
Priority			
TX parameters	[]		

However, all configuration parameters described in this Guide are the same parameters seen in JETset, the web-based graphical configuration utility.

Some chapters deal separately with the terminal server and remote access functions. The appendixes are common to both functions.

Note

1. There is a separate JETSTREAM 4000, 8500, LANSTREAM 2000, Installation Guide.
2. For those familiar with the product range there is a Quick Start Guide; this is a small folding leaflet which is packed with the product.

Revision history

Date	Part number	Description
November 1997	5500024-10	Initial release of manual.
September 1998	5500024-11	Minor update to manual content.
February 1999	5500024-12	Software Release Note 5600036-11 included in manual.
September 1999	5500024-13	Details of OEM mode included in manual.
March 2000	5500024-14	Minor update to set parallel CLI command section.
October 2000	5500024-15	Update of manual to include new Perle logos, revision and contact information.
November 2001	5500024-16	Update of manual to include details of selecting AUI interface type and to document the addition of 10/100Base-T functionality.
May 2003	5500024-17	Update manual to include the details on LAN speed configuration.

Contents

About this Guide	5
Revision history	7
Contents	9
Chapter 1 Configuring a Line: Terminal Server Connections	15
Contents	15
Introduction	15
Telnet/Rlogin into the unit	16
Starting Telnet/Rlogin from the unit	17
Login direct to host	20
Login for Sessions	24
Copy settings to other lines	26
Reset Serial Line to Default	27
Save to non-volatile memory	27
Reverse Telnet connection	28
Chapter 2 Host Control of Ports and Printing	31
Introduction	31
Remote Printing using LPD	33
Remote Printing Using RCP	38
Remote Printing Using Host-Based Print Handling Software	42
External host: Dialin Modem Connections	43
Local host: Dialout Modem Connections	44
Host to host: bidirectional Modem Connections	44
Modem and Printer Handling Using MTSD	45
Copy settings to other lines	53
Reset Serial Line to Default	53
Reset Parallel Line to Default	54
Save to non-volatile memory	54
Chapter 3 Configuring a Line: - SLIP and PPP Connections	57
Introduction	57
Chapter contents	57
Overview	57
SLIP, PPP and RADIUS	59

Use SLIP or PPP?	62
Setting Up the Line	63
Configuring SLIP	65
Configuring PPP	67
Modems: summary of configurable features	74
Copy settings to other lines	74
Reset Serial Line to Default	74
Save to non-volatile memory	75
Chapter 4 Configuring a User	77
Contents	77
Introduction	77
When you need User accounts	78
User accounts and RADIUS	78
Add a User Account	81
Configure a User Account	82
User Levels	87
Running Sessions	87
Change a User's Password	88
Delete a User Account	89
Language support	89
Save to non-volatile memory	92
Chapter 5 System Administration & BOOTP	95
Introduction	95
Becoming Admin User	95
Upgrading System Software	96
Downloading Terminal Definitions	96
TFTP configuration	98
BOOTP	99
DHCP Configuration and Operation	109
Rebooting	110
Resetting to Factory Defaults	110
Remote Configuration	111
Security	111
Off-line Configuration	111
Save Configuration to a file	113
Lost Password	114
Chapter 6 SNMP	115
Introduction	115

Chapter contents	115
Overview	115
Configuring SNMP support	115
Summary of Objects in the JS8500 Private MIB	116
JS8500 Private MIB Definitions	117
Network Management	120
Chapter 7 Guide for Operators on Terminals	123
Introduction	123
Chapter contents	123
Logging in	123
Modes of Operation	124
Changing your Password	127
Changing your Terminal Setup	127
Changing your User Environment	128
Logging Out	128
Running Sessions	128
Starting a Session	129
Predefining Sessions	130
Starting a Predefined Session	131
Hot-key Commands	131
Resuming a Session	132
Killing a Session	132
Chapter 8 Examples of SLIP / PPP connections	135
Introduction	135
Chapter contents	135
Setting up a Remote User (with PPP)	136
Joining together two networks	143
Chapter 9 The CLI commands	149
Introduction	149
add community	151
add DNS	151
add gateway	152
add host	153
add modem	153
add radius	154
add trap	155
add user	155
add WINS	156

admin	156
debug	157
delete ARP	157
delete community	158
delete DNS	158
delete gateway	159
delete host	159
delete modem	160
delete radius	160
delete trap	161
delete user	161
delete WINS	162
heap	162
help	162
kill line	163
kill parallel	163
kill session	164
logout	164
netload	165
netsave	166
ping	167
reboot	168
reset factory	169
reset line	170
reset parallel	170
reset user	171
restart	172
resume	172
rlogin	173
save	173
screen	175
set contact	175
set date	176
set ethernet interface RJ45	177
set ethernet interface AUI	177
set ethernet speed	177
set gateway	179
set host	179
set line	181
set location	183
set parallel	184
set ppp line	185

set radius	186
set server	187
set slip line	190
set telnet	190
set time	193
set user	193
show ARP	196
show date	197
show gateways	198
show hardware	199
show hosts	199
show interfaces	200
show line	201
show modems	203
show parallel	204
show ppp line	205
show radius	207
show routes	208
show server	209
show sessions	210
show slip line	211
show snmp	212
show telnet	213
show time	214
show user	214
start	215
telnet	216
version	217
Appendix A Summary of Line Service Types	219
Appendix B Troubleshooting	223
Introduction	223
Contents	223
General communication matters	224
BOOTP/DHCP problems	224
Callback problems	225
Host problems	225
Hub problems (LANSTREAM only)	226
JETset problems	227
Problems with JETstart	227
Language problems	227
Login problems	227
Modem problems	229

MTSD problems	229
PPP problems.....	229
Printing problems.....	230
Saving to FLASH memory	230
Telnet/Rlogin problems	231
Problems with terminals	231
Problems with Framed Routing.....	232
Emergency Recovery.....	233
Appendix C SLIP and PPP overview	235
Introduction	235
SLIP.....	235
PPP.....	237
Appendix D References	241
Appendix E ASCII and HEX conversion tables	243
Introduction	243
ASCII to Decimal and Hex Conversion Chart.....	243
Binary to Hex Conversion Chart.....	244
Appendix F Contacting Perle	247
Making a technical support query.....	248
Who to contact.....	248
Information needed when making a query	249
Making a support query via the Perle web page	250
Repair procedure.....	251
Website RMA (Return Material Authorisation) Form	251
Feedback about this manual.....	252
Perle support centres worldwide.....	253
Index	255

Chapter 1 Configuring a Line: Terminal Server Connections

Contents

- [Introduction](#)
- [Telnet/Rlogin into the unit](#)
- [Starting Telnet/Rlogin from the unit](#)
- [Login direct to host](#)
- [Login for Sessions](#)
- [Copy settings to other lines](#)
- [Reset Serial Line to Default](#)
- [Save to non-volatile memory](#)
- [Reverse Telnet connection](#)

For remote access connections using SLIP and PPP see Chapter 3 Configuring a Line: - SLIP and PPP Connections.

Note For an overview of all line types (including those discussed in other chapters in this manual) see Appendix A (Summary of Line Service Types).

Introduction

A terminal server connection allows a user or users to send and receive characters to/from a local host(s). This type of connection is useful for users who need to access an account on a host running TCP/IP. Those users will most likely be using a dumb terminal.

You will see that the JETSTREAM 4000, 8500 or LANSTREAM 2000 is called the 'unit'. The use of the word 'unit' avoids frequent repetition of the product name.

Tip The unit is primarily for remote access connections (using SLIP or PPP). For terminal server type connections we recommend that you change the default settings for the user parameters 'idle timer' and 'session timer'. By changing the settings you will tune the unit for terminal server connections. See Section *Configure a User Account*, sub-sections 'idle timer' and 'session timer'.

Telnet/Rlogin into the unit

You can telnet/rlogin into the unit from another computer on the local network (see Figure 1). For example you may wish to configure the unit and you prefer to do this across a network.

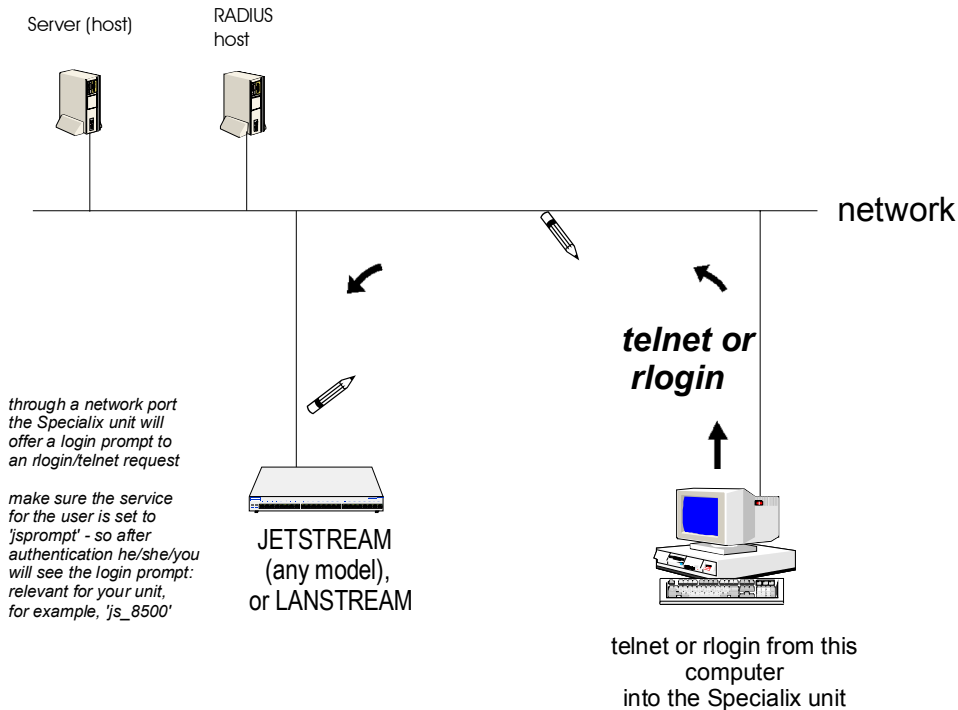
To set up the unit so that you (as system administrator) can telnet or rlogin into it, configure the following:

- use your own account (username 'admin') and use/set user 'service' to 'jsprompt'.

To set up the unit so that a user can telnet or rlogin into it, configure the following:

- configure a user account and use/set user 'service' to 'jsprompt'.

Figure 1 Telnet/rlogin into the unit.



Notes on telnet/rlogin into the unit:

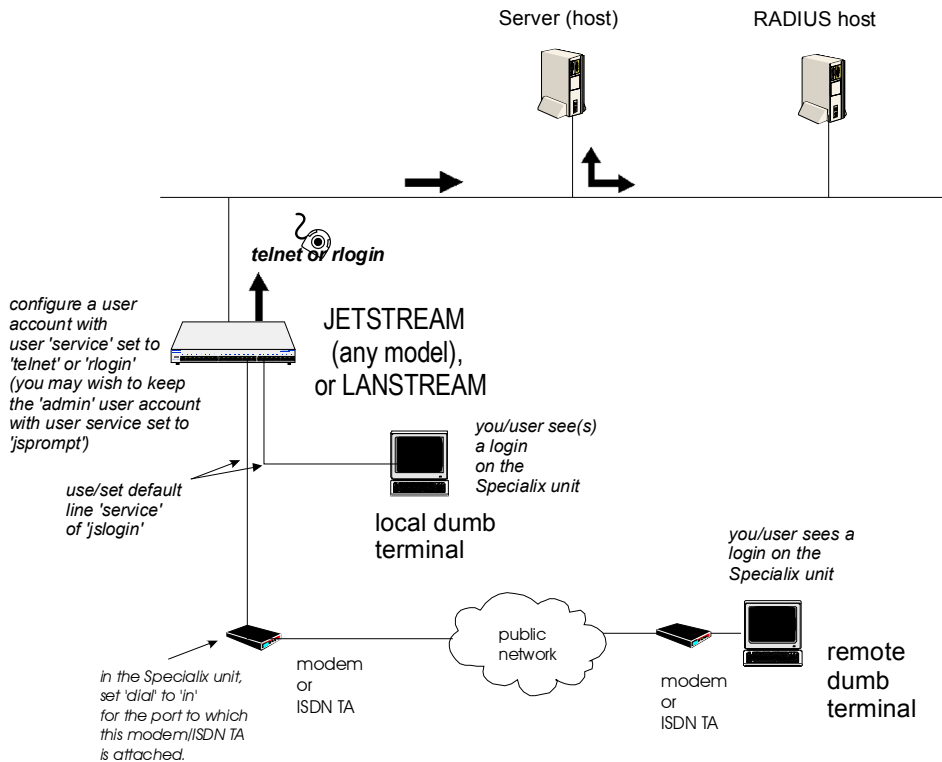
1. You cannot configure the line parameters when you/the user are accessing the unit via one of its network ports on a telnet/rlogin connection. Parameters such as 'terminal type' are negotiated automatically between the computer and the unit.
2. only two users can telnet into a unit simultaneously
3. there are no timeouts; the session is open permanently, until you reboot or logout.

For information on RADIUS authentication when telnet/rlogin are used, see Telnet/Rlogin and RADIUS on page 20.

Starting Telnet/Rlogin from the unit

You or a user may need to telnet/rlogin from the unit to another device. The method is to login to the unit and then be presented with the telnet/rlogin service from the unit. (As the system administrator you may wish to be presented with the command line prompt and then to manually start a telnet/rlogin session to the other device). We envisage that you will be connected to the unit via a serial line directly (or with a modem) into one of its front-mounted serial ports; see Figure 2.

Figure 2 Starting Telnet/Rlogin from the unit



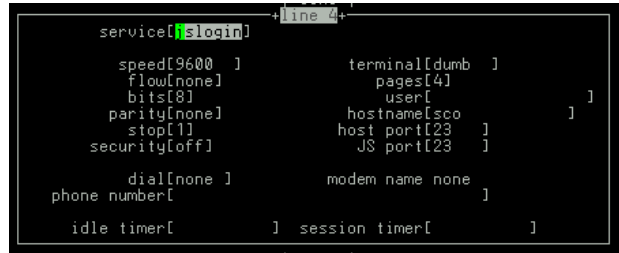
As the system administrator (username 'admin') you may wish to keep your own user 'service' as 'jsprompt' (after authentication you are presented with the unit command line prompt).

For a user you may prefer to configure the line so that he/she by-passes the unit and logs in directly on a host; if so, see Login direct to host on page 20. If your user needs to connect to several hosts - possibly simultaneously - you may prefer to configure sessions for him/her; if so see Login for Sessions on page 24.

To set up this type of connection configure the following:

cli syntax
set line,
show line

1. Select 'Line Settings' from the Line Configuration menu, then select a particular line; e.g line 4. The following form will be displayed (default values):



```

service[jslogin]
speed[9600 ]      terminal[dumb ]
flow[none]        pages[4]
bits[8]           user[ ]
parity[none]      hostname[sco ]
stop[1]           host port[23 ]
security[off]     JS port[23 ]

dial[none ]      modem name none ]
phone number[

idle timer[ ]    session timer[ ]
  
```

2. Go to the following fields:

Service use/select the default line service of 'jslogin' login.

Speed, Flow, Bits, Parity and Stop

change from the default line configuration of 9600 baud, software flow control, 8 data bits, no parity and 1 stop bit.

Terminal check the type of terminal which you will attach to this particular line, then select one of Wyse 60, ANSI or VT100. You can download additional terminal definitions, when you can use term1, term2 or term3; refer to Downloading Terminal Definitions on page 96.

User this field allows you to define the name of the user of the line. On rlogin connections (direct rlogin and silent rlogin), this field is mandatory because the user name is always passed to the UNIX host under the rlogin protocol. (On line service types 'jslogin', this is an option, enabling you to dedicate the line to a specific user. This user won't be prompted for their user name, just their password.) To select a user you must first add that user to the user table in the unit. See Section Add a User Account.

Hostname use the spacebar to cycle through the available hosts. Select the host that you want the user to log into. By default, the hostname field displays 'none' because there are no hosts in the host table; after you have entered hosts in the host table the 'hostname' field defaults to the first host in the host table.

Host Port by default, the Host (TCP) Port is set to 23 (telnet). In most cases you can use 23 for both telnet and rlogin.

Dial if your user is remote and he/she will be dialling in via modems/ISDN TAs set this field to 'in'

3. Press <return> to exit; if you do not wish to save your changes press the <escape> key.
4. If your user is remote and will be dialling in via modems/ISDN TAs (more actions):

cli syntax: Go to the Line Configuration Menu:
add modem

a). select 'Modems' then select 'Add Modem'. Enter the name of the modem/ISDN TA attached to the unit. You can enter a maximum of twenty names, each with nineteen alphanumeric characters.

b). from 'Modems' select 'Change Modem'. Select your modem/ISDN TA name. Enter the initialisation string; see your modem/ISDN TA documentation.

Press <return> to exit; if you do not wish to save your changes press the <escape> key.

set line

Go back to the 'Line Settings' menu. Select your line. When the line parameters form appears go the field 'modem name'. Press 'L' (upper or lower case) or the spacebar. Choose the modem name which you entered at Step 4.

5. Press <return> to exit; if you do not wish to save your changes press the <escape> key.

idle timer (*you may wish to change the default value*) enter a period in seconds for which the idle timer will run. Use this timer to close a connection because of user inactivity. When the idle timer expires the unit will end the connection. The default value is 300 seconds, meaning the idle timer will expire 300 seconds after the last user activity. The maximum value is 4294967 seconds (equal to 49 days, approximately). A value of 0 (zero) means the idle timer will not expire so the connection is open permanently.

Caution

In addition to this line idle timer, you can configure an idle timer associated with a particular user. The user idle timer will override the line idle timer. See Section Configure a User Account.

session timer (*you may wish to change the default value*) enter a period in seconds for which the session timer will run. Use this timer to forcibly close a user's session (connection). When the session timer expires the unit will end the connection. The default value is 0 (zero), meaning that the session timer will not expire (the session is open permanently, or until the user logs out). The maximum value is 4294967 seconds (equal to 49 days, approximately).

Caution

In addition to this line session timer, you can configure a session timer associated with a particular user. The user session timer will override the line session timer. See Section Configure a User Account.

6. Ignore the other fields in this form. Press <return> to exit; if you do not wish to save your changes press the <escape> key.

You can copy the settings for this line to all other lines; refer to Copy settings to other lines on page 26.

You can reset this line to default (an option as you exit this form); refer to Reset Serial Line to Default on page 27

Note *changes to a line will take effect the next time the user logs in. The exception is the 'terminal' parameter where the change will take effect immediately.*

Tip *You may want to save your configuration changes permanently; see Section Save to non-volatile memory.*

For information on RADIUS authentication when telnet/rlogin are used, see Telnet/Rlogin and RADIUS on page 20.

You may now need to configure a user account. Refer to Section Add a User Account.

Telnet/Rlogin and RADIUS

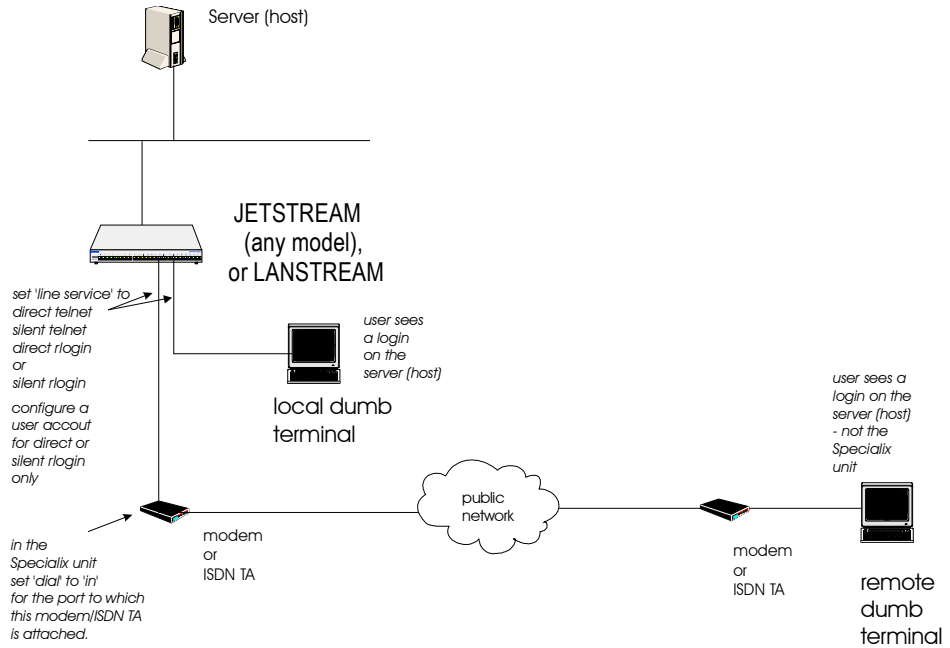
This section explains about RADIUS authentication of users when they are using the telnet/rlogin programs with the unit.

1. When you telnet/rlogin into the unit from another computer across a network (as shown in Figure 1):
 - all users will always be authenticated by the unit - the 'authentication' setting is ignored.
2. When you/a user connect(s) to the unit with the intention of starting a telnet/rlogin connection to another device (as shown in Figure 2):
 - the user with username 'admin' will always be authenticated by the unit - the 'authentication' setting is ignored
 - any other user can be authenticated by the unit or by RADIUS - the 'authentication' setting is observed

Login direct to host

To setup users so that they are presented with a login directly on a host machine, bypassing the JETSTREAM 4000, 8500 or LANSTREAM 2000 (the 'unit'), you will need to set up 'direct' or 'silent' connections. This scenario is shown at Figure 3.

Figure 3 Connections directly on a host (bypassing the unit)



Authentication of the user is done by the host, using its own table or RADIUS information.

cli syntax:
set line,
show line

1. Select 'Line Settings' from the Line Configuration menu, then select a particular line; e.g line 2. The following form will be displayed (example settings):

```

service[air rlg] +line 2+
  speed[9600 ]      terminal[wyse60]
  flow[none]       pages[4]
  bits[8]          user[ ]
  parity[none]     hostname[sco ]
  stop[1]          host port[23 ]
  security[off]    JS port[23 ]

  dial[none ]      modem name none ]
  phone number[ ]

  idle timer[1800 ] session timer[28800 ]
  
```

2. Go to the following fields:

Service use the spacebar to select one from direct telnet, direct rlogin, silent telnet, silent rlogin (or press ‘L’ (upper or lower case) to display a list). ‘Direct’ connections are temporarily established on the host, ‘silent’ connections are permanently established. Silent connections will consume system resources even when not in use.

For a fuller explanation of direct and silent see Section Definitions of Direct and Silent.

For an explanation of the telnet and rlogin see Section Merits of Telnet and Rlogin

By default, the line service is JS (JETSTREAM) login

Speed, Flow, Bits, Parity and Stop

change from the default line configuration of 9600 baud, software flow control, 8 data bits, no parity and 1 stop bit.

Terminal check the type of terminal which you will attach to this particular line, then select one of Wyse 60, ANSI or VT100. You can download additional terminal definitions, when you can use term1, term2 or term3; refer to Downloading Terminal Definitions on page 96.

User this field allows you to define the name of the user of the line. On rlogin connections (direct rlogin and silent rlogin), this field is mandatory because the user name is always passed to the UNIX host under the rlogin protocol. (On line service types ‘jslogin’, this is an option, enabling you to dedicate the line to a specific user. This user won’t be prompted for their user name, just their password.) To select a user you must first add that user to the user table in the unit. See Section Add a User Account.

Hostname use the spacebar to cycle through the available hosts. Select the host that you want the user to log into. By default, the hostname field displays ‘none’ because there are no hosts in the host table; after you have entered hosts in the host table the ‘hostname’ field defaults to the first host in the host table.

Host Port By default, the Host (TCP) Port is set to 23 (telnet). In most cases you can use 23 for both telnet and rlogin.

Dial If your user is remote and will be dialling in via modems/ISDN TAs, set the Dial field to ‘in’.

Note that with the direct and silent line services, the unit performs no modem/ISDN TA configuration or initialisation. You must configure the modem/ISDN TA before connecting it to the unit. Modems must be set to AUTO-ANSWER mode. In this form ignore the ‘modem name’ and ‘phone number’ fields.

idle timer *(you may wish to change the default value)* enter a period in seconds for which the idle timer will run. Use this timer to close a connection because of user inactivity. When the idle timer expires the unit will end the connection. The default value is 300 seconds, meaning the idle timer will expire 300 seconds after the last activity. The maximum value is 4294967 seconds (equal to 49 days, approximately). A value of 0 (zero) means the idle timer will not expire so the connection is open permanently.

Caution

In addition to this line idle timer, you can configure an idle timer associated with a particular user. The user idle timer will override the line idle timer. See Section Configure a User Account.

session timer *(you may wish to change the default value)* enter a period in seconds for which the session timer will run. Use this timer to forcibly close a user's session (connection). When the session timer expires the unit will end the connection. The default value is 0 (zero), meaning that the session timer will not expire (the session is open permanently, or until the user logs out). The maximum value is 4294967 seconds (equal to 49 days, approximately).

Caution

In addition to this line session timer, you can configure a session timer associated with a particular user. The user session timer will override the line session timer. See Section Configure a User Account.

3. Ignore the other fields in this form. Press <return> to exit; if you do not wish to save your changes press the <escape> key.

You can copy the settings for this line to all other lines; refer to Copy settings to other lines on page 26.

You can reset this line to default (an option as you exit this form); refer to Reset Serial Line to Default on page 27

Note *changes to a line will take effect the next time the user logs in. The exception is the 'terminal' parameter where the change will take effect immediately.*

Tip *You may want to save your configuration changes permanently; see Section Save to non-volatile memory.*

You may now need to configure user accounts. Refer to Section Add a User Account.

Definitions of Direct and Silent

Direct connections bypass the unit enabling the user to log straight into a specific host. A direct connection is recommended where a user logging in to the unit is not required. It is also recommended where multiple sessions are not a requirement. The message 'Press return to continue' is displayed on the user's screen. The user must hit a key to display the host login prompt. The message is redisplayed on logout.

Silent connections are the same as direct connections except that they are permanently established. The host login prompt is displayed on the screen. Logging out redisplay this prompt. Silent connections, unlike direct connections, however, make permanent use of pseudo tty resources and therefore consume host resources even when not in use.

Merits of Telnet and Rlogin

You can select the telnet or rlogin protocol for direct and silent connections. If unsure which to use, consider the following:

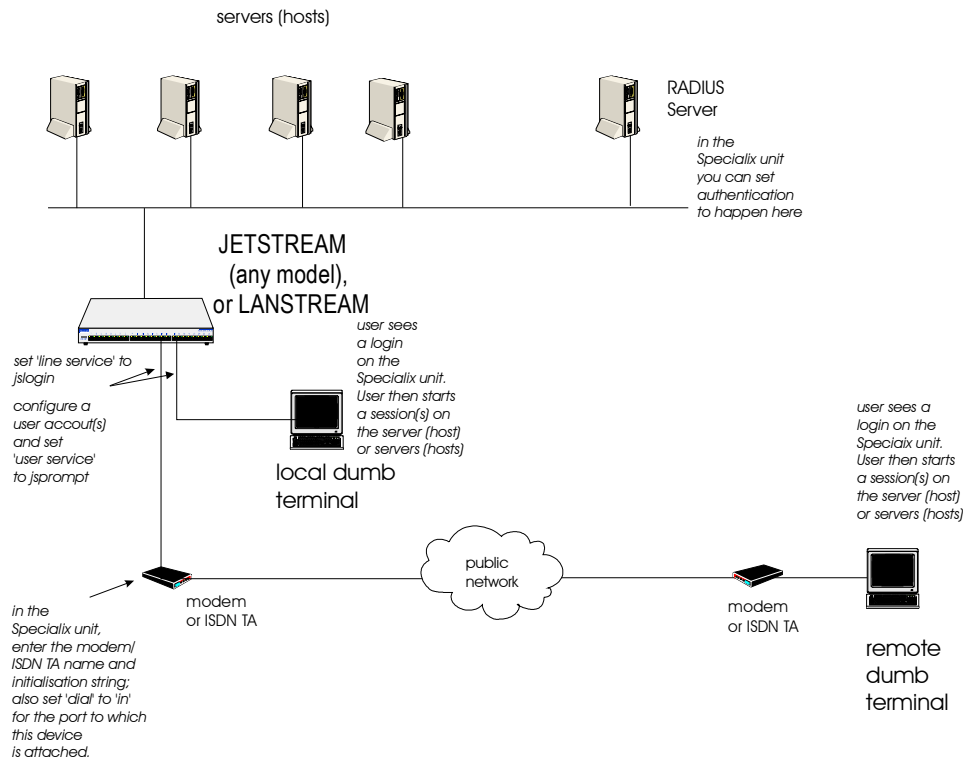
- **Telnet** can be used to access both UNIX and non-UNIX hosts; **rlogin** can normally only be used with UNIX hosts.
- Telnet provides more options for connecting to hosts, but rlogin uses fewer system resources.

- Rlogin passes your user name and a terminal type to the host. On some older versions of SCO UNIX, however, these may not be passed. Failure to pass the terminal type results in your TERM variable being set to 'unknown' upon login.

Login for Sessions

You can configure lines so that users login to the JETSTREAM 4000, 8500 or LANSTREAM 2000 (the 'unit') and then start a session or multiple sessions - via telnet or rlogin - on a host or hosts local to the unit. The session(s) are setup inside the unit; see Figure 4.

Figure 4 sessions on one or more servers (hosts), set up within the unit.



Authentication of the user is done firstly by JETSTREAM 4000, 8500 or LANSTREAM 2000, then by each host into which the user logs.

**cli syntax:
set line,
show line**

To configure a port so that users login to the unit and start session(s) on a local host(s) do the following:

1. Select 'Line Settings' from the Line Configuration menu, then select a particular line; e.g line 4. The following form will be displayed (example settings):

```

service[jslogin]
speed[9600 ]      terminal[dumb ]
flow[none]       pages[4]
bits[8]          user[
parity[none]     hostname[sco ]
stop[1]         host port[23 ]
security[off]    JS port[23 ]

dial[none ]      modem name none ]
phone number[

idle timer[      ] session timer[      ]

```

2. Go to the following fields:

Service select 'jslogin'.

Speed, Flow, Bits, Parity and Stop

change, if necessary, from the default line configuration of 9600 baud, software flow control, 8 data bits, no parity and 1 stop bit.

Terminal check the type of terminal which you will attach to this particular line, then select one of Wyse 60, ANSI or VT100. You can download additional terminal definitions, when you can use term1, term2 or term3; refer to Downloading Terminal Definitions on page 96.

Pages This is the number of video pages supported by the terminal attached to the line. If you don't specify the correct number of pages, you may experience problems with page displays when switching between sessions. The documentation supplied with your terminal should tell you how many pages it supports.

Host Port By default, the Host (TCP) Port is set to 23 (telnet). In most cases you can use 23 for both telnet and rlogin.

Dial If your user is remote and will be dialling in via modems/ISDN TAs, set the Dial field to 'in'.

idle timer *(change if you have any terminal server type connection)* enter a period in seconds for which the idle timer will run. Use this timer to close a connection because of user inactivity. When the idle timer expires the unit will end the connection. The default value is 300 seconds, meaning the idle timer will expire 300 seconds after the last activity. The maximum value is 4294967 seconds (equal to 49 days, approximately). A value of 0 (zero) means the idle timer will not expire so the connection is open permanently.

Caution

In addition to this line idle timer, you can configure an idle timer associated with a particular user. The user idle timer will override the line idle timer. See Section Configure a User Account.

session timer enter a period in seconds for which the session timer will run. Use this timer to forcibly close a user's session (connection). When the session timer expires the unit will end the connection. The default value is 0 (zero), meaning that the session timer will not expire (the session is open permanently, or until the user logs out). The maximum value is 4294967 seconds (equal to 49 days, approximately).

Caution

In addition to this line session timer, you can configure a session timer associated with a particular user. The user session timer will override the line session timer. See Section Configure a User Account.

3. Ignore the other fields in this form.
4. Press <return> to exit; if you do not wish to save your changes press the <escape> key.

Note *changes to a line will take effect the next time the user logs in. The exception is the 'terminal' parameter where the change will take effect immediately.*

**cli syntax:
add modem**

5. If your user is remote and will be dialling into the unit via modems/ISDN Terminal Adaptors, do the following:
 - a). from the Line Configuration Menu, select 'Add Modem'. Enter the name of the modem/ISDN TA attached to the unit. You can enter a maximum of twenty names, each with nineteen alphanumeric characters.
 - b). from the Line Configuration Menu, select 'Change Modem'. Select your modem name. Enter the initialisation string; see your modem/ISDN TA documentation.
6. Press <return> to exit; if you do not wish to save your changes press the <escape> key.

set line

7. Go back to the 'Line Settings' menu. Select your line. When the line parameters form appears go the field 'modem name'. Press 'L' (upper or lower case) or the spacebar. Choose the modem name which you entered at Step 5.
8. Press <return> to exit; if you do not wish to save your changes press the <escape> key.

You can copy the settings for this line to all other lines; refer to Copy settings to other lines on page 26.

You can reset this line to default (an option as you exit this form); refer to Reset Serial Line to Default on page 27

Tip *You may want to save your all your configuration changes permanently; see Section Save to non-volatile memory.*

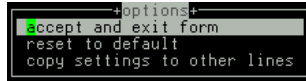
You will now need to configure user accounts and to setup user sessions. Go to Chapter 4 (Configuring a User).

Copy settings to other lines

This feature enables you to change a parameter (e.g. line service) and then copy that change to some or all lines. It is available in the Line Settings form (under the Line Configuration Menu).

- Select a line and make the required change (e.g. change line speed from 9600 baud to 57600 baud).
- Press <return> to display the 'Options' form:

- Select 'copy settings to other lines'. Another form will be displayed which allows you to select other lines.

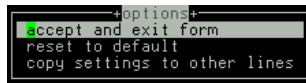


Reset Serial Line to Default

cli syntax:
reset line

This feature enables you to reset the serial line which you are configuring to the default settings. It is available in the Line Settings form (under the Line Configuration Menu). This line will be reset to 9600 baud, 8 data bits, 1 stop bit, no parity and software flow control; the line type will become 'jslogin', the TCP Port '23', the idle timer '300' seconds and the hostname the first host entered in the host table.

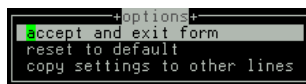
- Press <return> to display the 'Options' form:



- Select 'reset to default'.

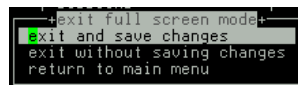
Save to non-volatile memory

When you exit a menu screen (form) after making changes, you will be presented with the options form:



If you choose to 'accept and exit form' your changes will be retained in RAM (volatile memory).

To save your changes permanently go to the Main Menu and select 'command line mode'; you will be presented with a form:



Choose 'exit and save changes'. All the changes made since last entering the menus will be saved to FLASH (permanent, non-volatile) memory. The writing to FLASH will take a few seconds and during this time the unit will not respond to user input.

WARNING

Do NOT turn off the power while the unit is writing to FLASH memory.

cli syntax:
screen

You should now be at the unit's command line prompt. To return the text menus type: `screen`

Saving to a file

netsave

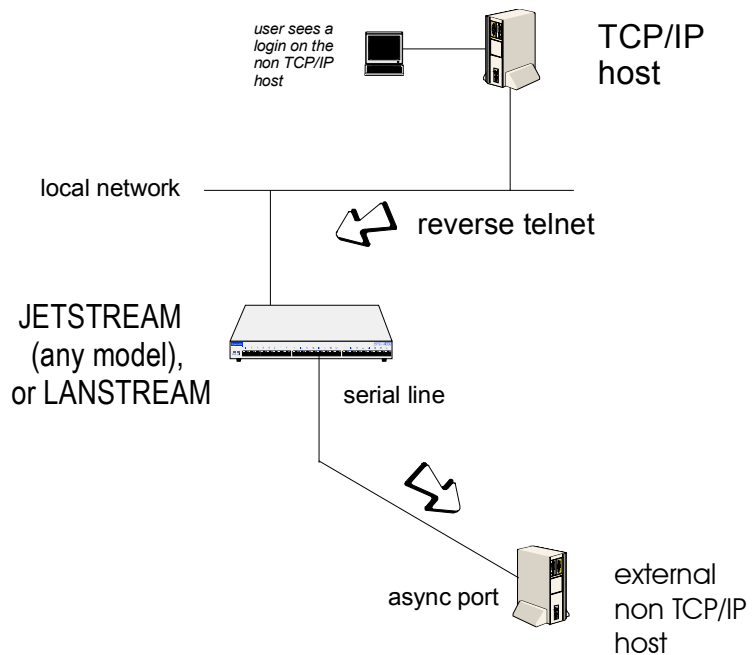
You can also save your configuration information to a file on a host. This can only be done in the cli; see Section `netsave`.

Reverse Telnet connection

cli syntax:
set line

A reverse telnet connection enables a TCP/IP host on the local network to establish a login connection via a JETSTREAM 4000, 8500 or LANSTREAM 2000 (the 'unit') port on a non-TCP/IP machine external to the network; (see Figure 5). The unit will effectively be transparent.

Figure 5A Typical Reverse Telnet Configuration



To set up a reverse telnet connection, follow these steps:

1. Select Line Settings from the Line Configuration menu then select the line that you want to configure.
2. Set the 'Service' field to rev tel.
3. Assign a TCP port number to the unit port using the 'JS Port' field. This TCP port number will be used by any host wanting to access the unit port. If you select a TCP port being used by another process, a connection will not be established (using a number in the range 900-1023 should be safe).
4. To set up a hunt group, assign the same TCP port number to more than one reverse telnet port. The unit will use the first free port it finds in the group.
5. Do *not* configure the idle and session timers; these timers have no effect on reverse telnet connections.
6. The 'Hostname' and 'Host Port' fields may contain default or last-used values, but these will be ignored.
7. The 'Security' field may be configured to 'on' or 'off' (default). The security field option authenticates the user before allowing access to the line when enabled.
8. The line should now be configured similar to the following:

```

service[rev tel]
speed[9600 ] terminal[dumb ]
flow[none] pages[4]
bits[8] user[ ]
parity[none] hostname[sco ]
stop[] host port[23 ]
security[off] JS port[900 ]

dial[none ] modem name none
phone number[ ]

idle timer[ ] session timer[ ]

```

9. Press <return> to exit; if you do not wish to save your changes press the <escape> key.
10. You can copy the settings for this line to all other lines; refer to Copy settings to other lines on page 26.
11. If you want to configure all lines with the same parameters, refer to Reset Serial Line to Default on page 27.
12. On the non-TCP/IP machine, configure the line for the required purpose (e.g. login).
13. To access the external machine from a TCP/IP host, use the following command:

```
telnet name js_port
```

Where:

name is the hostname of the JETSTREAM 4000, 8500 or LANSTREAM 2000 unit.

js_port is the TCP port number assigned to the JETSTREAM 4000, 8500 or LANSTREAM 2000 port.

Chapter 2 Host Control of Ports and Printing

Introduction

This chapter tells you about advanced uses of the JETSTREAM 4000, 8500 or LANSTREAM 2000 (the 'unit') with printers and modems. A TCP/IP host is required to run a program or utility to control the unit's ports, so that the ports appear local to the host. The program or utility could be LDP, RCP, a custom program or our own utility called MTSD. We discuss MTSD in detail.

This chapter is divided into the following sections:

- *Introduction*
- *Remote Printing using LPD*
- *Remote Printing Using RCP*
- *Remote Printing Using Host-Based Print Handling Software*
- *External host: Dialin Modem Connections*
- *Local host: Dialout Modem Connections*
- *Host to host: bidirectional Modem Connections*
- *Modem and Printer Handling Using MTSD*
- *Copy settings to other lines*
- *Reset Serial Line to Default*
- *Save to non-volatile memory*

Note For an overview of all line types (including those discussed in other chapters in this guide) see [Appendix A \(Summary of Line Service Types\)](#).

Figure 6 Using the unit to share a modem/ISDN TA pool

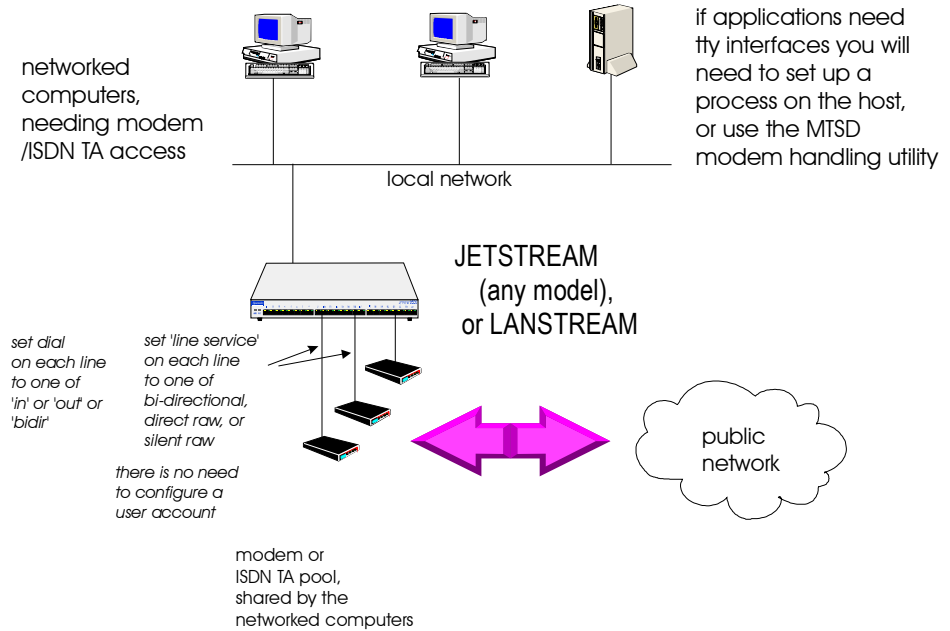
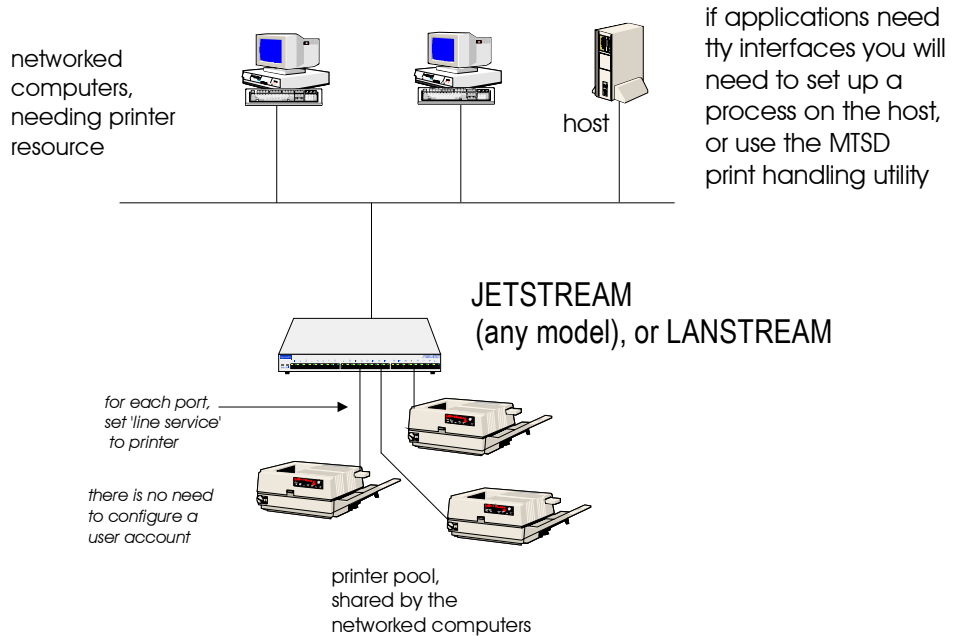


Figure 7 Using the unit to share a printer pool



Remote Printing using LPD

Printers connected to JETSTREAM 4000, 8500 or LANSTREAM 2000 (*the 'unit'*) serial and parallel ports can be accessed by other TCP/IP hosts on the network using the LPD protocol; see [Figure 7](#).

This section consists of:

[LPD Configuration step-by-step](#)

[LPD Configuration Example](#)

LPD Configuration step-by-step

In your unit you can use the following line service types:

printer

For serial port configuration see below; for parallel port configuration see the section [parallel port](#) on the next page.

serial port

1. Select 'Line Port Settings' from the Line Configuration menu. Select the *serial* line to which your printer is attached; (in the cli use the command `set line`). Set the `service` field to one of the line service types listed above. Look at the example line below (serial line default values shown):

```

service[printer]
speed[9600 ]      terminal[dumb ]
flow[none]        pages[4]
bits[8]           user[ ]
parity[none]      hostname[sco ]
stop[1]           host port[23 ]
security[off]     JS port[23 ]

dial[none ]      modem name none
phone number[ ]

idle timer[ ]    session timer[ ]

```

2. Configure the speed, flow, bits, parity and stop parameters.

It is *not* necessary to set the hostname `terminal`, `pages`, `user`, `dial`, `modem`, `name` and `phone number` fields; these are ignored by the unit for this line service (printer). The `JS port`, `idle` and `session timer` fields may contain default or last-used values, but these also will be ignored by the unit.

Tip To reset the line to default, press <Enter> from any point in the form and accept the 'reset to default' option; see [Reset Serial Line to Default on page 53](#).

3. Accept and exit the form. If you wish, copy the line settings to other lines (an additional option as you exit the form; see [Copy settings to other lines on page 53](#)).

Tip You may want to save your configuration changes permanently; see [Section Save to non-volatile memory](#).

4. Go now to the section [configuration continued.....](#)

parallel port

JS4000

1. Select 'Parallel Port Settings' from the Line Configuration menu. Select the *parallel* line to which your printer is attached; (in the cli use the command `set parallel`). Ensure the `service` field is set to `printer`. Look at the example line below (printer line service type default values shown):

```

parallel 1

service      [printer]

hostname     [none ]      host port     [23 ]
JS port      [23 ]

```

2. Configure the `hostname` parameter; it will default to the first host you have entered in the unit's host table.

You do not need to set the `host port` and `JS port` fields.

Tip To reset the line to default, press `<Enter>` from any point in the form and accept the 'reset to default' option; see [Reset Parallel Line to Default on page 54](#).

3. Accept and exit the form. If you wish, copy the line settings to other lines (an additional option as you exit the form; see [Copy settings to other lines on page 53](#)).

Tip You may want to save your configuration changes permanently; see [Section Save to non-volatile memory](#).

configuration continued.....

4. Kill the line: from the Main Menu go to the Line Configuration menu and select 'kill line' (in the cli use the command `kill line`).
5. You now need to configure LPD on the network host.

If your network host is running SCO Open Server v5 follow the LPD Configuration Example in [Remote Printing using LPD on page 33](#).

If you network host is running other operating systems, for example Windows NT, you will need to know:

the name/ip address of the Perle device

the printer queue name

For further information see [paragraph 2](#) in LPD Configuration Example on page 35 below.

6. To execute the `lpd` print job see [Executing an lpd job on page 37](#).

LPD Configuration Example

In this example the network host is running SCO Open Server v5.

1. On the network host, with root permission, type `scoadmin` and then make the following selections:
 - 1.1 From the Printer Menu, select Add Printer.
 - 1.2 Select Add TCP/IP printer.
 - 1.3 You should be presented with the following dialog box:

free format name →

Perle device name →

Queue name →

Add Printer Connected via TCP/IP

Name [jetstream1] Protocol Type [lpd(BSD)]

Make/model

HP LaserJet 5P/5MP (PCL)

HP LaserJet 5P/5MP (Postscript)

HP LaserJet 5Si/5Si MX (PCL)

Printer Connection Type < > On < * > On
 Network Remote Server ←

Remote System:
 |stimpv | [select] select option on remote server' (that is, on the Perle device)

Remote printer:
 |raw_2 |

[OK] [Cancel] [Help]

- 1.4 Using the example above, complete the fields in the form. For details on selections/input in the Remote System and Remote printer fields see the information in the paragraph below.
2. Check the following configuration information:

information you will need	field name in SCO Open Server 5	your action	example syntax and comments
name or ip address of Perle device	Remote System	enter/select the name or ip address of the Perle device. If you select the name, this is the JETSTREAM 4000, 8500 or LANSTREAM 2000 name recognised by the SCO system.	stimpv or 192.65.144.32

queue name Remote
 printer

for a *serial* port enter/select a queue name in the format:

raw_p<port_number> or
ascii_p<port_number>

for example:
raw_p4 or
ascii_p4

and for a *parallel* port in the format:

raw_<port_number> or
ascii_<port_number>

for example:
raw_4
ascii_4

If you want direct output to a hunt group,

omit the port number(s). For example:

raw_p or ascii_p (to
hunt the serial
ports, or
raw_ or ascii_ (to
hunt the parallel
ports)

For more information on queue names see section [queue types](#) below.

queue types

(refer to information [queue name](#) above) The Perle device will recognize two queue types, raw and ascii:

raw : the Perle device passes the complete print job - without filtering - through to the attached printer. Most print jobs will require the raw option.

ascii : the Perle device filters ascii characters from the print job. Some printers could require the ascii option, for example dumb printers.

You can append an optional `_d` or `_f` to the queue name which adds a <control d> or <form feed> to the end of the job. Some printers may require the above commands or characters.

3. If you are running SCO Open Server, exit scoadmin and go to [Executing an lpd job on page 37](#).

Executing an lpd job

To execute an *lpd* job from the command line (on a UNIX network host) use the following command:

```
lp filename
```

Notes

1. On a serial port match the line speed in the unit to the serial printer port speed.
2. If the port is not set up as a printer port, the job will fail.
3. If you want to set up a hunt group, make sure the same type of printer is connected to each of the unit's ports. The unit will output the file to the first free serial or parallel printer port. The syntax you have used will determine whether the unit hunts the serial or the parallel ports.

Remote Printing Using RCP

Printers connected to the serial and parallel ports of the units can be accessed by other TCP/IP hosts in the network using the RCP protocol; see [Figure 7](#). These connections are set up using the **printer** line service type.

This section consists of:

- [RCP Configuration step-by-step](#)
- [RCP Configuration Example](#)

For serial port configuration see the section [serial port](#) below; for parallel port configuration see the section [parallel port](#) on the next page.

RCP Configuration step-by-step

serial port

1. Select 'Line Port Settings' from the Line Configuration menu. Select the *serial* line to which your printer is attached; (in the cli use the command `set line`). Ensure the `service` field is set to `printer`. Look at the example line below (serial line default values shown):

```

+line 0+
service[printer]
  speed[9600 ]      terminal[dumb ]
  flow[none]       pages[4]
  bits[8]          user[
  parity[none]     hostname[sco ]
  stop[1]          host port[23 ]
  security[off]    JS port[23 ]
  dial[none ]     modem name none
  phone number[
  idle timer[      ] session timer[      ]

```

2. Configure the speed, flow, bits, parity and stop parameters.

It is *not* necessary to set the `hostname`, `terminal`, `pages`, `user`, `dial`, `modem`, `name` and `phone number` fields; these are ignored by the unit for this line service (printer). The `JS port`, `idle` and `session timer` fields may contain default or last-used values, but these also will be ignored by the unit.

Tip To reset the line to default, press <Enter> from any point in the form and accept the 'reset to default' option; see [Reset Serial Line to Default on page 53](#).

3. Accept and exit the form. If you wish, copy the line settings to other lines (an additional option as you exit the form; see [Copy settings to other lines on page 53](#)).

Tip You may want to save your configuration changes permanently; see [Section Save to non-volatile memory](#).

4. Go now to the section [configuration continued.....](#)

parallel port

JS4000

1. Select 'Parallel Port Settings' from the Line Configuration menu. Select the *parallel* line to which your printer is attached; (in the cli use the command `set parallel`). Ensure the `service` field is set to `printer`. Look at the example line below (printer line service type default values shown):

parallel 1			
service	[printer]		
hostname	[none]	host port	[23]
		JS port	[23]

2. Configure the `hostname` parameter; it will default to the first host you have entered in the unit's host table.

You do not need to set the `host port` and `JS port` fields.

Tip To reset the line to default, press <Enter> from any point in the form and accept the 'reset to default' option; see [Reset Parallel Line to Default on page 54](#).

3. Accept and exit the form. If you wish, copy the line settings to other lines (an additional option as you exit the form; see [Copy settings to other lines on page 53](#)).

Tip You may want to save your configuration changes permanently; see [Section Save to non-volatile memory](#).

configuration continued.....

4. Kill the line: from the Main Menu go to the Line Configuration menu and select 'kill line' (in the cli use the command `kill line`).
5. You now need to direct output from the network host to the printer.

The usual method is to issue the `rcp` command from the command line; see the section [executing an rcp job](#) below.

If you intend to send many print jobs you can either:

use a hunt group, (see the section [executing an rcp job](#) below), *or*

modify the printer interface script(s) on the network host so it will continue trying to send the print job when the unit's printer port is busy; see the section [modifying printer interface script](#) further below.

(If you do not wish to modify printer interface scripts, you may wish to print using `lpd`. The unit supports `lpd`; see [Section Remote Printing using LPD](#)).

executing an rcp job

To execute an `rcp` job from the command line, use the following commands:

port type on unit	syntax	example
a serial port	<code>rcp filename productname:pn</code>	<code>rcp myfile stimpy:p4</code>

a hunt group on serial ports	<code>rcp filename productname:p</code>	<code>rcp myfile stimp:y:p</code>
a parallel port	<code>rcp filename productname:n</code>	<code>rcp myfile stimp:y:1</code>
a hunt group on parallel ports	<code>rcp filename productname:</code>	<code>rcp myfile stimp:y:</code>

Where:

productname is the name ([servername](#)) you have assigned to either the JETSTREAM or LANSTREAM unit.

p indicates ‘serial port’ and is fixed.

n is the serial or parallel port (number) to which the printer is connected.

Caution

JETSTREAM 8500 only: in previous versions of software the hunt group on a serial port did not require you to specify the letter ‘p’. From now on you are required to specify the letter ‘p’ as shown above. This change is necessary to introduce hunt group working on the new parallel port (where fitted).

notes

1. On a serial port match the line speed in the unit to the serial printer port speed.
2. Multiple ‘printer’ connections will act as a hunt group, providing the same type of printer is connected to each port. The syntax you have used will determine whether the unit hunts the serial or the parallel ports.
3. If the unit’s port is not set up as a printer port, the job will fail.
4. If the unit’s port is busy, the job will fail (rejection message); this is a weakness of RCP. To prevent job failure you can modify the printer interface script(s) as shown below.

modifying printer interface script

On typical systemV based UNIX systems, the print spooler provides a set of back-end shell scripts for talking to printers. These scripts are usually found in the /usr/spool/lp directory tree. An example of how you might modify one of these scripts is given below.


```

while [ "$copies" -gt 0 ]
do
    for file
    do
        while true
        do
            rcp $file productname:pn
            if [ $? = 0 ]
            then
                break
            fi
        done
    done
    copies=`expr $copies -1`
done

```

RCP Configuration Example

This example describes in SCO UNIX how to setup to use RCP to print to a simple serial printer connected to a JETSTREAM 8500.

Example set-up:	<u>Device</u>	<u>Name</u>	<u>Comment</u>	<u>Configuration</u>
	Host Server	unix1	running SCO OpenServer 5.0.2	192.65.146.124
	JS8500	jstest	serial port 1 setup for rcp printing	192.65.146.122
	Printer Name	jstestp1	SCO printer name	
	Printer Model	jstestm1	Modified dumb printer model	
	Test Printer		Wyse 60 terminal	

JETSTREAM 8500 Configuration Set the required ports on the JETSTREAM 8500 to line service `printer` and the correct speed, etc.

SCO Configuration Add an entry for the `jstest` device in `/etc/hosts`

Test that rcp printing is working correctly using the `rcp` command from the command line; use syntax:

```
rcp /etc/hosts jstest:pl
```

In `/usr/spool/lp/model` find the printer model you need and copy it. For this example the printer model `dumb` was used and copied to `jstestm1`. Modify the new printer model to include the `rcp` command.

the original line was:

```
0<${file} eval ${FILTER} 2 >&1
```

the new line is:

```
rcp $file jstest:p1 2>&1
```

Create a new printer using scoadmin with a printer model of jstestm1 and a device of /dev/null.

Once the printer has been started (enable and accept) the lp command can be used to print to the JETSTREAM 8500.

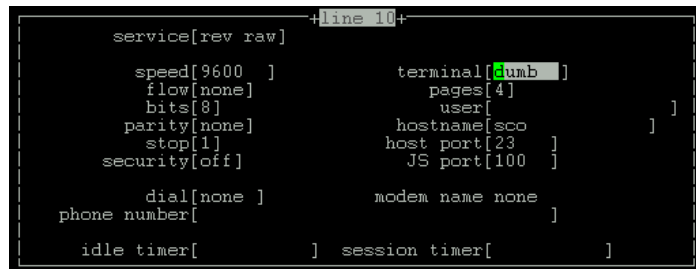
Remote Printing Using Host-Based Print Handling Software

cli syntax: set line

Printers connected to JETSTREAM 4000, 8500 or LANSTREAM 2000 ports can be accessed by TCP/IP hosts using print handling software. This type of connection uses the **reverse raw** line service. The print handling software needs to know the name of the unit and the TCP Port number assigned to the printer port. The same TCP Port can be assigned to a number of ports to form a hunt group.

To setup a reverse raw printing connection, follow these steps:

1. Select 'Line Settings' from the Line Configuration menu and select the line that you want to configure.
2. Set the Service field to 'rev raw'.



```

service[rev raw]
speed[9600 ] terminal[umb ]
flow[none] pages[4]
bits[8] user[ ]
parity[none] hostname[sco ]
stop[1] host port[23 ]
security[off] JS port[100 ]

dial[none ] modem name none
phone number[ ]

idle timer[ ] session timer[ ]
  
```

3. Configure the speed, flow, bits, parity and stop parameters for the line.
4. Enter a TCP port number in the JS port field. If you select a TCP port being used by another process, a connection will not be made (using a port number from 1024 upwards should work).
5. To set up a hunt group, assign the same TCP port number to each printer line. The unit will use the first free line in the group. You can set up a maximum of eight hunt groups.

Do not set the 'dial', 'modem name' and 'phone number' fields; these are ignored by the unit for this line service (reverse raw). The idle and session timer fields may contain default or last-used values, but these also will be ignored by the unit.

6. Accept and exit the form. If you wish, copy the line settings to other lines (an additional option as you exit the form; see [Copy settings to other lines on page 53](#)).

- On each TCP/IP host wanting to access the printer, set up a process to talk to the TCP port assigned to the unit's port. You can either write a program to do this, or you can use the MTSD print handling service described in the section [Section Modem and Printer Handling Using MTSD](#).

Tip You may want to save your configuration changes permanently; see [Section Save to non-volatile memory](#).

External host: Dialin Modem Connections

cli syntax:
set line

A dialin connection involves an external host connected to a JETSTREAM 4000, 8500 or LANSTREAM 2000 port trying to establish a connection with a TCP/IP host. In effect, the unit is trying to establish the connection. This type of connection uses the **silent raw** line service. The unit needs to know the name of the target TCP/IP host and the TCP Port number assigned, on the host, to listen for the dialin connection.

Note The unit performs no modem configuration or initialisation with the 'silent raw' line service. You must configure the modem BEFORE connecting it to the unit. Modems must be set to AUTO-ANSWER mode.

To set up a dialin connection, follow these steps:

- On the target TCP/IP host, assign a TCP port to listen for the dialin process.
- On the unit, select 'Line Settings' from the Line Configuration menu and select the line that you want to configure.
- Set the line service to 'sil raw'.
- Configure the speed, flow, bits, parity and stop parameters for the line.
- Enter the name of the target TCP/IP host in the hostname field.
- Enter the allocated TCP port number in the host port field.

```

+line 8+
service[sil raw]
  speed[9600 ]      terminal[dumb ]
  flow[none]       pages[4]
  bits[8]          user[ ]
  parity[none]     hostname[sco ]
  stop[1]          host port[1000 ]
  security[off]    JS port[23 ]
  dial[in ]        modem name none
  phone number[ ]
  idle timer[ ]    session timer[ ]
  
```

- Set the 'dial' field to 'in'. Do not set the 'modem name' and 'phone number' fields; these are ignored by the unit for this line service (silent raw). The JS port, idle and session timer fields may contain default or last-used values, but these also will be ignored by the unit.
- Accept and exit the form. If you wish, copy the line settings to other lines (an additional option as you exit the form; see [Copy settings to other lines on page 53](#)).
- On the TCP/IP host, set up a process to receive data on the Host TCP port. You can either write a program to do this, or you can use the MTSD modem handling service described in the section ["Section Modem and Printer Handling Using MTSD"](#).

Tip You may want to save your configuration changes permanently; see [Section Save to non-volatile memory](#).

Local host: Dialout Modem Connections

cli syntax: Modems connected to JETSTREAM 4000, 8500 or LANSTREAM 2000 ports can be accessed for dialout purposes by TCP/IP hosts using modem handling software. This type of connection uses the **reverse raw** line service. The modem handling software needs to know the name of the unit and the TCP Port number assigned to the modem port. The same TCP Port can be assigned to a number of ports to form a hunt group.

set line

Note *The unit performs no modem configuration or initialisation with the reverse raw line service. You must configure the modem BEFORE connecting it to the unit. Modems must be set to AUTO-ANSWER mode.*

To set up a dialout connection, follow these steps:

1. Select 'Line Settings' from the Line Configuration menu and select the line that you want to configure.
2. Set the Line Service field to 'rev raw'.

```

+line 11+
service[rev raw]
speed[9600 ]      terminal[dumb ]
flow[none]       pages[4]
bits[8]          user[ ]
parity[none]     hostname[sco ]
stop[1]          host port[23 ]
security[off]    JS port[1000 ]

dial[out ]      modem name none
phone number[ ]
idle timer[ ]   session timer[ ]

```

3. Configure the speed, flow, bits, parity and stop parameters for the line.
4. Enter a TCP port number to the JS port field. If you select a TCP port being used by another process, a connection will not be established (using a number in the range 1024 upwards should work).
5. To set up a hunt group, assign the same TCP port number to each dialout line. The unit will use the first free line in the group.
6. Set the dial field to 'out'. Do not set the 'modem name' and 'phone number' fields; these are ignored by the unit for this line service (reverse raw). The hostname, host port, idle timer and session timer fields may contain default or previous values, but these also will be ignored by the unit.
7. Accept and exit the form. If you wish, copy the line settings to other lines (an additional option as you exit the form; see [Copy settings to other lines on page 53](#)).
8. On each TCP/IP host that wants to access the modem(s), set up a process to talk to the unit's TCP port. You can either write a program to do this, or you can use the MTSD modem handling service described in the section "[Section Modem and Printer Handling Using MTSD](#)".

Tip *You may want to save your configuration changes permanently; see [Section Save to non-volatile memory](#).*

Host to host: bidirectional Modem Connections

cli syntax: You can set up bidirectional modem connections on a JETSTREAM 4000, 8500 or LANSTREAM 2000 port using the **bidir** line service. This enables a modem connected to a unit's port to be used for dialin and dialout purposes. To set up a bidirectional modem connection, follow these steps:

set line

1. On the network host targeted by the dialin connection, assign a TCP port to listen for the connection.
2. On the unit, select 'Line Settings' from the Line Configuration menu and select the line you want to configure.
3. Set the Line Service to **bidir**.

```

service[bidir ]
  speed[9600 ]      terminal[dumb ]
  flow[none]       pages[4]
  bits[8]          user[ ]
  parity[none]     hostname[sco ]
  stop[1]          host port[2000 ]
  security[off]    JS port[900 ]

  dial[both ]      modem name none
  phone number[ ]

  idle timer[ ]    session timer[ ]
  
```

4. Configure the speed, flow, bits, parity and stop parameters for the line.
5. To enable the dialout process, a TCP port number must be entered in the 'JS port' field. If you select a TCP port being used by another process, a connection will not be established (using a port from number 1024 upwards should work).
6. To set up a hunt group, specify the same TCP port number in the 'JS port' field of each line whose 'service' is set to 'bidir'. The unit will use the first free line in the group. You can create up to eight hunt groups.
7. For the dialin process, specify the TCP port assigned on the target host in the 'host port' field.
8. Enter the name of the target host in the 'hostname' field.
9. Set dial to 'both'. Do not set the 'modem name' and 'phone number' fields; these are ignored by the unit for this line service (bidir). The idle and session timer fields may contain default or last-used values, but these also will be ignored by the unit.
10. Accept and exit the form. If you wish, copy the line settings to other lines (an additional option as you exit the form; see [Copy settings to other lines on page 53](#)).
11. On the TCP/IP host targeted by the dialin connection, you must set up a process to receive data on the chosen TCP port. You can write your own program to do this or you can use the MTSD modem handling service described in the section [Section Modem and Printer Handling Using MTSD](#).
12. On each TCP/IP host which wants to use the dialout facility, set up a process to talk to the unit's TCP port. You can either write a program to do this, or you can use MTSD.

Tip You may want to save your configuration changes permanently; see [Section Save to non-volatile memory](#).

Modem and Printer Handling Using MTSD

MTSD is a host-based modem/print handling utility which enables applications, which need tty interfaces, to use JETSTREAM 4000, 8500 or LANSTREAM 2000 (the 'unit') ports. Such applications are kermi, uucp and lp; they use the unit's serial ports (and parallel ports - if fitted) so that the ports appear to be on the host. MTSD can be used to provide the following services:

- Dialin modem handler

- Dialout modem handler
- Bidirectional modem link
- Printer server

These modes can be invoked from the command line or set up to start automatically at boot (by editing UNIX start-up files). Thereafter the user can read/write to the link file created by the process.

MTSD can be installed on any TCP/IP host running UnixWare/SVR4 or SCO UNIX system.

Installing MTSD

You will find MTSD on the Supplemental disk/CD supplied with the unit. The diskette contains an executable file, makefile and source code for each of the SCO and SVR4 operating systems. The executables are called `mtsd.sco` and `mtsd.svr4`. To install/compile MTSD, follow these steps:

1. Tar the contents of the diskette/CD onto the TCP/IP host, and

either

- a. Copy the appropriate executable file to the hard disk (into `/usr/bin`, for example). MTSD is now installed.

or

- b. Use the source code and makefiles to compile MTSD on other operating systems.

or

- c. If you wish to compile the SCO and SVR4 makefiles, use the following make commands:

```
make sco
make svr4
```

Note Any changes to the source code are not supported by Perle.

Operation of MTSD

The modes of operation and the commands used to invoke them are described below. All MTSD commands can be abbreviated to the shortest unambiguous form. A comprehensive menu-driven help utility can be accessed by typing `mtsd -help` in the directory in which MTSD is resident. The help utility provides information on each mode of operation and each command option. MTSD outputs a software version number when run.

Start a Dialin Modem Handling Process

On dialin connections, MTSD will now, by default, start a login process on a pseudo tty directly (rather than set up a getty to spawn a login process on the linkfile).

Instead of reopening the same pseudo tty, MTSD selects the next available device in the list `p01->pff->q01->qff->r01->rff->p01`.

To set up a process to receive data on the TCP port assigned to the dialin connection, use the following command:

```
mtsd -dialin -hostport<tcpportno>
```

Where:

<tcpportno> is the TCP port to accept connection on the host.

The section “[Section External host: Dialin Modem Connections](#)” describes how to set up a dialin connection on a port.

Invoking a non-login process

On dialin connections, MTSD by default invokes /bin/login with 'sane' tty settings. There are a set of options which enable you to invoke a non-login process.

These are as follows:

-path <pathname>

pathname of required process (e.g. /bin/cat).

-prog <program_name>

name of program (e.g. cat).

-parg1...9 <argument>

enable you to specify a maximum of 9 arguments.

-termfile <filename>

the name of the file containing the termio settings (in stty -g format) to be used by the pseudo tty instead of the default 'sane' settings. After completion of the invoked process, the 'sane' tty settings will be resumed.

-nologin

defines the process as a USER_PROCESS for the purpose of updating /etc/utmp and wtmp files correctly.

An example is given below:

```
mtsd -dialin -hostport <tcpportno> -path /bin/cat -prog cat -  
parg1<filename>-nologin
```


-ttyname option on dialin connections

On dialin connections, the **-ttyname** option will enable you to allocate a specific name to the selected pseudo tty. This name will then be displayed, instead of the pty device name, when commands such as ps, tty and who are issued. When the connection is established, the pseudo tty will be removed from the /dev directory and replaced by the specified ttyname. This will be recorded in the file /etc/mtsd/ttyname enabling MTSD to recover the pseudo tty should the system crash.

Note You may have to create the /etc/mtsd/ directory.

-nolinger option on dialin connections

There is a mechanism which prevents a network connection being closed before all data has been received and acknowledged by the other end. It is called the SO_LINGER mechanism

The **-nolinger** option enables you to disable the SO_LINGER mechanism. If you are experiencing problems with the SO_LINGER mechanism, try using the **-drain** option to extend the timeout before resorting to the **-nolinger** option.

Dialin under Unix SVR4

On dialin connections under SVR4, the line discipline module is added by default. The relevant option is -noldterm.

Start a Dialout Modem Handling Process

MTSD can be used to set up a dialout process to connect to the TCP port assigned to the JETSTREAM 4000, 8500 or LANSTREAM 2000 port. To set up a dialout process, use the following command:

```
mtsd -dialout/-printer -mtsname <hostname>
-mtsport <tcpportno> -linkfile <filename>
```

Where:

tcpportno is the TCP port number assigned to the unit's port. If this TCP port is assigned to a hunt group, MTSD will use the first free port in the group.

filename is the name you want to assign to the file linked to the pseudo tty being used for the process.

hostname is the hostname or internet address of the unit.

The section [Section Local host: Dialout Modem Connections](#) describes how to set up dialout connections on the unit's serial ports.

For dialout connections, a **-noclose** option is provided which will hold the pseudo tty open after the network connection has closed, thus avoiding any connection closing issues. The **-inactivity** option enables you to set a period in minutes after which the pseudo tty should be closed regardless.

Start a bidirectional Modem Handling Process

MTSD can be used to set up a dialin process to receive data on the host TCP port number and read/write to a named link file, then start a dialout process to read from the link file and connect to the JETSTREAM 4000, 8500 or LANSTREAM 2000 TCP port.

Note that the linkfile will be unlinked during dialin operation to prevent a dialout process being started. The link will be restored as soon as the dialin process has completed.

To start this process, enter the following command:

```
mtsd -both -mtsport <tcpportnoA> -hostport <tcpportnoB> -  
link <filename> -mtsname <hostname>
```

Where:

tcpportnoA is the TCP port assigned to the unit's port. If the TCP port is used by a hunt group, MTSD will use the first free port it finds.

tcpportnoB is the TCP port number assigned on the TCP/IP host for the dialin connection.

filename is a name you want to assign to the link file.

hostname is the hostname or internet address of the unit.

The section [Section Host to host: bidirectional Modem Connections](#) describes how to set up a bidirectional connection.

NOTE: When running `ugetty` using the MTSD bidirectional facility, you must set it up so that it doesn't send the 'login:' prompt until the connection has been established. If you are running SCO UNIX this is performed by MTSD.

Start a Print Handling Process

MTSD can be used to start a print handling process to read/write from a named link file and connect to the TCP port assigned to the printer port. To start this process, enter the following command:

```
mtsd -print -mtsname <hostname> -mtsport <tcpportno>
[- newline] -linkfile <filename>
```

Where:

hostname is the hostname or internet address of the unit.

tcpportno is the TCP port assigned to the unit's port that the printer is attached to. If this TCP port number is assigned to a hunt group, the first free port in the group will be used.

newline is an optional argument which will perform newline to carriage return newline mapping.

filename is a name you want to assign to the link file. You must configure your UNIX printer to use this file as the print device.

The section "[Section Remote Printing Using Host-Based Print Handling Software](#)" describes how to set up a remote printing connection.

List of MTSD command options

Table 1

A full list of MTSD command options is:

MTSD Command Option	Function
-both bidirectional	Select bidirectional operation
-debug	If you include this argument, brief debug information will be displayed.
-dialin in	select dial-in operation
-dialout out	select dial-out operation
-drain <i>n</i>	This option enables you to specify the number of seconds before a connection is closed down. The default is 5 seconds. If you find that files or print jobs are being truncated, increase this value.
-hostport <tcpportno>	TCP port to accept connection on host
-inactivity	inactivity before connection is closed
-linkfile file	select linkfile name
-mtsname host <hostname>	select JETSTREAM 4000, 8500 or LANSTREAM 2000 to connect to

-mtsport <tcpportno>	TCP port assigned to hunt group on the unit
-newline mapping	Enable NL to CRNL mapping on output
-noclose	keep network connection open
-noldterm nolinedisc	Do not push on 'ldterm/linedisc'
-nolinger	Do not invoke SO_LINGER
-nologin	invoke a program other than a login
-opens n	This argument enables you to specify the number of times (after a one-second interval) that MTSD attempts to open the master pseudo tty. By default, MTSD makes 10 attempts. You will need to increase this value if the following error message is displayed: MTSD: re-open of master pty failed.
-pargx <argument>	arguments; x is in the range 1-9
-path <program_path>	program's path
-print	select print operation to the unit
-prog <program_name>	program to be invoked
-reconnects n	This option enables you to specify the number of times (after a two second interval) that MTSD will try to establish a connection with the unit. The default is 50. You will need to increase this value if you see the following message: MTSD: reconnection tries exhausted - aborting.
-retry n	This option enables you to specify the number of times (after a one-second interval) that MTSD attempts to read the master pseudo tty before deciding that no process is active. By default, MTSD makes 5 attempts. You will need to increase this value if you find that connections are being closed whilst still active. If you find that connections are being reopened too quickly, set retry to 0.
-termfile	termio settings file to use
-ttyname	specify a fixed tty name
-verbose	Include this argument if you want to receive full debug information.

Copy settings to other lines

This feature enables you to change a parameter (e.g. line service) and then copy that change to some or all lines. It is available in the Line Port Settings form and Parallel Port Settings form (under the Line Configuration Menu).

- Select a line and make the required change (e.g. change a serial line speed from 9600 baud to 57600 baud).
- Press <return> to display the 'Options' form:

```
+options+
accept and exit form
reset to default
copy settings to other lines
```

- Select 'copy settings to other lines'. Another form will be displayed which allows you to select other lines.

Reset Serial Line to Default

cli syntax:
reset line

This feature enables you to reset the serial line which you are configuring to the default settings. It is available in the Line Port Settings form (under the Line Configuration Menu). This line will be reset to 9600 baud, 8 data bits, 1 stop bit, no parity and software flow control; the line type will become 'jslogin', the TCP Port '23' and the hostname the first host entered in the host table.

- Press <return> to display the 'Options' form:

```
+options+
accept and exit form
reset to default
copy settings to other lines
```

- Select 'reset to default'.

Reset Parallel Line to Default

cli syntax:
reset parallel

This feature enables you to reset the parallel line which you are configuring to the default settings. It is available in the Parallel Port Settings form (under the Line Configuration Menu). This line will be reset to line type 'printer', the hostname the first host entered in the host table, the host port '23' and the JS port '23'.

- Press <return> to display the 'Options' form:

```
+options+
accept and exit form
reset to default
copy settings to other lines
```

- Select 'reset to default'.

Save to non-volatile memory

When you exit a menu screen (form) after making changes, you will be presented with the options form:

```
+options+
accept and exit form
reset to default
copy settings to other lines
```

If you choose to 'accept and exit form' your changes will be retained in RAM (volatile memory).

To save your changes permanently go to the Main Menu and select 'command line mode'; you will be presented with a form:

```
+exit full screen mode+
exit and save changes
exit without saving changes
return to main menu
```

Choose 'exit and save changes'. All the changes made since last entering the menus will be saved to FLASH (permanent, non-volatile) memory. The writing to FLASH will take a few seconds and during this time the unit will not respond to user input.

WARNING

do NOT turn off the power while the unit is writing to FLASH memory.

You should now be at the command line prompt. To return the text menus type:

cli syntax: screen

Saving to a file

netsave

You can also save your configuration information to a file on a host. This can only be done in the cli; see [Section *netsave*](#).

Chapter 3 Configuring a Line: - SLIP and PPP Connections

Introduction

This chapter deals with setting up SLIP and PPP connections on a line. It describes how your SLIP or PPP service can be started by a RADIUS host. There is also a summary of the configurable features of modems.

You will see that the JETSTREAM 4000, 8500 or LANSTREAM 2000 is called the '*unit*'. The use of the word '*unit*' avoids frequent repetition of the product names.

Chapter contents

This chapter is divided into the following sections:

- Overview
- SLIP, PPP and RADIUS
- Use SLIP or PPP?
- Setting Up the Line
- Configuring SLIP
- Configuring PPP
- Modems: summary of configurable features
- Copy settings to other lines
- Reset Serial Line to Default
- Save to non-volatile memory

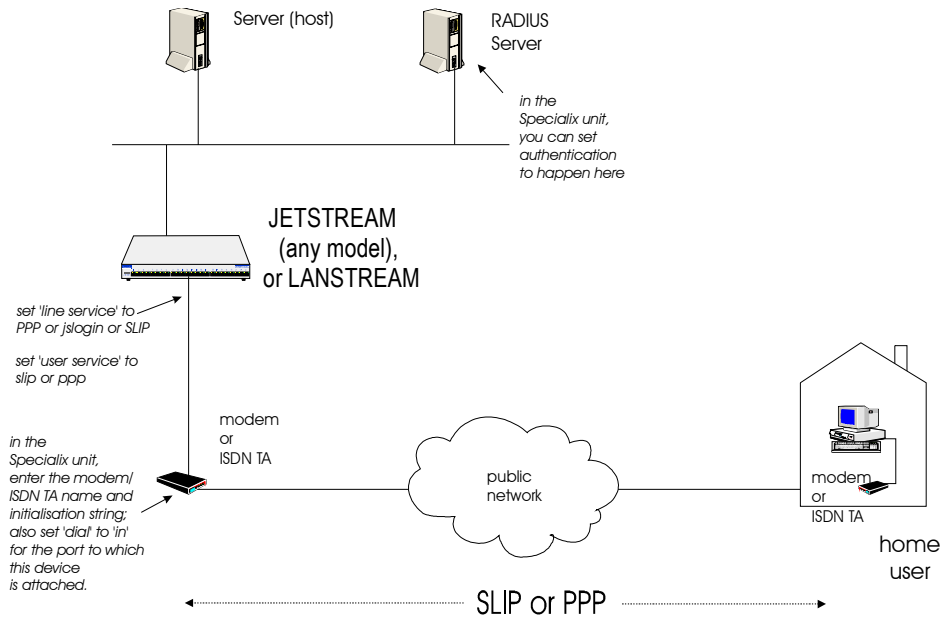
Note For an overview of all line types (including those discussed in other chapters in this manual) see Appendix A (Summary of Line Service Types).

Overview

We discuss two main uses of a SLIP or PPP connection:

1. Remote user. With SLIP or PPP on a port so that a remote user can connect and use the network as if that user is connected locally. See Figure 8.

Figure 8 A remote access connection



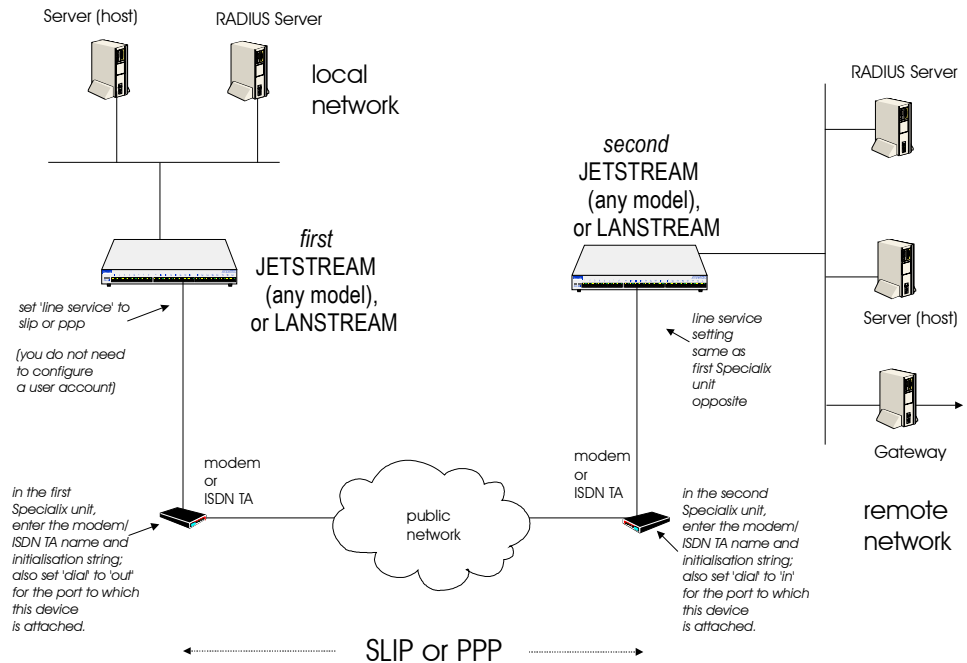
You will need to configure the port (Setting Up the Line on page 63), configure SLIP (Configuring SLIP on page 65) or PPP (Configuring PPP on page 67).

An example of a remote access connection using PPP, including the setup of a remote user is described in Chapter 8.

2. Joining together two networks. With SLIP or PPP you can use two units to connect together two networks. The units will be acting as routers.

Figure 9

Joining together two networks



In the above scenario calls can be made from the local to the remote network, but not the other way round. (To allow calls from the remote to the local network, you would change the 'dial' parameters from 'out' to 'in' on the modem/ISDN TA attached to the first unit and from 'in' to 'out' on the modem/ISDN TA attached to the second unit).

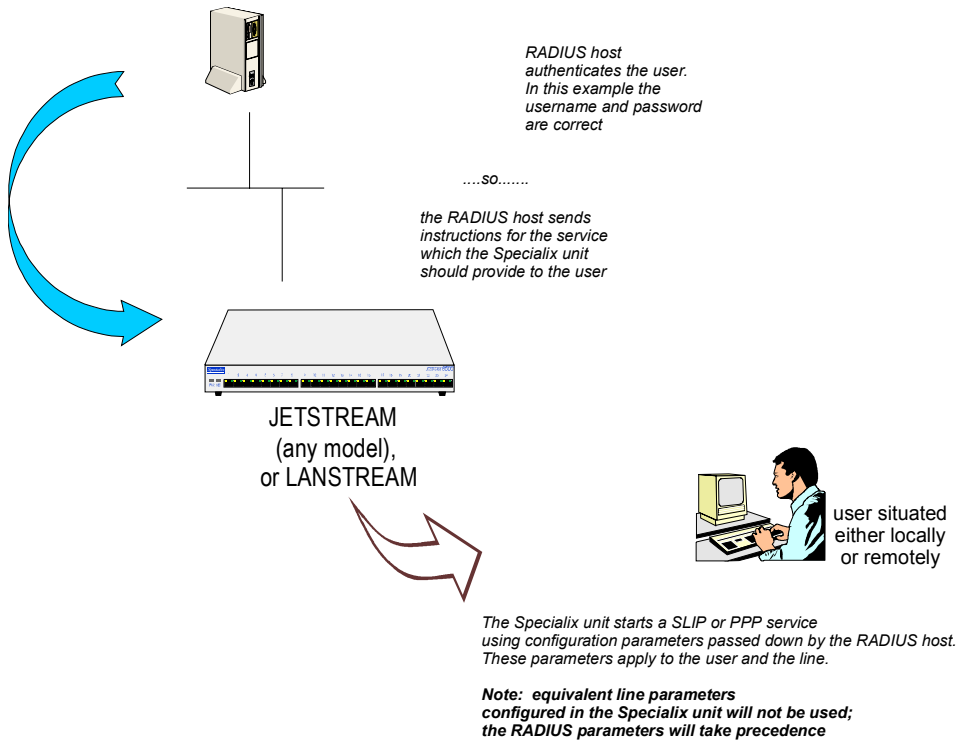
You will need to configure the line (Setting Up the Line on page 63) then configure SLIP (Configuring SLIP on page 65) or PPP (Configuring PPP on page 67).

An example of joining together two networks is presented in Joining together two networks on page 143

SLIP, PPP and RADIUS

When a user is authenticated by RADIUS the JETSTREAM 4000, 8500 or LANSTREAM 2000 (the 'unit') starts a user service of SLIP or PPP based on instructions passed down by the RADIUS host. SLIP or PPP parameters configured in the unit will not be used; see Figure 10.

Figure 10 SLIP or PPP service from a RADIUS host



How to configure authentication is explained in the JETSTREAM 4000, 8500, LANSTREAM 2000, Installation Guide, Section Initial Configuration.

An example of RADIUS parameters is shown in Figure 11; the file shown here is maintained on the RADIUS host.

Figure 11 example RADIUS user file: PPP service

```
angelaPassword = "rodeo"  
User-Service = Framed-User,  
Framed-Protocol = PPP,  
Framed-Address = 192.65.144.6,  
Framed-Netmask = 255.255.255.0,  
Framed-Routing = None,  
Framed-Compression = Van-Jacobson-TCP-IP,  
Framed-MTU = 1500,  
Idle-Timeout = 0,  
Session-Timeout = 0,  
Callback-Number = "981587793258"
```

An explanation of the file shown in Figure 11 is as follows:

User-Service and **Framed-Protocol** is the entry which instruct the unit to start a PPP service for the user (this equates to a user service of PPP; see Configure a User Account on page 82. However, since this user has been authenticated by RADIUS *all* the user parameters are provided by RADIUS).

Framed-Address, **Framed-Netmask**, **Framed-Compression** and **Framed-MTU** all have equivalent parameters in the unit's PPP line configuration (see Configuring PPP on page 67). The RADIUS parameters override the unit's equivalent parameters (see Table 2 for a cross-reference of SLIP/PPP line parameters).

Caution: the exception to the above rule is a **Framed-Address** value of 255.255.255.254. When this value is specified in the RADIUS file, the unit will use the Remote ip address configured for a PPP line in the unit.

Any RADIUS parameters specified in the RADIUS file but not supported by the unit, e.g. **Framed-Routing**, will be accepted by the unit but not processed. The start of the user service should not be affected by such parameters.

Idle-Timeout and **Session Timeout** have equivalent parameters in the unit's general line configuration (see Setting Up the Line on page 63). The RADIUS parameters override the unit's equivalent parameters (see Table 2 for a cross-reference of SLIP/PPP line parameters).

Callback Number is associated with a user (i.e. it is not a line parameter in the unit). Since this user has been authenticated by RADIUS, all the user parameters (including a callback number) are provided by RADIUS.

If you have user 'angela' also listed in the unit's user table (i.e. a duplicate entry - we do not recommend this action), all the user parameters configured in unit (see Chapter 4) for 'angela' will be overridden by the parameters in the RADIUS file; (for the user to be authenticated by the RADIUS host, where you

have a duplicate entry, the password for ‘angela’ in the unit would have to be different to that entered in the RADIUS user’s database *or* authentication in the unit would have to be set to RADIUS (i.e. RADIUS only)).

Additional note:

The unit has additional parameters which you can configure for a line (e.g. speed, flow, modem name), for SLIP (e.g. local ip address, suppress ICMP) and for PPP (ACCM, security). If there are no RADIUS parameters specified in the RADIUS file for these unit’s parameters, then the unit will use its’ own configured values.

To summarize, JETSTREAM 4000, 8500 or LANSTREAM 2000 begins a SLIP or PPP service for a user (when authentication has been carried out by the RADIUS host) with a mixture of values - some passed down by the RADIUS host and others taken from the unit’s own configuration.

Table 2 RADIUS: line, SLIP and PPP parameters supported by JETSTREAM 4000, 8500 or LANSTREAM 2000

RADIUS parameters (supported by the unit)	equivalent unit parameter	where to find the unit’s parameter
Framed-Address	Remote IP address	Section Configuring SLIP, Section Configuring PPP
Framed-Netmask	Subnet Mask	Section Configuring SLIP, Section Configuring PPP
Framed-MTU	Max TX Unit	Section Configuring SLIP
	Max receive unit	Section Configuring PPP
Framed-Compression	VJ_comp	Section Configuring SLIP, Section Configuring PPP
Idle Timeout	Idle Timer	Section Setting Up the Line
Session Timeout	Session Timer	Section Setting Up the Line

Use SLIP or PPP?

If you require any of the features listed below, use PPP, otherwise SLIP should be sufficient.

IP Address Negotiation. SLIP provides no mechanism for informing the other end of a link of its IP address, whereas PPP will do so.

Error Checking. SLIP does not error check whereas PPP does. This is not necessarily a problem in SLIP since most upper layer protocols have their own error checking.

Some systems exchange UDP packets with checksum disabled, which would cause problems should that part of an IP packet get corrupted.

Authentication. Once SLIP has started you cannot authenticate the remote device, whereas as PPP provides the option of using security protocols PAP or CHAP. See Section Configuring PPP, then sub-section ‘Security’ for further details.

Software Flow Control. You cannot use software flow control on SLIP links since there is no way of escaping control characters from the data stream. PPP has a facility (called ACCM) which allows specific control characters to be escaped from the data stream. See Section Configuring PPP for more details.

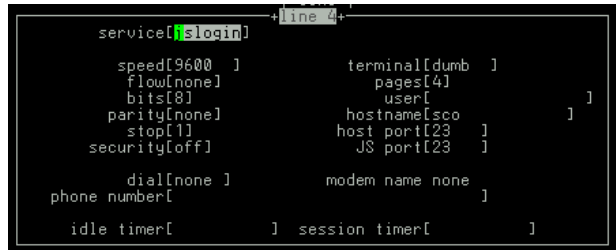
For more information on the SLIP and PPP protocols see Appendix C (SLIP and PPP overview).

Setting Up the Line

Note You can also use RADIUS to initiate a SLIP or PPP connection; this is explained in SLIP, PPP and RADIUS on page 59.

cli syntax:
set line,
show line

1. Select 'Line Settings' from the Line Configuration menu, then select a particular line; e.g. line 2. The following form will be displayed (default values):



```
service[login] line 4
speed[9600 ]      terminal[dumb ]
flow[none]       pages[4]
bits[8]          user[ ]
parity[none]     hostname[sco ]
stop[1]          host port[23 ]
security[off]    JS port[23 ]
dial[none ]     modem name none
phone number[ ]
idle timer[ ]   session timer[ ]
```

2. Go to the following fields: (use the spacebar to cycle through the line types (or type letter 'L' (upper or lower case) to list all possible values)

- Service .** We recommend you set:
- PPP** - when you want a remote access service connection (see Figure 8) using PPP, or when you want to use the unit as a router (see Figure 9) with PPP. In both cases the user (whether real or dummy) will be authenticated within PPP (provided you use Security - PAP or CHAP).
- jslogin** - when you want a remote access service connection (see Figure 8) using SLIP. Do **not** use the option 'SLIP' because there would be no authentication of the user; (instead, you will set SLIP for a particular user - see Section Configure a User Account).
- Choosing the 'jslogin' option, the unit will present the login prompt: the user will be required to enter a name and password and hence will be authenticated.
- If you are using scripts on the remote machine you may want the user to be prompted for a username and password; in this case you will want to set a line service of 'JS login'.
- SLIP** - when you want to use the unit as a router (see Figure 9) with SLIP. There will be no authentication of each unit by the other unit.
- Speed, Bits, Parity and Stop** change as necessary from the default line configuration of 9600 baud, 8 data bits, no parity, 1 stop bit
- Flow** Flow Control field. The possible values are either 'soft' (software) or 'hard' (hardware). The default value is 'none'.
For SLIP, set to 'hard' only.
For PPP, set to either 'soft' or 'hard' ('hard' recommended). If you select 'soft' you must set the parameter ACCM when you configure PPP for the line (in Configuring PPP on page 67).
- (Hostname)** do not enter a hostname; this field is used on terminal server connections only).
- Host port** this is the host TCP port number and is set by default to 23. In most cases you can use the default value.
- Dial** set to '**in**' if your user is remote and will be dialling in via modem or ISDN TA; set to '**in**' or '**out**' if using the unit as a router, depending on which end of the link your unit is situated (see Figure 9).
- Phone Number** when dial is set to 'out' and the line 'service' is set to 'slip' or 'ppp' enter a phone number for the unit to dial (you should only have this combination of settings when you are using two units back-to-back, i.e. as routers).
- Idle Timer** (*use only when using the unit as a router (see Figure 9)*); enter a period in seconds for which the idle timer will run. Use this timer to close a connection because of inactivity. When the idle timer expires the unit will end the connection. The maximum value is 4294967 seconds (equal to 49 days, approximately). A value of 0 (zero) means the idle timer will not expire, so the connection is open permanently.

Session Timer *(use only when using the unit as a router (see Figure 9)); enter a period in seconds for which the session timer will run. Use this timer to forcibly close the session (connection). When the session timer expires the unit will end the connection. The default value is 0 (zero), meaning that the session timer will not expire (the session is open permanently, or until you kill the line. The maximum value is 4294967 seconds (equal to 49 days, approximately).*

3. Ignore the other fields in this form. Press <return> to exit; if you do not wish to save your changes press the <escape> key.

cli syntax:
add modem

4. Go to the Line Configuration Menu:

a). select 'Add Modem'. Enter the name of the modem/ISDN TA attached to the unit. You can enter a maximum of twenty names, each with nineteen alphanumeric characters.

b). select 'Change Modem'. Select your modem/ISDN TA name. Enter the initialisation string; see your modem/ISDN TA documentation.

5. Press <return> to exit; if you do not wish to save your changes press the <escape> key.

set line

6. Go back to the 'Line Settings' menu. Select your line. When the line parameters form appears go the field 'modem name'. Press 'L' (upper or lower case) or the spacebar. Choose the modem name which you entered at Step 4.

7. Press <return> to exit; if you do not wish to save your changes press the <escape> key.

You can copy the settings for this line to other lines (an option as you exit this line); refer to Copy settings to other lines on page 74.

You can reset this line to default (an option as you exit this form); refer to Reset Serial Line to Default on page 74

8. You may want to save your configuration permanently; if so, refer to Save to non-volatile memory on page 75.

Configuring SLIP

Note You can use RADIUS to run your SLIP connection; this is explained in SLIP, PPP and RADIUS on page 59.

cli syntax:
set slip line,
show slip line

Select 'SLIP' from the Line Configuration menu. Then select a line. The SLIP form will be displayed (default values shown):

```

+slip_line 7+
local ip address[ ] remote ip address[ ]
 subnet mask[ ]
  mtu[256 ]          suppress icmp[off]
interact priority[on ] vj_comp[on ]
 tx parameters[on ]

```

The details of the SLIP parameters are:

Local ip address. This is the IP address of the unit end of the SLIP link. For routing to work you must enter an IP address in this field. Choose an address which is part of the same network or subnetwork as the remote end; e.g. if the remote end is address 192.101.34.146, your local ip address may be 192.101.34.145; (in the cli, example syntax would be:
set slip li 1 lipaddr 192.101.34.145)

Do not use the unit's (main) ip address in this field; if you do so, routing will not take place correctly.

Remote ip address This is the IP address of the remote end of the SLIP link. This must be specified. Choose an address which is part of the same network or subnetwork as the unit (see comment in 'Local ip address' above). Enter the remote ip address in dot notation, e.g. 192.101.34.146 (or in the cli, example syntax would be: set slip li 5 ripaddr 192.101.34.146)

If your user is authenticated by the unit this remote ip address will be overridden if you have set a 'framed ip' address for the user with values other than 255.255.255.254 or 255.255.255.255; see Section Configure a User Account, sub-section 'framed ip'.

If your user is authenticated by RADIUS *and* the RADIUS parameter 'Framed-Address' is set in the RADIUS file (see Figure 11) the unit will use the value in the RADIUS file in preference to the 'Remote ip address' value configured here.

Subnet Mask this is the subnet mask of the node on the remote end of the SLIP link. This field is optional. This parameter should be entered in dot notation e.g. 255.255.255.224

If your user is authenticated by RADIUS *and* the RADIUS parameter 'Framed-Netmask' is set in the RADIUS file (see Figure 11) the unit will use the value in the RADIUS file in preference to the 'Subnet Mask' value configured here.

Maximum transmission unit (mtu)

The Maximum Transmission Unit (mtu) parameter restricts the size of individual SLIP packets being sent by the unit. Enter a value in bytes between 256 and 1006, e.g. 512 (in the cli, example syntax would be: set slip li 1 mtu 512). The default value is 256. For more information on this parameter see Section Configure a User Account, sub-section 'framed mtu'.

If your user is authenticated by the unit this mtu value will be overridden when you have set a 'framed mtu' value for the user; see Section Configure a User Account, sub-section 'framed mtu'.

If your user is authenticated by RADIUS *and* the RADIUS parameter 'Framed-MTU' is set in the RADIUS file (see Figure 11) the unit will use the value in the RADIUS file in preference to the 'mtu' value configured here.

Suppress icmp This option causes ICMP (Internet Control Management Protocol) packets directed to this SLIP link to be discarded. The possible values are 'on' and 'off'; the default is off.

Interactive priority this determines whether interactive traffic (e.g. telnet sessions) is given priority over batch type traffic (e.g. ftp) thus avoiding the situation where a user has to wait for their character to be echoed while several large ftp packets are transferred. The possible values are 'on' and 'off'; the default is on.

VJ Compression. This determines whether Van Jacobson compression is used on this link; i.e. whether you are using SLIP or C-SLIP (compressed SLIP). The choices are ‘on’ (C-SLIP) or ‘off’ (SLIP); the default is ‘on’. Select ‘on’ will turn on VJ compression. C-SLIP greatly improves the performance of interactive traffic, such as Telnet or Rlogin; see Appendix C (SLIP and PPP overview) for more information.

In the cli, example syntax would be: `set slip li 1 vj on.`

If your user is authenticated by the unit this VJ compression value will be overridden if you have set a ‘framed compression’ value for a user; see Section *Configure a User Account*, sub-section ‘framed compression’.

If your user is authenticated by RADIUS *and* the RADIUS parameter ‘Framed-Compression’ is set in the RADIUS file (see Figure 11) the unit will use the value in the RADIUS file in preference to the ‘VJ compression’ value configured here.

TX parameters meaning Transmit parameters. This will output to the screen of the user all the SLIP parameters configured for that line/port. TX parameters are useful in some applications such as Trumpet Winsock. Options are ‘on’ or ‘off’.

Tip You may want to save your configuration changes permanently; see Section *Save to non-volatile memory*.

Tip If you want to configure several lines with the same parameters, go to Section *Copy settings to other lines* or Section *Reset Serial Line to Default*

Configuring PPP

Note You can use RADIUS to initiate your PPP connection; see *SLIP, PPP and RADIUS* on page 59.

An example of a remote access connection using PPP, including the setup of a remote user is described in Chapter 8.

cli syntax: Select ‘PPP’ from the Line Configuration menu. Then select a line. The PPP form will be displayed (default values displayed):

set PPP line,
show PPP line

```

+ppp line 6+
local ip address[ ] remote ip address[ ]
 subnet mask[ ] accm[ ]
 mru[1500] security[chap]
 user[ ] password[ ]
 ruser[ ] rpassword[ ]
 address_comp[on ] proto_comp[on ]
 vj_comp[on ] magic_neg[off]
 ipaddr_neg[off]
 conf req. to[3 ] term req. to[3 ]
 conf req. retries[10 ] term req. retries[2 ]
 conf nak retries[10 ] auth_tmout[1 ]
 roaming_callback[off] challenge_interval[ ]

```

Complete the fields as follows:

Local ip address. This is the IP address of the unit end of the PPP link. For routing to work you must enter a local IP address. Choose an address which is part of the same network or subnetwork as the remote end; e.g. if the remote end is address 192.101.34.146, your local ip address may be 192.101.34.145; (in the cli, example syntax would be:

```
set ppp li 6 lipaddr 192.101.34.145)
```

To see an example of ip address usage, refer to 'Figure 28 allocating local and remote IP addresses'. Do not use the unit's (main) ip address in this field; if you do so, routing will not take place correctly.

Remote ip address. This is the IP address of the remote end of the PPP link. This must be specified. Choose an address which is part of the same network or subnetwork as the unit (see comment in 'Local ip address' above). Enter the remote ip address in dot notation, e.g.192.101.34.146; (or in the cli, example syntax would be: set ppp li 6 ripaddr 192.101.34.146).

If you set the PPP parameter 'IP address negotiation' to 'on' the unit will ignore the remote ip address value you enter here and will allow the remote end to specify its ip address.

If your user is authenticated by the unit this remote ip address will be overridden if you have set a 'framed ip' address for the user other than 255.255.255.254; see Section Configure a User Account, sub-section 'framed ip'.

If your user is authenticated by RADIUS *and* the RADIUS parameter 'Framed-Address' is set in the RADIUS file (see Figure 11) the unit will use the value in the RADIUS file in preference to the 'Remote ip address' value configured here. The exception to this rule is a Framed-Address value in the RADIUS file of 255.255.255.254; this value allows the unit to use the remote ip address value configured here.

Subnet Mask this is the subnet mask of the node on the remote end of the PPP link. This field is optional. This parameter should be entered in dot notation e.g. 255.255.255.224 (or in the cli, e.g., set ppp li 9 255.255.255.224).

If your user is authenticated by RADIUS *and* the RADIUS parameter 'Framed-Netmask' is set in the RADIUS file (see Figure 11) the unit will use the value in the RADIUS file in preference to the 'Subnet Mask' value configured here.

ACCM. This allows the specification of an accm (asynchronous control character map) of characters that should be escaped from the data stream. This is entered as a 32 bit hexadecimal number with each bit specifying whether or not the corresponding character should be escaped.

The bits are specified most significant bit first and are numbered 31-0. Thus if bit 17 is set, the 17th character should be escaped i.e. 0x11 (XON). So entering the value 000a0000 (in the cli, e.g.: set ppp li 1 accm 000a0000) will cause the control characters 0x11 (XON) and 0x13 (XOFF) to be escaped on the link, thus allowing the use of XON/XOFF (software) flow control.

If you have selected software flow control on the line (see Setting Up the Line on page 63) you must enter a value of 000a0000 for the ACCM.

The default value is 00000000, which means no characters will be escaped.

Max. receive unit The Maximum Receive Unit (mru) parameter specifies the maximum size of PPP packets that the unit's port will accept. Enter a value in bytes between 64 and 1500; e.g. 512 (in the cli, example syntax would be: `set ppp li 1 mru 512`). The default value is 1500. For more information on this parameter see Section *Configure a User Account*, sub-section 'framed mtu'.

If your user is authenticated by the unit the 'mru' value will be overridden when you have set a 'framed mtu' value for the user; see Section *Configure a User Account*, sub-section 'framed mtu'.

If your user is authenticated by RADIUS *and* the RADIUS parameter 'Framed-MTU' is set in the RADIUS file (see Figure 11) the unit will use the value in the RADIUS file in preference to the 'mru' value configured here.

Security. This specifies what type of authentication will be done on the link: none, PAP or CHAP. The default is CHAP.

You can use PAP and/or CHAP to:

- a) authenticate a port or user on the unit, from a remote location, or
- b) authenticate a remote client/device, from the unit.

PAP is a one time challenge of a client/device requiring that it respond with a valid username and password. A timer operates during which successful authentication must take place. If the timer expires before the remote end has been authenticated successfully the link will be terminated.

CHAP challenges a client/device at regular intervals to validate itself with a username and a response, based on a hash of the 'secret' (password). A timer operates during which successful authentication must take place. If the timer expires before the remote end has been authenticated successfully the link will be terminated.

With both PAP and CHAP make sure the unit and the remote client/device have the same setting. e.g. if the unit is set to PAP but the remote end is set to CHAP the connection shall be refused. For help - where your remote end is a Windows NT or 95 PC - see *Setting up a Remote User (with PPP)* on page 136, sub-section 'Windows NT4 or 95 configuration option'.

In the cli, to turn on PAP (for example) the syntax would be:
`set ppp li 7 security pap`

If you have selected a line service of 'jslogin', PAP or CHAP will not take place since the user will have already been authenticated. In this case setting security to PAP or CHAP will have no effect.

User . Complete this field only if you :

- have specified PAP or CHAP (security protocols) in the 'Security' field, *and*
- you wish to dedicate this line to a single remote user, and this user will be authenticated by the unit, *or*
- you are using the unit as a router (back-to-back with another unit).

'User' is the name the remote device will use to authenticate a port on this unit (the opposite of the parameter 'Remote User'). The remote device will only authenticate your unit's port when PAP or CHAP are operating. You can enter a maximum of sixteen alphanumeric characters, e.g. kevinc8 (or, in the cli, example syntax would be `set ppp li 1 user kevinc8`)

When connecting together two networks, enter a dummy user name; e.g. JS_HQ.

Note *If you want a reasonable level of security the user name and password should not be similar to a user name or password used regularly to login to the unit.*

Password. Complete this field only if you :

- have specified PAP or CHAP (security protocols) in the 'Security' field, *and*
- you wish to dedicate this line to a single remote user, and this user will be authenticated by the unit, *or*
- you are using the unit as a router (back-to-back with another unit).

'Password' means the following:

- in the 'Security' field, when you have specified PAP 'Password' is the password the remote device will use to authenticate the port on this unit (the opposite of the parameter 'Remote Password'). The remote device will only authenticate your unit's port when PAP or CHAP are operating.

- in the 'Security' field, when you have specified CHAP 'Password' is the secret (password) known to both ends of the link upon which responses to challenges shall be based. The remote device will only authenticate your unit's port when PAP or CHAP are operating.

In both cases, you can enter a maximum of 16 alphanumeric characters; (in the cli, example syntax would be: `set ppp li 7 password *****`)

Remote User. Complete this field only if you :

- have specified PAP or CHAP (security protocols) in the 'Security' field, *and*
- you wish to dedicate this line to a single remote user, and your user will be authenticated by the unit, *or*
- you are using the unit as a router (back-to-back with another unit).

'Remote User' is the name the unit will use to authenticate the port on the remote device (the opposite of the parameter 'User'). Your unit will only authenticate the port on the remote device when PAP or CHAP are operating. You can enter a maximum of sixteen alphanumeric characters;

(in the cli, example syntax would be: `set ppp li 6 ruser kevin`)

When connecting together two networks, enter a dummy user name; e.g. JS_SALES.

Note *If you want a reasonable level of security the user name and password should not be similar to a user name or password used regularly to login to the unit.*

Remote Password. Complete this field only if you :

- have specified PAP or CHAP (security protocols) in the 'Security' field, *and*
- you wish to dedicate this line to a single remote user, and this user will be authenticated by the unit, *or*
- you are using the unit as a router (back-to-back with another unit).

'Remote password' means the following:

- in the 'Security' field when you have specified PAP, 'Remote Password' is the password the unit will use to authenticate the remote device.

- in the 'Security' field when you have specified CHAP, 'Remote Password' is the secret (password) known to both ends of the link upon which responses to challenges shall be based.

In summary 'Remote Password' is the opposite of the parameter 'Password'. Your unit will only authenticate the remote device when PAP or CHAP are operating.

In both cases, you can enter a maximum of sixteen alphanumeric characters; (or, in the cli, e.g., `set ppp li 1 rpassword *****`)

Address/Control compThis determines whether compression of the PPP Address and Control fields shall take place on the link. The choices are 'on' or 'off'; the default is 'on'. For most applications this should be enabled; i.e. 'on'. In the cli example syntax would be:
`set ppp li 1 address_comp on`

Protocol compressionThis determines whether compression of the PPP Protocol field shall take place on this link. The choices are 'on' or 'off'; the default is 'on'. For most applications this should be enabled; i.e. 'on'. In the cli example syntax would be:
`set ppp li 1 proto_comp on`

VJ Comp. This determines whether Van Jacobson Compression is used on this link. The choices are 'on' or 'off'; the default is 'on'. Select 'on' will turn on VJ compression. Select 'on' will turn on VJ compression. C-SLIP greatly improves the performance of interactive traffic, such as Telnet or Rlogin; see Appendix C (SLIP and PPP overview) for more information. In the cli, example syntax would be: `set ppp li 1 vj on`.

If your user is authenticated by the unit this VJ compression value will be overridden if you have set a 'framed compression' value for a user; see Section [Configure a User Account](#), sub-section 'framed compression'.

If your user is authenticated by RADIUS *and* the RADIUS parameter 'Framed-Compression' is set in the RADIUS file (see Figure 11) the unit will use the value in the RADIUS file in preference to the 'VJ compression' value configured here.

Magic No. negotiationThis is a mechanism whereby a line can determine if it has been looped back. The choices are 'on' or 'off'; the default is 'off'. If enabled (on) this option allows the sending of random numbers on the link. The random numbers should be different, unless the link has been looped back. In the cli, example syntax would be: `set ppp li 1 magic_neg off`.

IP address negotiation. This parameter specifies whether or not IP address negotiation shall take place. IP address negotiation is where the unit allows the remote end to specify its ip address. The values are 'on' or 'off'. The default value is 'off'.

If set to 'on' the unit allows the remote end to specify its ip address; the ip address specified by the remote end will then be used in preference to the Remote ip address set for a line.

If set to 'off' the unit will *not* allow the remote end to specify its ip address. The Remote ip address set for the line will be used.

In the cli, example syntax would be: `set ppp li 7 ipaddr_neg on`.

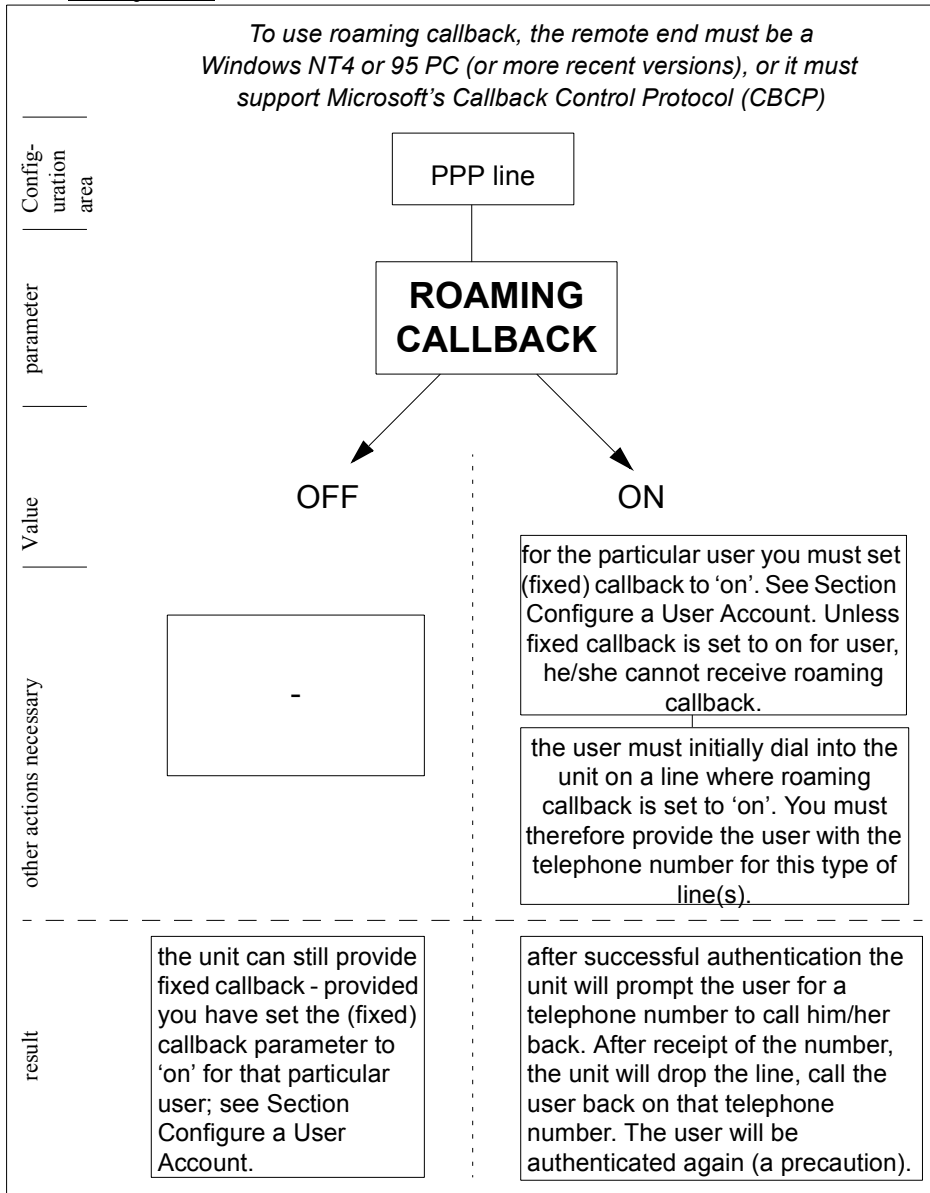
When configuring your user (Configure a User Account on page 82), if you set 'framed ip' address to 255.255.255.255, the unit will override the value for IP address negotiation set here. The result is that the unit will allow the remote end to specify its ip address.

- Configure req. timeout**This parameter specifies the maximum time in seconds that LCP (Link Control Protocol) will wait before it considers a 'configure request' packet to have been lost. (in the cli example syntax would be: set ppp li 8 cr_tmout 3).
- Terminate req. timeout**This parameter specifies the maximum time in seconds that LCP (Link Control Protocol) will wait before it considers a 'terminate request' packet to have been lost; (in the cli example syntax would be: set ppp li 24 tr_tmout 3).
- Configure req. retries**This parameter specifies the maximum number of times a 'configure request' packet will be sent before the link is terminated; (in the cli example syntax would be: set ppp li 23 cr_retry 10)
- Terminate req. retries**This parameter specifies the maximum number of times a 'terminate request' packet will be sent before the link is terminated; (in the cli example syntax would be: set ppp li 13 tr_retry 2)
- Configure NAK retries**This parameter specifies the maximum number of times a 'configure nak' packet will be sent before the link is terminated; (in the cli example syntax would be: set ppp li 2 nak_retry 10)
- Authentication timeout.** The timeout in minutes during which successful PAP or CHAP authentication must take place; (you must have PAP or CHAP turned on). If the timer expires before the remote end has been authenticated successfully the link will be terminated. (in the cli example syntax would be: set ppp li 5 auth_tmout 1)
- Roaming callback**allows the user to specify a telephone number which the unit should use to callback him/her. This feature is particularly useful for a mobile user. The possible values are 'on' and 'off'; the default is 'off'. The operation of roaming callback is shown diagrammatically in Figure 12.
- Roaming callback can only work with a user whose (fixed) callback parameter is set to 'on'. See Section Configure a User Account. Roaming callback therefore overrides (fixed) callback.
- The user is allowed 30 seconds to input a telephone number after which the unit ends the call.
- Challenge_interval**sets the interval in minutes at which the unit will issue a CHAP re-challenge to the remote end. The default value is 0 (zero) meaning CHAP re-challenge is disabled. During CHAP authentication an initial CHAP challenge takes place, and is unrelated to CHAP re-challenges. The initial challenge takes place even if re-challenges are disabled.
- Some PPP client software does *not* work with CHAP re-challenges so you may wish to leave the parameter disabled in the the unit.

Tip You may want to save your configuration changes permanently; see Section Save to non-volatile memory.

Tip If you want to configure several lines with the same parameters, go to Section Copy settings to other lines or Section Reset Serial Line to Default

Figure 12 Roaming callback



Modems: summary of configurable features

A summary of the configurable features for modems is listed below.

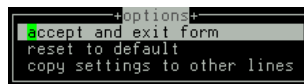
Note all references to modems apply equally to ISDN Terminal Adaptors

- cli syntax:**
set line
- you can set the 'dial' parameter to 'in', 'out' or 'none' (default 'none') in the line parameters sub-menu. Setting 'in' or 'out' tells the unit that there is a modem on that line. The unit will communicate with the modem through various RS232 signals. The 'dial' parameter can be set for all line services (e.g. jslogin, silent raw).
- set line**
- when dial is set to 'out' *and* the line service is set to 'slip' or 'ppp' you can enter a 'phone number for the unit to dial (line parameters sub-menu). This combination of circumstances occurs when you have two units connected back-to-back; i.e. they are acting as routers (see Figure 9).
- add modem**
set modem
- when the 'dial' parameter to 'in' and the line service is set to 'js_login', 'slip' or 'ppp' the unit can initialise a modem. You enter a modem name and initialisation string in the modems sub-menu. The unit will initialise that modem before any new connection is started.
 - The unit will ignore any modem names or initialisation strings with the following line service types: `direct` (all types), `silent` (all types), `printer`, `reverse`, `bidir`
You can however, set the 'dial' parameter.
 - when you are connecting from a terminal the unit offers automatic baud rate detection on the line. If you do not see any characters, or garbled characters, you send line breaks (<break> key) until the correct line speed setting is reached. The feature is explained in more detail in Section Logging in.

Copy settings to other lines

This feature enables you to change a parameter (e.g. line service) and then copy that change to some or all lines. It is available in the Line Settings form (under the Line Configuration Menu).

- Select a line and make the required change (e.g. change line speed from 9600 baud to 57600 baud).
- Keeping the cursor in the modified field, press <return> to display the 'Options' form:



- Select 'copy settings to other lines'. The change will be made to all lines.

Reset Serial Line to Default

- cli syntax:**
reset line
- This feature enables you to reset the serial line which you are configuring to the default settings. It is available in the Line Settings form (under the Line Configuration Menu). The line will be reset to 9600 baud, 8 data bits, 1 stop bit, no parity and software flow control; the line type will become 'JS login', the TCP Port '23', the Idle Timer '300' seconds and the hostname the first host entered in the host table.

- Press <return> to display the 'Options' form:

```
+options+
accept and exit form
reset to default
copy settings to other lines
```

- Select 'reset to default'.

Save to non-volatile memory

When you exit a menu screen (form) after making changes, you will be presented with the options form:

```
+options+
accept and exit form
reset to default
copy settings to other lines
```

If you choose to 'accept and exit form' your changes will be retained in RAM (volatile memory).

To save your changes permanently you will need to exit the menu system. Return to the Main Menu and select 'command line mode'; you will be presented with a form:

```
+exit full screen mode+
exit and save changes
exit without saving changes
return to main menu
```

Choose 'exit and save changes'. All the changes made since last entering the menus will be saved to FLASH (permanent, non-volatile) memory. The writing to FLASH will take a few seconds and during this time the unit will not respond to user input.

WARNING

do NOT turn off the power while the unit is writing to FLASH memory.

You should now be at the command line prompt. To return the text menus type:

cli syntax:
screen

```
screen
```

Saving to a file

netsave

You can also save your configuration information to a file on a host. This can only be done in the cli; see Section `netsave`.

Chapter 4 Configuring a User

Contents

- Introduction
- When you need User accounts
- User accounts and RADIUS
- Add a User Account
- Configure a User Account
- User Levels
- Running Sessions
- Change a User's Password
- Delete a User Account
- Language support
- Save to non-volatile memory

Introduction

You need to configure user accounts on the JETSTREAM 4000, 8500 or LANSTREAM 2000 (the 'unit') for those users who want particular types of Terminal Server or Remote Access connections. If you are using a RADIUS host you may not need user accounts for those users who are authenticated by the RADIUS host; see User accounts and RADIUS on page 78.

When you set up a User account you will see, as an example, the following form in the text menus:

```
+user julie+
username julie          language[english ]
screen switch[1 ]      level[normal ]
service[jsprompt ]     ip_host[ ]
tcp port[23 ]          callback[off ]
phone number[ ]
idle timer[ ]          session timer[ ]
framed ip[255.255.255.254] framed netmask[ ]
framed mtu[1500 ]     framed compression[on ]
```

More detail on this form is contained in Configure a User Account on page 82.

When you need User accounts

The types of **terminal server connections** where you will need to configure user accounts are where users:

- have a login directly on a local host, by-passing the unit (using the rlogin protocol)
- are authenticated by unit and then have a telnet or rlogin service started on a host
- want a single or multiple session(s) on a host; here they initially login to the unit before starting that session. The unit is used to configure and start the session.

The **remote access connections** where you will need to configure user accounts are where users:

- are being provided a remote access service, i.e. a SLIP or PPP connection, and they are being authenticated by unit.

As the system administrator you will have your own user account (default name 'admin').

The unit's login accounts are password-protected and assigned a user level; this level restricts the user to certain commands; see Section User Levels. A maximum of 32 user accounts can be created.

Note You may not need user accounts for users authenticated by the RADIUS host; see User accounts and RADIUS on page 78.

User accounts and RADIUS

You can have a maximum of 32 user accounts on the JETSTREAM 4000, 8500 or LANSTREAM 2000 (the 'unit'). You will also be able to configure user accounts on the RADIUS host (the quantity will vary depending on the host). Therefore some users can be authenticated by the unit, other users by RADIUS. You could have other combinations of maintaining user accounts; i.e. duplicated on both the unit and the RADIUS host or, alternatively all user accounts stored on the RADIUS host only (except username 'admin' - this will always be stored in the unit and always authenticated by the unit). Whichever method you choose, make sure the setting for 'authentication' is correct - see JETSTREAM 4000, 8500, LANSTREAM 2000, Installation Guide, Section RADIUS configuration.

Figure 13 When RADIUS authenticates users (1 of 2)

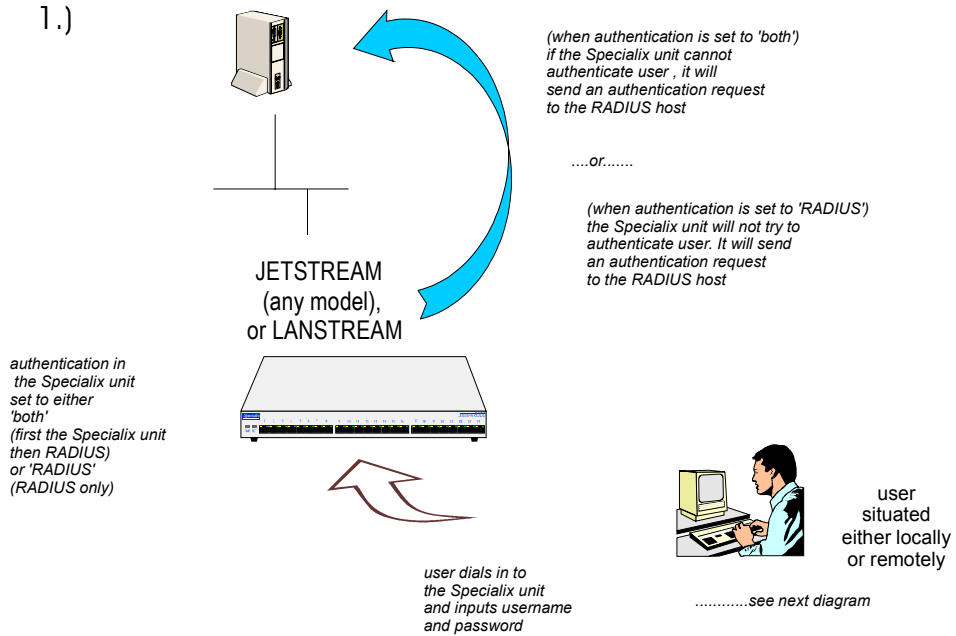


Figure 14 When RADIUS authenticates users (2 of 2)

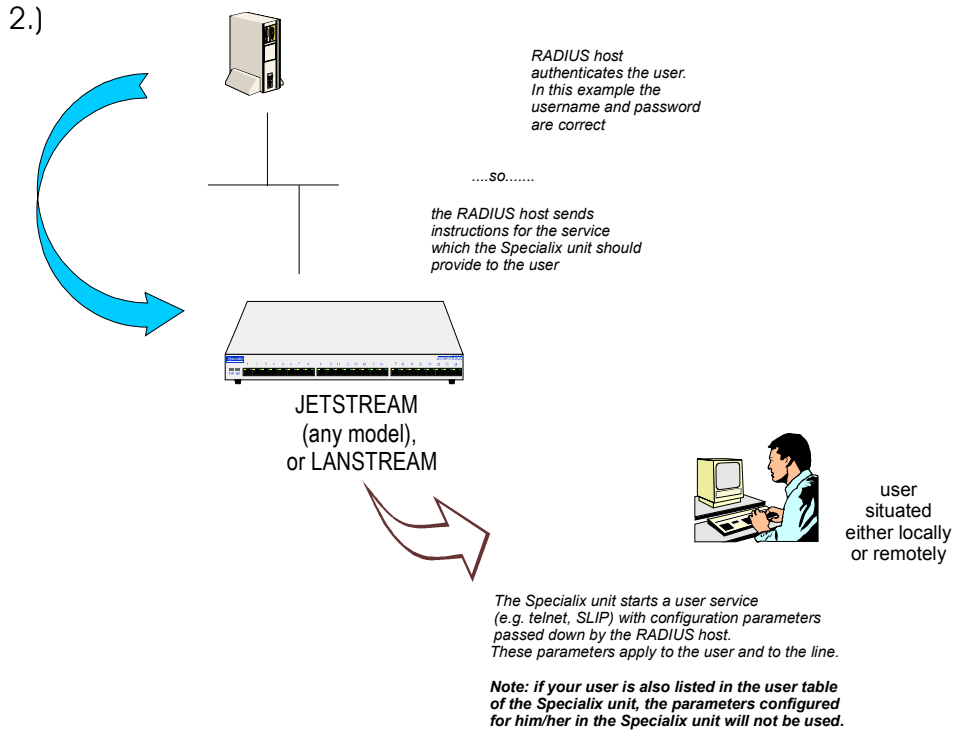


Figure 13 and Figure 14 show that when a user is authenticated by RADIUS the unit starts a user service - such as telnet or SLIP - based on instructions passed down by the RADIUS host. User parameters - such as 'service' or 'ip_host' are taken entirely from the RADIUS host. (This situation is totally different from users authenticated in the unit, where user parameters are taken from the unit's database).

An example of parameters passed down by a RADIUS host to the unit is shown in Figure 15; this file is maintained on the RADIUS host.

Figure 15 example RADIUS user file: telnet service

```
davePassword = "garage"
User-Service = Callback-login,
Login-Host = 192.101.34.199,
Login-Service = Telnet,
Login-TCP-Port = 23,
Class = "Indirect Sales Group",
Session-Timeout = 1800,
Idle-Timeout = 600,
CallBack-Number = "3592"
```

An explanation of the file shown in Figure 15 is as follows:

- the file contains a mixture of user parameters (e.g. callback-number) and line parameters (e.g. login-host).
- this user has been authenticated by RADIUS; therefore, all user parameters are passed down to the unit in this file.
- if you also have user 'dave' listed in the unit's user table (i.e. a duplicate entry - we do not recommend this action) all the user parameters configured in the unit for user 'dave' will be overridden by the parameters in the RADIUS file; (for the user to be authenticated by the RADIUS host, where you have a duplicate entry, the password for 'dave' in the unit would have to be different to that entered in the RADIUS user's database *or* authentication in the unit would have to be set to RADIUS (i.e. RADIUS only)).
- `Class = "Indirect Sales Group"` is a RADIUS class attribute. The unit can only process a string of maximum 32 characters; therefore limit your string to this size. In this example "Indirect Sales Group" is 20 characters (including spaces).
- line parameters override those configured in the unit; see SLIP, PPP and RADIUS on page 59 for a more detailed discussion on line parameters.

Add a User Account

cli syntax: Select 'Add User' from the Users menu.

add user

Enter a username, maximum sixteen characters (do not use spaces). If your user is equipment (see User Service 'TCP clear:' in the next section) allocate an appropriate name, e.g. barcode2.

Enter a password, maximum sixteen characters (do not use spaces). Re-enter the password.

Admin users can change user passwords using the ‘Set Password’ feature described in Change a User’s Password on page 88. Normal users can change their own passwords; see Section Changing your Password.

Configure a User Account

Tip You are about to configure a user account in the unit. Your configuration will only be used if the user is authenticated by the unit. If the user is authenticated by RADIUS, the unit will use configuration details for users sent by the RADIUS host; see User accounts and RADIUS on page 78.

cli syntax: set user

1. Select ‘Change User’ from the Users menu. Choose your user from the list of names. As an example, the following form will be displayed (default values):

```

+user julie+
username julie          language[english ]
screen switch[1 ]      level[normal ]
service[jsprompt ]     ip host[          ]
tcp port[23 ]          callback[off ]
phone number[          ]
idle timer[            ] session timer[      ]
framed ip[255.255.255.254] framed netmask[    ]
framed mtu[1500 ]      framed compression[on ]
  
```

2. Go to the following fields:

Screen switch (ignore this field unless the user will be running sessions and has a user level of ‘normal’ (see Section Running Sessions)

this is the ‘hot-key’ command used, in conjunction with other keys, for switching between sessions. This may need to be changed if it clashes with an application a user is going to run in one of their sessions. It must be entered in hex format; the default is ‘1’ (^A). Refer to the ascii code chart in ASCII to Decimal and Hex Conversion Chart on page 243. Normal users can change their own screen switch character using the menus: Sessions>Set Up User>User environment.

Service instructs the unit to start a user service by selecting one from the following list (once the user is authenticated successfully by the unit):

js prompt: a login on the unit (the default setting). Use this service for you as the system administrator, or for users who wish to run a single or multiple sessions on Terminal Server connections; these sessions are configured within the unit (see Section Running Sessions).

Telnet: a Telnet service provided by the unit. Use this service when you/a user is connected directly to a port via a serial line (i.e. not connected into one of the network ports). When the telnet service starts, the user will be authenticated by the host. Now go to the IP Host and TCP Port No fields.

Tip When specifying the ‘telnet’ option, we recommend you set the ‘line service’ on that particular line to ‘jslogin’; see Section Starting Telnet/Rlogin from the unit.

Rlogin: an Rlogin service provided by the unit. Use this service when you/a user is connected directly to a port via a serial line (i.e. not connected into one of the network ports). When the rlogin service starts, the user will be authenticated by the host. Now go to the IP Host field.

Tip When specifying the 'rlogin' option, we recommend you set the 'line service' on that particular line to 'jslogin'; see Section Starting Telnet/Rlogin from the unit.

TCP clear: use for devices which require a login, i.e. authentication. Such devices could be a bar code reader or smart card. 'TCP clear' provides a channel on which 8-bit data is passed, without interpretation, to a host. It has the same meaning as the TCP Clear login service specified in the RADIUS Authentication rfc; see Appendix D (References).

SLIP: The SLIP service will be started using the SLIP parameters set for that line; see Section Configuring SLIP. There will be no further login prompt (unless callback is operating). The SLIP line settings will be taken from the settings configured for that line.

Tip When specifying the 'SLIP' option, we recommend you set the 'line service' on that particular line to 'jslogin'; see Section Setting Up the Line.

PPP: The PPP service will be started using the PPP parameters set for that line; see Section Configuring PPP. There will be no further login prompt (unless callback is operating). The PPP line settings will be taken from the settings configured for that line.

Tip When specifying the 'PPP' option, we recommend you set the 'line service' on that particular port to 'jslogin'; see Section Setting Up the Line.

Note Note also that some types of user service have the same name as line service types, e.g. 'user service: SLIP' and 'line service:SLIP'. User 'service' is explained in Section Configure a User Account.

TCP Port No. (ignore this field unless you have selected a user Service of 'telnet')

(telnet only) enter the TCP/IP port number of the host with which the unit should start the telnet service. The default port is 23; in most cases you should leave the value at default.

phone number. enter a telephone number for the unit to call back the user; do not use spaces. You must also have 'callback' set to on. (The number you enter is unrelated to the 'phone_number' or 'dial' parameters you can set for a line).

idle timer. (you may wish to change this setting for terminal server connections) enter a period in seconds for which the idle timer will run. Use this timer to close a connection because of user inactivity. When the idle timer expires the unit will end the connection. The default value is 300 seconds, meaning the idle timer will expire 300 seconds after the last activity. The maximum value is 4294967 seconds (equal to 49 days, approximately). A value of 0 (zero) means the idle timer will not expire so the connection is open permanently.

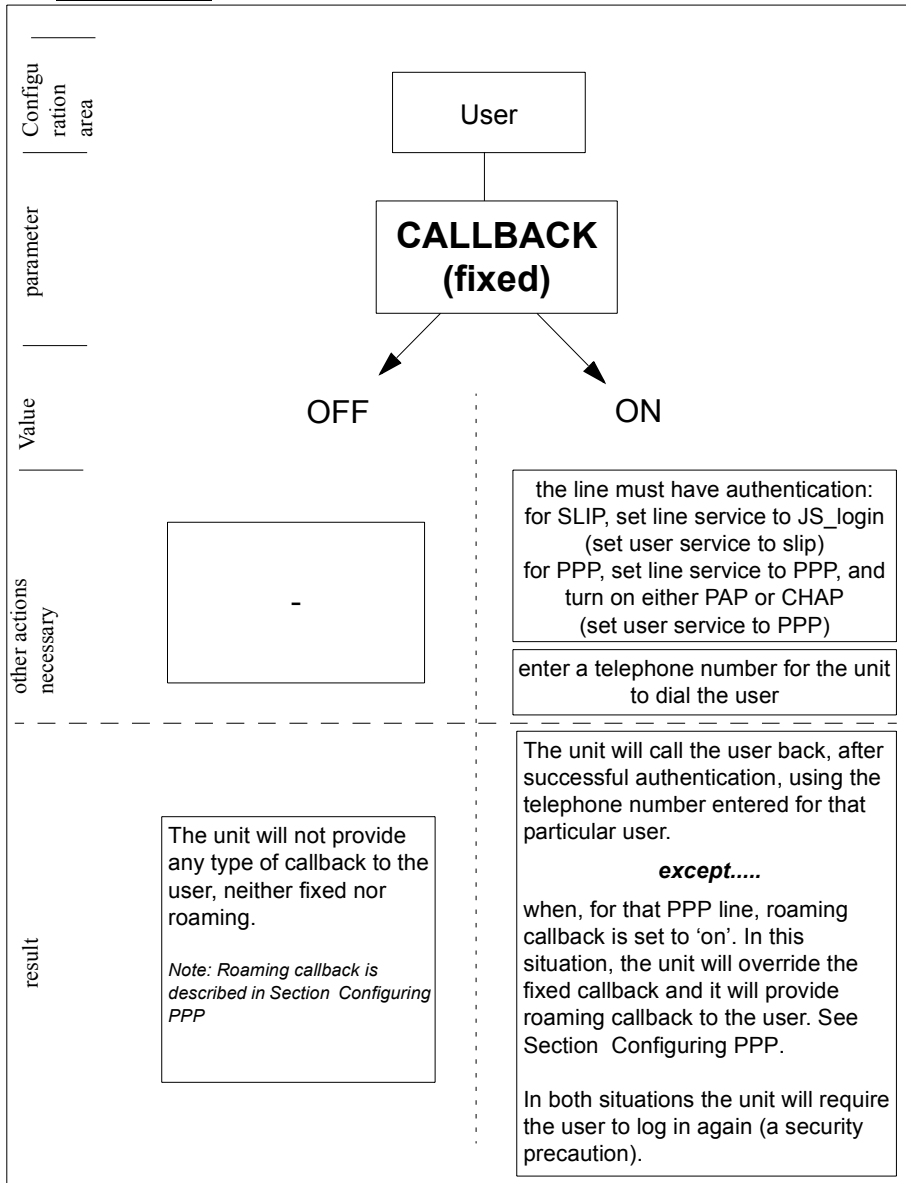
Note: this idle timer will override the idle timer which you can configure for a line.

session timer. (you may wish to change this setting for terminal server connections) enter a period in seconds for which the session timer will run. Use this timer to forcibly close a user's session (connection). When the session timer expires the unit will end the connection. The default value is 0 (zero), meaning that the session timer will not expire (the session is open permanently, or until the user logs out). The maximum value is 4294967 seconds (equal to 49 days, approximately).

Note: this session timer will override the session timer which you can configure for a line.

Language	<p>select either English or customlang (customised language); how to set up a customlang is explained in Language of your choice on page 90.</p> <p>The language change will take effect when the user next logs in to the unit. On your own account, as system administrator (default name 'admin'), the language change will take effect as soon as you accept and exit this form.</p> <p>For more information on language availability and use, see Section Language support.</p>
Level	<p>this field cycles through 'admin', 'normal' and 'restricted'. These are privilege levels and are described in Section User Levels. The 'admin' user (i.e. you as system administrator) always has 'admin' level account (maximum privileges).</p>
IP Host .	<p><i>(ignore this field unless you have selected a user service of 'telnet' or 'rlogin' or 'tcp clear').</i></p> <p>0.0.0.0 - default. The unit will use the default ip host configured for all users who login to the unit. The default ip host is set in the 'server configuration' menu; see JETSTREAM 4000, 8500, LANSTREAM 2000, Installation Guide, Section Initial Configuration (or in the cli see command 'set server'). The IP address entered here does not affect the host table or any line configuration.</p> <p>255.255.255.255 - specified by user. The unit will prompt the user for an IP address or hostname, when the telnet or rlogin service is started. When the user service is set to Telnet, Rlogin or TCP Clear, the unit will give the user two attempts the enter the required information.</p> <p>n.n.n.n - (where 'n' is a number) you specify in this field the IP address of a host with which the unit should start the telnet or rlogin service for this user.</p>
callback.	<p>(callback for a user is also known as FIXED callback) the values are either 'on' or 'off' (default is off). When 'on' enter a phone number for the unit to call the user back; see the field 'phone number'; (the callback setting is unrelated to the 'dial' parameter you can set for a line).</p> <p><i>Note:</i> the unit will only allow callback when a user is authenticated. If the protocol over the link does not provide authentication there will be no callback. Hence, when the line service is set to 'PPP' you must use either PAP or CHAP (see Configuring PPP on page 67, sub-section 'Security'), because these protocols provide authentication.</p> <p>For a diagrammatic view of callback, see Figure 16. Note that the unit supports another type of callback - ROAMING callback - which is configurable for a line when you are using the PPP protocol; see Configuring PPP on page 67.</p>

Figure 16 Callback for a user



framed ip.

(use only when the user service field is set to 'slip' or 'ppp') this is the ip address of the remote user. Enter the address in dot decimal notation as follows:

255.255.255.254 (default) - if you enter this value, the unit will use the remote ip address set for the line; see Section Configuring SLIP or Section Configuring PPP.

255.255.255.255 (when user service is set to 'ppp') - if you enter this value the unit will allow the remote machine to specify its ip address; (it therefore overrides the parameter 'ip address negotiation' which you can configure for PPP).

255.255.255.255 (when user service is set to 'slip') - if you enter this value the unit will use the remote ip address set for the line (no negotiation).

n.n.n.n - (where n is a number); enter an ip address of your choice. This ip address will then be used in preference to the remote ip address set for a line.

framed netmask. (use only when the user service field is set to 'slip' or 'ppp'). If the remote user is on a subnet, enter the subnet mask. This field is for your information only; it is not processed by the software.

framed mtu. (use only when the user service field is set to 'slip' or 'ppp') This field specifies the maximum size of packets in bytes being transferred across the link. On noisy links it may be preferable to fragment large packets being transferred over the link since there will be quicker recovery from errors. Depending on whether you have selected a user 'service' of SLIP or PPP, details are as follows:

for PPP, framed mtu will be the maximum size of packets that the the unit port will accept. This value is negotiated between the two ends of the link. The default value is 1500 bytes. Enter a value in bytes in the range 64-1500. An example value is 512 bytes; this will restrict the unit to accepting packets no greater than 512 bytes in length.

for SLIP, framed mtu will be the maximum size of packets being sent by the unit. The unit will send SLIP packets in the range 256-1006 bytes. The default value is 256 bytes. An example setting is 512: this will restrict the unit to sending SLIP packets no greater than 512 bytes in length.

The framed mtu value will be used in preference to the mtu/mru values set for a line; see Section Configuring SLIP or Section Configuring PPP.

framed compression.

(use only when the user service field is set to 'slip' or 'ppp') this parameter determines whether Van Jacobsen Compression is used on the link. Select either 'on' or 'off' (default is 'off'). VJ compression is a means of reducing the standard TCP/IP header from 40 octets to approximately 5 octets. This gives a significant performance improvement particularly when interactive applications are being used. Such an application is typing, where a single character can be passed over the link with a 40 octet header attached. VJ Compression has little effect on other types of link, such as ftp, where the packets are much larger.

The framed compression value will be used in preference to the VJ compression values set for a line; see Section Configuring SLIP or Section Configuring PPP.

3. Press <return> to exit; accept or discard the form as you wish.

Tip You may want to save your configuration changes permanently; see Section Save to non-volatile memory.

Note Changes you make in this form, as the system administrator, will only take effect for a user when the user next logs in to the unit.

If you set up any restricted users, you must predefine their sessions; they can only open sessions predefined for them by the admin user (see "Predefine User Sessions" section).

User Levels

There are four user levels which can be used to determine the level of access the user has to JETSTREAM 4000, 8500 or LANSTREAM 2000 commands:

Admin the system administrator. The admin user has total access to the unit. You can create more than one admin user account but we recommend that you only have one.

Normal (default) normal users have access to the Sessions menu only. They can start sessions, predefine sessions and change their own user environment.

Restricted these users have access to a restricted Sessions menu; they can only open sessions predefined for them by the admin user. Predefined sessions can even be configured to start automatically at login.

Menuing only be able to initiate sessions defined for that user. All other functionality is barred.

Tip You may want to save your configuration changes permanently; see Section *Save to non-volatile memory*.

CLI prompts

For admin users, the cli prompt is followed by a hash sign, for example JS_8500#. For normal and restricted users the prompt will be followed by a dollar or pound sign, for example JS_8500\$ (or JS_8500£). The display of a dollar or pound sign will vary according to the characters supported by your terminal.

Running Sessions

Note This section applies to using the unit as a Terminal Server. See Chapter 1 (Configuring a Line: Terminal Server Connections)

Users who have successfully logged into the unit (user service set to 'jsprompt') can start up to four login sessions on TCP/IP hosts. These users start sessions through the menu option 'Sessions'; see Section Running Sessions.

Multiple sessions can be run simultaneously on the same host or on different hosts. Users can switch between different sessions and also between sessions and the unit using hot-key commands; (see Section Hot-key Commands).

Users with a privilege level of 'admin' and 'normal' can predefine sessions, even configure them to start automatically on login to the unit. Users with a privilege level of 'restricted' can only start sessions predefined for them by you as the system administrator; see Section Predefining Sessions.

Predefine User Sessions

cli syntax: This option enables you to predefine up to four sessions for any user. You must predefine at least one session for each restricted user because they can only open predefined sessions.
set user

Select 'Set Sessions' from the Users menu. Select a user from the list displayed and press <return>. The Sessions form will be displayed:

Set Sessions				
Session	1	2	3	4
Type	[off]	[off]	[off]	[off]
Hostname	[socrates]	[socrates]	[socrates]	[socrates]
Termttype	[]	[]	[]	[]
Auto	[off]	[off]	[off]	[off]
Echo	[off]	[off]	[off]	[off]
Mapnl	[off]	[off]	[off]	[off]
Mode	[off]	[off]	[off]	[off]
Intr	[7f]	[7f]	[7f]	[7f]
Quit	[1c]	[1c]	[1c]	[1c]
EOF	[4]	[4]	[4]	[4]
Erase	[8]	[8]	[8]	[8]

These are the default settings. The fields after 'Auto' are telnet options.

Type 'off', 'telnet' or 'rlogin'. When not set to 'off', a predefined session will use up one of the user's 4 session slots whether active or not.

Hostname you can only predefine sessions on hosts defined in the host table. The first entry in the host table will be entered as the default.

Termttype when connecting to a UNIX host, you must define your terminal type in accordance with its UNIX TERM variable.

Auto If this field is set to 'on', the session will start up automatically when the user logs on. When more than one session is set to autostart, session 1 will be displayed first. If this field is set to 'off', the session must be started using the 'Start Predefined Sessions' option on the Sessions menu.

Tip You may want to save your configuration changes permanently; see Section *Save to non-volatile memory*.

Effect of Timers on Sessions

There is one idle timer and one session timer which apply to *all* sessions for a particular user. The respective timers are either:

- the line idle and session timers, (see Login direct to host on page 20)
or, if set,
- the user idle and session timers (see Configure a User Account on page 82)

The user timers take precedence over the line timers.

Change a User's Password

cli syntax: Select 'Set Password' from the Users menu.

set user Select a user from the list displayed.

You will be prompted to enter a password. This can be up to sixteen characters long (do not use spaces). Use the key to backspace if necessary. Enter the password and press <return>.

When prompted, re-enter the password and press <return>.

The password change will take effect next time the user logs in.

Tip You may want to save your configuration changes permanently; see Section *Save to non-volatile memory*.

Delete a User Account

cli syntax: You will be unable to delete the default admin user, users that are logged in or users dedicated to a specific line.
delete user

Select 'Delete User' from the Users menu.

Select the user that you want to delete from the list displayed.

You will be asked to confirm the deletion; type 'y' and press <return>.

The user will be deleted.

Tip You may want to save your configuration changes permanently; see Section *Save to non-volatile memory*.

Language support

This section gives you additional information about the languages you can use in the text menus/cli.

You have five other language files supplied on the supplemental diskette/CD: French, German, Italian, Spanish and Mandarin. Additionally you can use any of these language files to obtain a translation into a language of your choice. You download the language file (whether the language is supplied or translated) into the unit. You select the language option of 'customlang' (i.e. custom language); the text menus and cli then display in your language.

You can view menus/cli in one other language only (as well as English). If you download another language file, this new language will replace the first language you downloaded.

You can revert to English at any time; the English language is stored permanently in the unit and is not overwritten by your new language.

Each user logged into the unit can operate in a separate language; i.e. user A in English, User B in the 'customlang', etc.

Other Supplied languages

French, German, Italian Spanish and Mandarin language files are provided on the supplemental diskette/CD. To load one of these four languages into the unit - so that the text menus and cli appear in the language - do the following:

1. Open the supplemental diskette/CD and identify the language file; the files have intuitive names; e.g. 'french.txt' 'deutsch.txt', etc.
2. Copy the language file to a host machine on the network; place it in the main file system or on the main hard drive.

3. Either: use the TFTP defaults in the unit or, configure as necessary, TFTP in the unit; see Section TFTP configuration.

**cli syntax:
netload**

4. In the cli of the unit enter your hostname and filename; e.g

```
netload customlang socrates /temp/francais.txt
```

Do *not* enter a drive letter! Also, the path and/or filename must begin with the 'forward slash' character /

The unit will download the language file via TFTP.

set user

5. To set an individual user to the new language, go to to the Users menu and, in the language field select 'customlang'. In the cli (only) you can set individual users or all users to the new language; see the set user * command.

logout

6. The user will see the change of language when he/she logs out (Main Menu - Sessions Menu - logout) and logs back into the unit. If, as Admin user, you change your language setting to 'customlang', you will see the text menus display in the new language when you save and exit the 'Change User' form.

Notes on the supplied languages:

If you download a new software version, you can continue to use your language unchanged; however, we recommend translating the new strings - see Section Effect of Software upgade on Language Files.

A Factory Reset will reset the 'customlang' to English (factory default language).

On successful download the customlang in the unit will be overwritten by the new language.

Language of your choice

In addition to English or one of the supplied languages (see Other Supplied languages on page 89) you can display the text menus and cli in any language of your choice. Your language may use a different alphabet. Using one of the ascii language files provided on the supplemental diskette/CD you obtain a translation into your preferred language. You then download the new language file by TFTP into the unit. This new language becomes the 'customlang' (custom language).

In detail you do as follows:

1. open the supplemental diskette/CD and identify the language file which you will use for the translation. The language files contain a list of text strings which appear in the text menus and cli. An example of some text in an English language file is shown below:

```
all lines
arbitrary tcp port
alter your security level to admin
download extra language file
hostname/web address
host port
```

line number
line settings
JETSTREAM/LANSTREAM address

For further guidance on translating a language text file, see Section Translation guidance.

2. Choose a name for your new language file.
3. Copy the language file to a host machine on the network; place it in the main file system or on the main hard drive.
4. Either: use the TFTP defaults in the unit or, configure as necessary, TFTP in the unit; see Section TFTP configuration.

**cli syntax:
netload**

5. In the cli of the unit enter your hostname and filename; e.g

```
netload customlang socrates /temp/ourlang.txt
```

Do not enter a drive letter! Also, the path and/or filename must begin with the 'forward slash' character /

The unit will download the language file via TFTP.

set user

6. To set an individual user to the new language, go to to the Users menu and change their language to 'customlang'. In the cli (only) you can set individual users or all users to the new language; see the set user * command.

logout

7. The user will see the change of language when he/she logs out (Main Menu - Sessions Menu - logout) and logs back into the unit. If, as Admin user, you change your language setting to 'customlang', you will see the text menus display in the new language when you save and exit the 'Change User' form.

Notes on the customlang feature:

If you download a new software version, you can continue to use your translated language unchanged; however, we recommend translating the new strings - see Section Effect of Software upgade on Language Files.

A Factory Reset will reset the customlang to English (factory default language).

On successful download the customlang in the unit will be overwritten by the new language.

Translation guidance

To help you with your translation of supplied ascii text language files we offer the following guidance:

1. The unit will support alphabets other than English, up to a maximum of 128 characters
2. translate line for line: do not omit lines if you do not know the translation; leave the original untranslated text in place
3. maintain the same sequential order of lines; i.e. if 'all lines' is followed on the next line by 'arbitrary tcp port', do the same in your translated file

4. if a line contains only numbers, e.g. 38400, leave that line in place, unchanged (unless you are using a different alphabet)
5. if you are unsure how many characters are allowed on a line, see other text files on the supplemental diskette/CD; these files should give you guidance on line lengths. Restrict your translations of each line to the maximum number of characters allowed on that line
6. terminate each line with a carriage return

Effect of Software upgrade on Language Files

If you receive a software upgrade for the unit, the language files supplied on the supplemental diskette/CD may also have been updated. We will endeavour to provide a list of those changes in another text file on the same supplemental diskette/CD.

Note The upgrade of your software will not change the display of the language in the text menus/cli.

If you are already using one of the supplied languages (French, etc.) you may want to update the language file in the unit's memory; follow the steps detailed in Other Supplied languages on page 89. Until you update the unit's memory, new text strings (e.g. for a new parameter) will appear in English.

If you are already using a language translated from an earlier version of one of the supplied language files you may wish to amend your translation. When a language file is updated we will try to maintain the following convention:

1. new text strings (e.g. a new parameter) will be added to the bottom of the file (not inserted into the body of the existing file)
2. existing text strings - if amended - will be amended in situ; i.e. in their current position in the file
3. the existing sequence of lines will be unchanged
4. until you have the changes translated, new text strings will appear in the menus/cli in the default language (English)

Save to non-volatile memory

When you exit a text menu screen (form) after making changes, you will be presented with the 'options' form:

options
accept and exit form

If you choose to 'accept and exit form' your changes will be retained in RAM (volatile memory).

To save your changes permanently you will need to exit the text menu system completely. Return to the Main Menu and select 'command line mode'; you will be presented with a form:

```
exit full screen mode

exit and save changes

exit without saving changes

return to main menu
```

Choose 'exit and save changes'. All the changes made since last entering the menus will be saved to FLASH (permanent, non-volatile) memory.

You will now be at the command line prompt. To return the menus type:

```
screen
```

Saving to a file

cli syntax:
netsave

You can also save your configuration information to a file on a host. This can only be done in the cli; see Section `netsave`.

Chapter 5 System Administration & BOOTP

Introduction

This chapter describes the other major tasks that you - as the system administrator - may need to perform. It is divided into the following sections:

- Becoming Admin User
- Upgrading System Software
- Downloading Terminal Definitions
- TFTP configuration
- BOOTP
- DHCP Configuration and Operation
- Rebooting
- Resetting to Factory Defaults
- Remote Configuration
- Security
- Off-line Configuration
- Save Configuration to a file
- Lost Password

Becoming Admin User

normal Command: This menu option enables you to become an admin user, if you know the admin password. Prior to this action you must be a 'normal user' (the default); select 'Become Admin User' from the Sessions menu. You will be asked to enter the admin user password:

Enter Password:

You will then be logged in as the admin user. The full main menu will be displayed. Note that you cannot become a normal user unless you log out and log back in again.

Upgrading System Software

Follow the instructions in the JETSTREAM 4000, 8500, LANSTREAM 2000, Installation Guide, Section Software Upgrade.

Note that you can configure TFTP in the unit; see Section TFTP configuration.

When you have upgraded the software, existing passwords will be unchanged.

Downloading Terminal Definitions

All terminal types can be used on the JETSTREAM 4000, 8500 or LANSTREAM 2000 (the 'unit'). Terminal types which are not defined on the unit, however, are unable to use Full Screen mode (menus) and may not be able to page through sessions properly. When installed, the unit has three defined terminal types - Wyse60, VT100 and Ansi.

If you are not using, or cannot emulate, any of these terminal types, you can add up to three additional terminal definitions to the unit. The terminal definitions can be downloaded from a TCP/IP host.

Three sample terminal definitions are supplied on the Supplemental disk/CD supplied with the unit. These are TVI950, IBM3161 and Adds Viewpoint.

To download terminal definitions, follow these steps:

1. Decide which TCP/IP host you are going to use. It must be a UNIX machine and must have *tftp* enabled.
2. Configure *tftp* in the unit as necessary; see Section TFTP configuration.
3. Tar the sample files from the Supplemental disk/CD onto the boot host. They are called ET.tvi950, ET.addsvp and ET.ibm3161. Copy them to a directory of your choice. Make sure they have global read and execute permission for their entire path.
4. If you need to create your own terminal definition files, refer to Creating Terminal Definition Files on page 97. Copy them to a directory of your choice. Make sure they have global read and execute permission for their entire path.

Note *if you are using tftp with the secure option, i.e. "tftpd -s /tftpboot", create a directory under /tftpboot/ and place the term files in this directory.*

cli syntax:
netload

5. Exit the menus, go into the cli and use the `netload` command; refer to `netload` on page 165 for information on this command.

set line

6. You can stay in the cli or re-enter the menus. In the menus go to the line configuration menu, then the line settings sub-menu and select a particular line. From the line parameters displayed go to the 'terminal' field and press L (for 'list'; upper or lower case). You should see:

```
terminal
wyse60
vt100
ansi
dumb
term1
term2
term3
```


7. select one of term1, term2 or term3; (these definitions default to Wyse60). Your downloaded terminal definition is either 'term1', 'term2' or 'term3' (as specified when you used the 'netload' cli command).
8. To copy this new term type to all other lines, press <return> and follow the screen prompts. See Copy settings to other lines on page 26 for more information.

Tip *If you have problems using arrow keys using a downloaded terminal definition, you can use Ctrl-K, Ctrl-J, Ctrl-H and Ctrl-L for up, down, left and right respectively.*

Creating Terminal Definition Files

To create new terminal definition files, you need to copy and edit the information from the terminfo database.

1. On the UNIX host, change directory to /usr/lib/terminfo/x (where x is the first letter of the required terminal type). For a Wyse60, for example, you would enter the command **cd /usr/lib/terminfo/w**
2. The termcap files are compiled, so use the command **infocmp termfile** to read the required file (for example: **infocmp wy60**).
3. Check the file for the attribute **xmc#n** (where n is greater than or equal to 1). This attribute will corrupt menu and form displays making the terminal type unsuitable for using Full Screen mode.
4. If the terminal definition is suitable, change to a directory of your choice.
5. Rename and copy the file to the directory specified at step 4. using the command **infocmp termfile > termn** where n is greater than or equal to 1; (e.g. **infocmp wy50 > term1**). Make sure the file has global read and execute permission for its entire path.
6. Edit the file to include the following capabilities in this format:

```
term=
acsc=
bold=
civis=
clear=
cnorm=
cup=
rev=
rmacs=
rmso=
smacs=
smso=
page=
circ=
```

For example:

```
term=AT386 | at386 | 386AT | 386at | at/386 console
acsc=jYk?lZm@qDtCu4x3
bold=\E[1m
civis=
clear=\E[2J\E[H
```

```

cnorm=
cup=\E[%i%p1%02d;%p2%02dH
rev=\E4A
rmacs=\E[10m
rmso=\E[m
smacs=\E[12m
smso=\E[7m
page=
circ=n

```

Note As you can see from the example, capabilities which are not defined in the terminfo file must still be included (albeit with no value). Each entry has an 80 character limit.

On some versions of UNIX, some of the capabilities are appended with a millisecond delay (of the form `$<n>`). These are ignored by the unit and can be left out.

The ‘acsc’ capability, if defined, contains a list of character pairs. These pairs map the characters used by the terminal for graphics characters to those of the standard (VT100) character set.

Include only the following character pairs:

jx, kx, lx, mx, qx, tx, ux and xx

(where *x* must be substituted by the character used by the terminal). These are the box-drawing characters used to display the forms and menus of Full Screen mode. They must be entered in this order.

The last two capabilities will not be found in the terminfo file. In the ‘page’ field you must enter the escape sequence used by the terminal to change screens. The ‘circ’ field defines whether the terminal can use ‘previous page’ and ‘next page’ control sequences. It must be set to ‘y’ or ‘n’. These capabilities can be found in the documentation supplied with the terminal.

TFTP configuration

cli syntax:
set server tftp

You can configure TFTP in the JETSTREAM 4000, 8500 or LANSTREAM 2000 (the ‘unit’). It is used for transferring files to/from a host; the files could be, for example, configuration, new software or custom language files. From the Network Configuration Menu, select ‘tftp’; you should see the following:



```

+tftp+
  retry[5]
  timeout[3]

```

retry should tftp fail, retry is the number of retries the unit will make to transfer a file to/from a host. Enter a value between 0 and 255. The default value is 5. A value of 0 means that the unit will not attempt a retry.

timeout is the time in seconds the unit will wait for successful transmit or receipt of tftp packets before retrying a transfer. Enter a value between 1 and 255. The default value is 3.

BOOTP

5.0.0.1 Contents of BOOTP section

- Overview
- How to setup BOOTP,
the bootptab file entry
the bootfile
- BOOTP messages output to screen
- Disabling the BOOTP reply
- Booting multiple units
- Multiple BOOTP servers
- Example of BOOTP

Introduction

You can use BOOTP to perform the following actions on a single or multiple JETSTREAM 4000, 8500 or LANSTREAM 2000 (the *unit(s)*)s on its/their boot-up:

- auto-configure with minimal information; e.g. only an ip address
- auto-configure with basic setup information (ip address, subnet mask, broadcast address, etc.)
- download a new version of software
- download a full configuration profile (saved from another unit)

BOOTP is particularly useful for multiple installations: you can do all the unit's configuration in one BOOTP file, rather than configure each unit manually.

Another advantage of BOOTP is that you can connect a unit to the network, turn on its power and let auto-configuration take place. All the configuration is carried out for you during the BOOTP process.

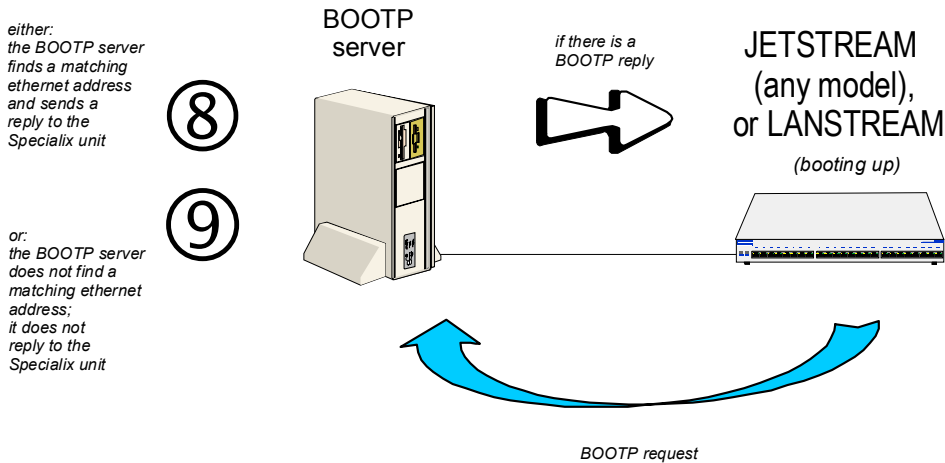
The the unit's implementation of BOOTP is compatible with RFC 951; see Appendix D (References) for detail on this RFC.

Overview

On bootup or power-up, the unit will send a broadcast request to the BOOTP server(s) on the network. The request contains the ethernet address of the unit; it asks for network configuration details (internet address, subnet mask, etc.). This process is shown in Figure 17.

You can stop the BOOTP server from replying to the unit; see Disabling the BOOTP reply on page 106

Figure 17 BOOTP request and response



The BOOTP server checks the ethernet address and looks for a matching address in its boottab file:

- if a matching ethernet address is found the BOOTP server will reply to the unit; the reply will contain network configuration information. This information is listed in the boottab file for that particular unit (identified by its hardware address). The unit then boots using the information sent to it.
- if no matching ethernet address is found the BOOTP server does not reply; the unit boots from internal memory.

Refer to Figure 18 for an explanation of the following text:

the BOOTP response contains network configuration information; e.g. ip address, subnet mask, broadcast address. It may also contain details of a bootfile (not mandatory)

a bootfile (if you specify one) contains a unit's specific boot information; e.g. authentication method of users, access permission for the GUI. It may also contain details of other files (not mandatory); e.g. software version, language files and a general configuration file

a configuration file (if you specify one) contains general configuration parameters; these parameters will have been created from another unit and saved to a file

in the bootp response the minimum parameters to specify are **:ht** and **:ha**

there is no minimum number of parameters to specify in the bootfile or configuration file; unspecified parameters will remain unchanged in the unit's memory

After processing the BOOTP response the unit will download additional files, as follows:

- if a bootfile is specified, the unit will then download that bootfile (using tftp).

if the bootfile specifies other files e.g. a software file, the unit will compare that filename with the filename in its memory; if it has changed the unit will then download that other file using tftp. If the filename has not changed the unit will not download it.

Note In the bootp response you do not have to specify a bootfile. In the bootfile you do not have to specify other files, such as the software file. If you wish, you can make an entry in the bootptab file only.

Figure 18 the files used in the BOOTP process

Entry for the unit in bootptab file...

```
js8500_blue:\
:ht=1:\
:ha=0080ba000057:\
::bf=/tmp/8500p.bfc:\
:ip=192.101.34.211:\
:ds=192.65.144.44:\
:sm=255.255.255.224:\
:hn:\
:dn=perle.com:\
:gw=192.101.35.254:\
:vm=rfc1048:
```

Boot file named '8500p.bfc'....

```
# cat 8500p.bfc
GUI_ACCESS      yes
SECURITY        no
AUTH_TYPE       0
IP_HOST         192.101.34.199
TFTP_RETRY      3
TFTP_TIMEOUT    21
CUSTOM_LANG     SWEDISH
EXTRA_TERM1     192.65.144.95:/src/pscx/et/et1.0183
EXTRA_TERM2     192.65.144.95:/src/pscx/et/et2.0183
EXTRA_TERM3     192.65.144.95:/src/pscx/et/et3.0183
SW_FILE         192.65.144.95:/src/pscx/js8500.bin
CONFIG_FILE    192.65.144.95:/src/pscx/cfg/jconfig.01
#
```

software file js8500.bin....

configuration file config.01....

compiled software for loading into FLASH memory on the unit

a copy of the configuration parameters saved from a unit onto a host; excludes parameters unique to the original unit. This file can be downloaded to any unit.

How to setup BOOTP

Your nominated BOOTP server should be on the same network as the the unit(s). The BOOTP server can also be on a different segment of the same network, provided that segment is connected by a bridge.

You can locate your BOOTP server on another network to the unit; this means that the bootp request and replies have to pass through a router or gateway. You must configure your router or gateway:

- to pass through BOOTP requests and replies
- for RIP

Note that if you have an existing unit, you do *not* have to enter the details of the gateway or router into the unit before using bootp. Details of gateways or routers pre-configured in the unit will be ignored during the bootp process.

5.0.0.2 the bootptab file entry

Find the bootptab file on the host; on UNIX systems the bootptab file is usually file /etc/bootptab. Make an entry for the unit; an example for a single unit is shown at Figure 19. An example for multiple units is shown at Figure 21.

Figure 19 bootptab file entry for a single unit

```
js8500_blue:\

:ht=1:\
:ha=0080ba000057:\
:ip=192.101.34.211:\
:ds=192.65.144.44:\
:sm=255.255.255.224:\
:hn:\
:bf=/tmp/8500p.bfc:\
:dn=perle.com:\
:gw=192.101.35.254
```

This entry should include the ethernet address of the unit. Other standard BOOTP tags which the unit supports are listed below, together with the unit's interpretation:

ht (hardware type) set to 1 (=10Mb ethernet).
ha (hardware address) the ethernet address of the unit.

- ip** (internet address) enter the ip address to assign to the unit.
- sm** (subnet mask) enter the subnet mask of the unit.
- hn** (host name) enter as :hn:\ which causes the name at the start of the file (js8500_blue) to be allocated to this unit.
- bf** (bootfile name) enter the name of the file containing specific configuration information; see Figure 20.
- ds** (domain servers) enter the ip address of up to two nameservers.
- gw** (gateway) enter the ip address of a single passive gateway

Caution

use the 'gw' flag only in very specific circumstances; see Note 5. below.

Notes on the above BOOTP tags:

1. Specify the fields that you wish; you do not have to specify all of them. E.g. if you wish to download only the internet address to the unit, specify the **ip** field (you must specify - as a minimum - the **ha** and **ht** fields).
2. If the subnet mask (**sm**) has not been explicitly specified by a BOOTPREPLY packet, it will be derived from the class of internet address.
3. If domain name servers are specified their port number will always be set to the default for a name server (53).
4. If you require a bootfile (**bf**) it must be on the same host as the bootptab file entry.
5. include the **gw** (gateway) flag only if your BOOTP server is on a different network and your gateway (or router) is *not* configured to support RIP.

The effect of using the '**gw**' field is:

- to make only this gateway available in the unit; it will be a passive gateway. You can view the details of the gateway only in the cli, using the 'show routes' command.

- to turn off RIP in the unit; i.e. the unit will ignore RIP messages broadcast on the network

- the unit will ignore gateways pre-configured in the unit or added after boot-up. It will respond only to the single gateway.

- you delete the gateway as follows: omit the '**gw**' field in the bootptab file entry and re-boot the unit. You can now add/configure active and passive gateways into the unit.

Gateways are detailed in the 8500 Installation Guide, Chapter 2 (Initial Set-up). An overview of RIP is given in Appendix D (RADIUS & Networking) of the same Guide.

5.0.0.3 the bootfile

If you wish to download basic configuration information to the unit you must create a bootfile. This file is a text file formatted in a particular style; an example is shown at Figure 20.

Note *The bootfile must be located on the same host as the bootptab file*

Figure 20
An example bootfile

```
# cat 8500p.bfc

SW_FILE192.65.144.95:/src/pscx/sw/js8500.bin
CONFIG_FILE192.65.144.95:/src/pscx/cfg/jconfig.0183
GUI_ACCESSYes
AUTH_TYPE0
IP_HOST192.101.34.199
SECURITYno
TFTP_RETRY3
TFTP_TMOU21
CUSTOM_LANG192.65.144.7:/etc/js/config/js8500_blue/polish
EXTRA_TERM1192.65.144.95:/src/pscx/et/et1.0183
EXTRA_TERM2192.65.144.95:/src/pscx/et/et2.0183
EXTRA_TERM3192.65.144.95:/src/pscx/et/et3.0183

#
```

Notes on the above example:

1. The bootfile can have line entries for other files, e.g. a software or configuration file. The unit will download these files only if the filename has changed (excludes the pathname).
2. The format of each line entry in the file is:
PARAMETER_NAME <white space> parameter value
<carriage return/line feed>
3. The parameter name must be in UPPER CASE and match exactly the strings shown in Figure 20; e.g. AUTH_TYPE and CUSTOM_LANG.
4. An explanation of these parameters is shown in Table 3.
5. Include only those parameters which you want to configure. For example you may not wish to download a configuration file, so omit the line beginning CONFIG_FILE (or precede the line with a hash # character).
6. If a domain name and nameserver are configured, either in the bootptab entry or in the unit's memory, you can replace ip addresses with hostnames in lines specifying additional files; e.g.

```
SW_FILESophocles:/src/pscx/sw/js8500.bin
```

Table 3 Bootfile parameters

Parameter	Value	Brief Meaning	Fuller explanation
SW_FILE	a filename and a full pathname - all pre-fixed by hostname/ip address	a version of software	8500 Installation Guide, Section Using TFTP from a host

Parameter	Value	Brief Meaning	Fuller explanation
CONFIG_FILE	a filename and full pathname - all pre-fixed by hostname/ip address	a set of saved configuration parameters from an existing unit. Note: these parameters include user passwords.	configuration parameters which are not listed in the BOOTPTAB file entry or in the bootfile. The relevant configuration parameters are listed in Section netsave. The parameters will not overwrite network configuration parameters specified in your bootfile.
GUI_ACCESS	on, off	access to the unit from a web browser	8500 Installation Guide, Section Initial Configuration
AUTH_TYPE	both, local or radius	authentication method employed by the unit for all users	8500 Installation Guide, Section Initial Configuration
IP_HOST	ip address in dot decimal notation	default ip host for a user when user service is set to 'telnet' 'rlogin' or 'tcp clear'	Section Configure a User Account
SECURITY	on, off	'reverse' line types, 'printer' line type and remote configuration - all restricted to devices listed in the the unit's host table	Section Security
TFTP_RETRY	numeric; e.g. 5	number of tftp attempts before aborting	Section TFTP configuration
TFTP_TMOU	numeric; e.g. 3	period in seconds before retrying a download/upload	Section TFTP configuration
CUSTOM_LANG	a filename and full pathname pre-fixed by hostname/ip address	name of a translated language file	Section Language of your choice

Parameter	Value	Brief Meaning	Fuller explanation
EXTRA_TERM1 (or 2, or 3)	a filename and full pathname - all prefixed by a hostname/ip address	termcap files for specific terminal types	Section Creating Terminal Definition Files

BOOTP messages output to screen

The unit will output BOOTP messages to your screen during bootup, provided you are connected to the unit via its Admin Port. Information on using the Admin Port is detailed in the 8500 Installation Guide, The Admin Port on page 37.

On bootup the unit will always send a BOOTP request to BOOTP servers, so you will see the message:

```
INIT: attempting BOOTP
```

If the unit does not receive a BOOTP reply you will see the message:

```
INIT: no bootphost/server found on this network
```

If you want the unit to boot from a BOOT server then this message means BOOTP is not working. Consult Section BOOTP/DHCP problems for help.

Disabling the BOOTP reply

You cannot disable BOOTP in the unit; however, you can stop the BOOTP host from sending a BOOTP reply to the unit. You stop the reply by placing a hash # character in the bootptab file entry as follows:

- in Figure 19, place a hash before all the lines, e.g.

```
# :ht=1:\
# :ha=0080ba000057:\
..
# :gw=192.101.35.254:\
```

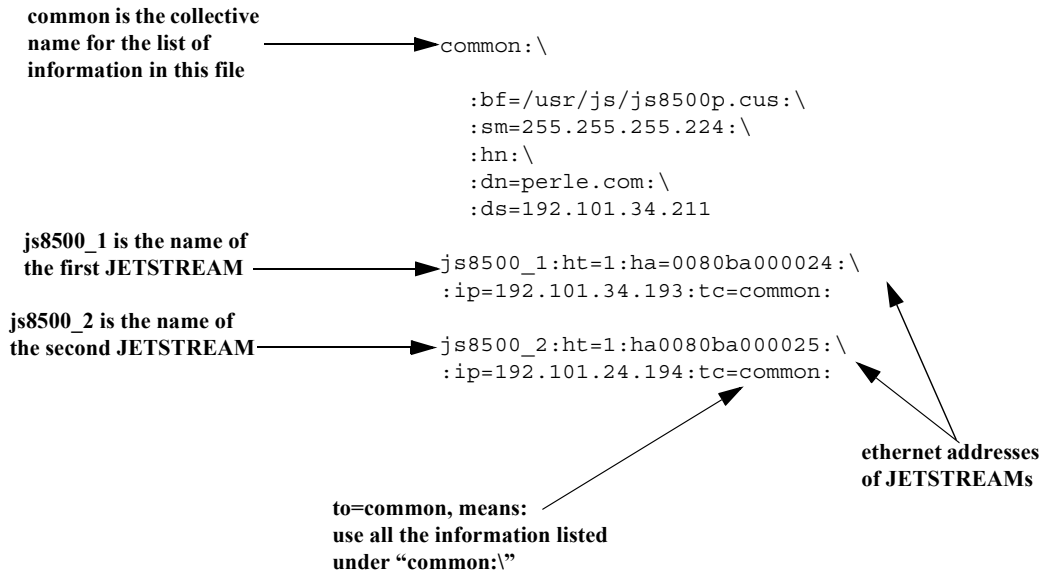
- in Figure 21 you would place a hash before the line referring to each JETSTREAM; e.g:

```
# js8500_2:ht=1:ha=0080ba000025:\
# ip=192.101.34.194:tc=common:
```

Booting multiple units

You can boot multiple unit's simultaneously using BOOTP; we recommend you alter the format of your bootptab file entry, as shown in Figure 21. You make one set of parameters in a single area (in this example 'common') and point each unit's entry to this area called 'common'.

Figure 21 bootptab file entry for multiple units



Notes on the above figure:

1. The example shown is for the JETSTREAM 8500.
2. List each unit at the bottom of the file.
3. So that all units use the same BOOTP information, terminate each unit's entry with the same syntax, using the format `tc=name` (in the example above `tc=common`).
4. You will see that all the unit's are being directed towards the same bootfile (as listed in the 'bf' field in the area 'common'). This is acceptable - however all your the unit's will have the same configuration parameters.
5. The bootfile must be on the same host as the bootptab file entry.

Multiple BOOTP servers

You may well wish to have a secondary BOOTP server as a back-up to the primary BOOTP server.

The unit will operate with BOOTP when you have a second, third or more BOOTP servers on your network. During a reboot the unit processes the first BOOTP reply received and ignores subsequent replies. If the bootptab file entries are identical on all your BOOTP servers the first reply received by the unit will be the same as the other replies.

The rules for multiple BOOTP servers are:

- we recommend they are located on the same network; however if they are on different network see the advice at How to setup BOOTP on page 102
- if you specify a bootfile (**bf**), each BOOTP server must contain an identical copy of this bootfile
- the software file (SW_FILE) and/or configuration file (CONFIG_FILE) can be located on any host; they do not have to be on the BOOTP server machines

Example of BOOTP

Here is a working example of BOOTP, used to download a new version of software. We are using tftp with the 'secure' option:

1. If possible choose a BOOTP server which is located on the same network as the unit. Our BOOTP server was located like this.
2. Enable BOOTP on the machine you have chosen as the BOOTP server. E.g. on our SCO Open Server 5 machine we modified file /etc/inetd.conf, as follows:

```
tftp dgram udp wait root /etc/tftpd tftpd -s /tftpboot
bootps dgram udp wait root /etc/bootpd bootpd -c/tftpboot
```
3. Reboot the BOOTP server to ensure that BOOTP is operating.
4. Make an entry in file /etc/bootptab for your unit; e.g.

Figure 22
Our example entry in a BOOTPTAB file

```
js8500_3:\

:ht=1:\
:ha=0080BA00004b:\
:ip=192.65.146.120:\
:ds=192.165.144.6:\
:sm=255.255.255.0:\
:hn:\
:bf=/test:\
:dn=specialix.co.uk
```

5. Create the bootfile specified in the above entry; i.e. file 'test':

Figure 23
Our example bootfile

```
# cat test

SW_FILE192.65.146.71:/js8500.fl5
GUI_ACCESSyes
AUTH_TYPE0
IP_HOST192.65.146.71
SECURITYno
TFTP_RETRY3
EXTRA_TERM1homer:/src/pscx/et/et1.0183
EXTRA_TERM2homer:/src/pscx/et/et2.0183
EXTRA_TERM3homer:/src/pscx/et/et3.0183

#
```

6. In the bootfile (above) we specified the software file(SW_FILE). Specify the pathname for the file; in our example we placed the software file in the same directory as the bootfile.
7. Reboot the unit. After receiving details from the bootptab file, the unit should download the bootfile and the software file. The unit should then place the new software file into FLASH memory.

DHCP Configuration and Operation

The DHCP protocol provides an industry standard alternative to BOOTP and provides a more sophisticated method of managing IP addresses and configuration parameters. It should be particularly useful when managing the unit from a Windows NT server environment and some versions of UNIX such as UnixWare 7.

DHCP is a superset of the BOOTP configuration service which it completely replaces. DHCP is backward compatible with BOOTP in that the entire suite of BOOTP tags is supported within DHCP. DHCP is now often used in favor of BOOTP as it is supported on a wide range of network operating systems, however to ensure compatibility with existing installations, the JETSTREAM 4000, 8500, or LANSTREAM 2000 (the 'unit') will continue to fully support BOOTP.

The major differences between BOOTP and DHCP are:

- BOOTP is largely reliant on a network client's low level Ethernet address (MAC address) for client information look-up, DHCP has no such limitation, although it is still possible to associate a specific IP address to a specific MAC address.
- Client information supplied by DHCP is supplied on a lease basis, that is to say that the client negotiates with the server for the lease of an IP address for a specific period of time. This allows for the allocation of a fixed pool of client addresses that are allocated by the DHCP server on a "first come first served" basis.

No additional configuration is required in the unit to enable DHCP, however your network server will need to have it's DHCP service configured for JETSTREAM or LANSTREAM clients and if boot file download is required, then the TFTP service should be configured and running. DHCP/BOOTP can also be disabled completely by setting the configurable server dhcp parameter to off. See Section 1.6 for details.

The administrative interface to the DHCP sever manager depends on the operating system running on your network server and is beyond the scope of this document. Consult your system documentation for details of configuring the DHCP service on your server's operating system.

How to setup BOOTP on page 102 (How to set-up BOOTP) describes in detail the BOOTP/DHCP tags (client information items) that are supported by both BOOTP and DHCP. In addition on Microsoft Windows NT, DHCP allows for the configuration of WINS server names.

If automatic configuration of JETSTREAM/LANSTREAM clients is required, only one service DHCP, BOOTP or RARP should be enabled on your network server.

We strongly recommend that you do not run both the BOOTP and DHCP services on the same network to configure JETSTREAM/LANSTREAM clients unless you are very familiar with the potential interactions that may result.

Rebooting

cli syntax: From the Network Configuration menu select 'Reboot'. You will be asked whether you wish to save your
reboot configuration changes to non-volatile memory:

```
Save config to FLASH ROM (y/n)
```

The unit will close all connections and then reboot.

Note As installed from SCO, TCP/IP for SCO XENIX will not allow the unit to reboot across the network. This problem can be resolved by a simple modification to **the file /etc/inetd.conf**. The line that reads:

```
tftp dgram udp wait sync /etc/tftpd tftpd
```

should be changed to:

```
tftp dgram udp wait root /etc/tftpd tftpd
```

Resetting to Factory Defaults

cli syntax: This feature enables you to reset the unit to its default settings. This will clear all configuration data entered
reset factory by the admin user, and all user accounts, except the default admin user, will be deleted. Select 'Reset' from the Network Configuration menu; you will be asked to confirm the reset:

```
Confirm reset to factory defaults (y/n)
```

Type 'y' to reset the unit, 'n' to cancel the command.

Remote Configuration

Using JETset

The easiest way to configure the unit remotely is to connect to the unit from your web browser and use the JETset program.

Telnet

You can also start a telnet session on the unit's telnet port (23) from another host on the network. No prior configuration is necessary to use this feature; two such sessions can be run simultaneously. You will be prompted for a login name and password. All functionality will be available except the ability to access other hosts. You can use Full Screen mode if you use a terminal type defined on the unit.

The unit has a security feature which enables you to restrict incoming connections to only those hosts defined in the host table. This is described in Section Security.

SNMP

Using network management software you can configure the unit remotely from a host or other networked computer. See Chapter 6 (SNMP) for more information.

Security

cli syntax: set server

The remote access features of the JETSTREAM 4000, 8500 or LANSTREAM 2000 (the '*unit*') mean that you access the unit over a network from other hosts or devices. Remote access features are remote configuration, reverse and printer line types. To help prevent unauthorised access, the unit includes a security feature which enables you to restrict incoming connections to those hosts or devices defined in the host table. This feature is enabled/disabled using the 'Security' option on the Network Configuration menu.

The 'security' and 'gui access' parameters are unrelated.

Off-line Configuration

A unit can be configured by:

- Downloading a configuration file from an attached host. See netload on page 165 for information on how to load a JETSTREAM/LANSTREAM configuration file.
- Including a reference to a configuration file (CONFIG_FILE) in the 'Boot' file, referenced by the 'bootptab' file in the BOOTP/DHCP response, see Overview on page 99 for further details. This method allows for the complete configuration of the unit by JETstart and BOOTP/DHCP.

The CONFIG_FILE can be created by saving the configuration of an existing unit, see Save Configuration to a file on page 113, or by using **JETstart**.

JETstart is a Java applet specifically designed for producing configuration files for JETSTREAM4000, 8500 and LANSTREAM2000 units. JETstart will only run in a Java enabled browser. It works by asking context sensitive questions about the intended use of your unit, and uses this to create a configuration file which can be downloaded into the unit.

Note *JETstart is a service and line configuration program and is not designed to configure the JETSTREAM/LANSTREAM server parameters (such as server IP address, WINS, DNS etc.), please use BOOTP/DHCP or manual configuration for these items.*

Running JETstart

JETstart has been developed using the Java Development Kit v1.1.6 and is therefore only supported by Netscape Navigator version 4.05, and later, and Microsoft Internet Explorer version 4.0, and later.

1. To open JETstart in your browser, double-click the file **Jetstart.htm** on the Perle CDROM.
2. Within the JETstart page, click the **JETstart** button, at the bottom left of the window, to enter the configuration applet.
3. The first configuration screen allows you to select the type of connection you want for each line:
Terminal serverTS
Remote access serverRAS
PrinterPR
Serial port emulationSPE
4. You are then requested screen-by-screen to define the parameters for each connection type.
5. The last screen prompts you to save the configuration information as a file, which can then be downloaded to one or more Jetstream/Lanstream units.

Security

JAVA applets running in browsers are subject to restrictions on file I/O, network connections etc., as imposed by the browser's security policy. JETstart requires the ability to write a file to disk, and to display a file dialog box, in order to save the generated JETSTREAM/LANSTREAM configuration file to your computer.

5.0.0.4 Netscape 4.05 (and later)

If you are running Netscape Navigator, you will be asked if you want to grant the applet permission to write a file. Click the Grant' button.

5.0.0.5 Internet Explorer 4

If you are running Microsoft Internet Explorer under Windows NT or 95, you will need to run the Registry Editor, (for example run regedit.exe) and add the path of the file wizard.zip (which is in your installation directory) to the Classpath key in HKEY_LOCAL_MACHINE\Software\Microsoft\Java VM, eg. append ;C:\jetstart\wizard.jar to Classpath (if wizard.jar is installed in C:\jetstart).

Additionally, adjustments to the security policy should be made from the browser, enabling File Dialog creation and file I/O as follows:

1. From the 'View' menu, choose 'Internet Options'
2. Select the 'Security' tab
3. Select 'Local intranet zone' from the 'Zone' selection box
4. Click the 'Custom' radio button
5. Click the 'Settings' button
6. From the 'Java Permissions' subsection of the 'Java' section, click the 'Custom' radio button
7. Click the 'Java Custom Settings' button
8. Choose the 'Edit Permissions' tab
9. In the section 'Unsigned Content', subsection 'Run Unsigned Content', subsection 'Additional Unsigned Permissions', click the Enable radio button for 'Access to all files' and 'Dialogs'
10. Click 'OK'
11. Click 'OK'
12. Click 'Apply'
13. Click 'OK'

5.0.0.6 HotJava

If you are running Sun's HotJava, from the Edit menu, choose Preferences then Applet Security. Set Default settings for Unsigned Applets to Medium Security. You will now be prompted to permit file I/O when saving the configuration.

Save Configuration to a file

cli syntax:
netsave,
netload

You can save the configuration of your JETSTREAM 4000, 8500 or LANSTREAM 2000 (the '*unit*') to a file on a remote host using TFTP. You can use this configuration file to configure other units.

The following information will be saved:

- User Profiles, including passwords
- Port Configuration
- Host Table
- Gateways

RADIUS details

Modems

SNMP

Information unique to this unit (name, ip address) will not be saved. Make sure you have write permission to the file. You can configure tftp in the unit; see Section TFTP configuration.

Caution

Passwords remain with a configuration file. When you download a new configuration file make sure you know the passwords in that file.

Lost Password

If you are an admin user, and you lose your password, there is no way of logging in without it. This restriction is for security reasons. Unless there is another user with admin level privileges (who will have the ability to change your password) you will have to reset the JETSTREAM 4000, 8500 or LANSTREAM 2000 (the *'unit'*) to its factory default settings.

cli syntax:
set user

If a user forgets his/her password, you can assign a new password; go to the Users Menu and select 'set password'.

Chapter 6 SNMP

Introduction

This chapter describes the JETSTREAM 4000, 8500 or LANSTREAM 2000 (the ‘unit’) support of SNMP.

Chapter contents

This chapter is divided into the following sections:

- Overview
- Configuring SNMP support
- Summary of Objects in the JS8500 Private MIB
- JS8500 Private MIB Definitions
- Network Management

Overview

The Simple Network Management Protocol (SNMP) is a protocol for access and control of network management information on TCP/IP networks. JETSTREAM 4000, 8500 or LANSTREAM 2000 (the ‘unit’) provides an SNMP agent, able to respond to SNMP requests generated by SNMP Managers. The unit’s implementation of SNMP is compatible with MIB II (RFC 1213) as specified by the SNMP SMI document (RFC1155). For a full description of SNMP, refer to your SNMP documentation.

Enterprise-specific parameters are defined by the unit’s Private MIB, known as the JS8500 Private MIB (the LANSTREAM uses the same MIB). Summary of Objects in the JS8500 Private MIB on page 116 gives a summary of the objects defined by this MIB. The full version of the MIB is in Table 5.

Configuring SNMP support

From the Main Menu select ‘network configuration’ and then ‘snmp’.

cli syntax:
set contact
set location

Select ‘snmp contact information’ to configure the SNMP sysContact and sysLocation objects; an example screen is shown below:

```
          +-----+
contact   location
[miked   ] [red ]
```

add trap
delete trap

Select 'edit traps' to create up to four trap communities; an example screen is shown below:

```

+traps+
trap      internet address
[pink    ][192.65.144.190 ]
[turquoise][192.65.144.191 ]
[        ][          ]
[        ][          ]

```

SNMP Trap messages generated by the unit will only be broadcast to hosts defined by SNMP Trap communities.

Note The unit generates no enterprise-specific traps.

add community
delete community

Select 'edit communities' to create up to four communities; an example screen is shown below:

```

+communities+
community internet address permissions
[public   ][192.65.144.199 ] [none   ]
[netman   ][192.65.144.192 ] [readonly]
[        ][          ] [none   ]
[        ][          ] [none   ]

```

The unit's SNMP Agent will only provide information to hosts defined by an SNMP community.

Summary of Objects in the JS8500 Private MIB

Table 4

OBJECT NAME	ADDRESS	TYPE	PERMISSIONS
ServerInfo	1.3.6.1.4.1.667.2.1	Aggregate	not-accessible
freeSpace	1.3.6.1.4.1.667.2.1.1	Guage	read-only
swVersion	1.3.6.1.4.1.667.2.1.2	DisplayString	read-only
serverName	1.3.6.1.4.1.667.2.1.3	DisplayString	read-only
domaiName	1.3.6.1.4.1.667.2.1.4	DisplayString	read-only
portsInfo	1.3.6.1.4.1.667.2.2	Aggregate	not-accessible
portsNumber	1.3.6.1.4.1.667.2.2.1	INTEGER	read-only
portsInfoTable	1.3.6.1.4.1.667.2.2.2	Aggregate	not-accessible
portsInfoEntry	1.3.6.1.4.1.667.2.2.2.1	Aggregate	not-accessible
portId	1.3.6.1.4.1.667.2.2.2.1.1	INTEGER	read-only
terminalType	1.3.6.1.4.1.667.2.2.2.1.2	INTEGER	read-write
baudRate	1.3.6.1.4.1.667.2.2.2.1.3	INTEGER	read-write
dataBits	1.3.6.1.4.1.667.2.2.2.1.4	INTEGER	read-write

OBJECT NAME	ADDRESS	TYPE	PERMISSIONS
parity	1.3.6.1.4.1.667.2.2.2.1.5	INTEGER	read-write
stopBits	1.3.6.1.4.1.667.2.2.2.1.6	INTEGER	read-write
pages	1.3.6.1.4.1.667.2.2.2.1.7	INTEGER	read-write
defaultUser	1.3.6.1.4.1.667.2.2.2.1.8	INTEGER	read-write
validUser	1.3.6.1.4.1.667.2.2.2.1.9	INTEGER	read-write
dial	1.3.6.1.4.1.667.2.2.2.1.10	INTEGER	read-write
flowControl	1.3.6.1.4.1.667.2.2.2.1.11	INTEGER	read-write
service	1.3.6.1.4.1.667.2.2.2.1.12	INTEGER	read-write
hostPort	1.3.6.1.4.1.667.2.2.2.1.13	INTEGER	read-write
localPort	1.3.6.1.4.1.667.2.2.2.1.14	INTEGER	read-write
host	1.3.6.1.4.1.667.2.2.2.1.15	INTEGER	read-write
pinDCD	1.3.6.1.4.1.667.2.2.2.1.16	INTEGER	read-only
pinDTR	1.3.6.1.4.1.667.2.2.2.1.17	INTEGER	read-only
pinRTS	1.3.6.1.4.1.667.2.2.2.1.18	INTEGER	read-only
charSends	1.3.6.1.4.1.667.2.2.2.1.19	Counter	read-write
charReceiveds	1.3.6.1.4.1.667.2.2.2.1.20	Counter	read-write
phoneNumber	1.3.6.1.4.1.667.2.2.2.1.21	DisplayString	read-only
modemName	1.3.6.1.4.1.667.2.2.2.1.22	DisplayString	read-only
idleTimer	1.3.6.1.4.1.667.2.2.2.1.23	INTEGER	read-only
SessionTimer	1.3.6.1.4.1.667.2.2.2.1.24	INTEGER	read-only

JS8500 Private MIB Definitions

Table 5

OBJECT TYPE	SYNTAX	ACCESS	STATUS	DEFINITION
ServerName	DisplayString	Read-write	Mandatory	The hostname of the unit
freeSpace	Gauge	Read-only	Mandatory	The amount of free memory available on the unit
swVersion	DisplayString	Read-only	Mandatory	The software version number
serverInfo	ServerInfo	Not accessible	Mandatory	A list of objects relating to general server information
domainName	DisplayString	Read-write	Mandatory	The domain name of the unit
portsNumber	INTEGER	Read-only	Mandatory	The number of ports on the unit
portsInfoTable	SEQUENCE of PortsInfoEntry	Not accessible	Mandatory	The serial ports info table

OBJECT TYPE	SYNTAX	ACCESS	STATUS	DEFINITION
portsInfoEntry	PortsInfoEntry	Not accessible	Mandatory	An entry in the PortsInfoTable, relating to a port
portID	INTEGER	Read-only	Mandatory	An index that uniquely identifies the port; starts from 1 and must be less than or equal to 24
terminalType	INTEGER { wyse60(1) vt100(2) ansi(3) dumb(4) term1(5) term2(6) term3(7) }	Read-write	Mandatory	The terminal type of the port
baudRate	INTEGER { b75(1) b300(2) b600(3) b1200(4) b1800(5) b2400(6) b4800(7) b9600(8) b19200(9) b38400(10) b57600(11) b115200(12) b230400(13) }	Read-write	Mandatory	The baud rate of the port
dataBits	INTEGER { d5(1) d6(2) d7(3) d8(4) }	Read-write	Mandatory	The number of databits of the port
parity	INTEGER { none (1) odd (2) even (3) }	Read-write	Mandatory	The parity of the port
stopBits	INTEGER { s1 (1) s2 (2) }	Read-write	Mandatory	The number of stop bits of the port

OBJECT TYPE	SYNTAX	ACCESS	STATUS	DEFINITION
pages	INTEGER { p1 (1) p2 (2) p3 (3) p4 (4) p5 (5) p6 (6) p7 (7) }	Read-write	Mandatory	The number of pages of the port
defaultUser	INTEGER	Read-write	Mandatory	The default user of the port
validUser	INTEGER { no (1) yes (2) }	Read-write	Mandatory	Is there a default user user of the port ?
dial	INTEGER { none (1) in (2) out (3) }	Read-write	Mandatory	The dial status of the port
flowControl	INTEGER { none (1) soft (2) hard (3) both (4) }	Read-write	Mandatory	The flow control being used on the port
service	INTEGER { jslogin(1) directraw (2) silentraw (3) printer (4) directtelnet (5) silenttelnet (6) reversetelnet (7) reverseraw (8) bidir (9) directlogin (10) silentlogin (11) slip (12) ppp (13) }	Read-write	Mandatory	The type of connection being used on the port
hostPort	INTEGER	Read-write	Mandatory	The host TCP port of the port
localPort	INTEGER	Read-write	Mandatory	The local TCP port assigned to the port
host	INTEGER	Read-write	Mandatory	The host for virtual connections
pinDCD	INTEGER { off (1) on (2)}	Read-only	Mandatory	The current status of the port's DCD pin.

OBJECT TYPE	SYNTAX	ACCESS	STATUS	DEFINITION
pinDTR	INTEGER { off (1) on (2)}	Read-only	Mandatory	The current status of the port's DTR pin.
pinRTS	INTEGER { off (1) on (2)}	Read-only	Mandatory	The current status of the port's RTS pin.
charSends	Counter	Read-write	Mandatory	The (resettable) count of the number of characters sent through the port
charReceives	Counter	Read-only	Mandatory	The (resettable) count of the number of characters received by the port
phoneNumber	DisplayString	Read-only	Mandatory	The phone number used for this port
modemName	DisplayString	Read-only	Mandatory	The modem name used for this port
idleTimer	INTEGER	Read-only	Mandatory	The idle timer for this port
sessionTimer	INTEGER	Read-only	Mandatory	The session timer for this port

Network Management

If you have separate network management software you can interrogate and configure the unit using SNMP. For example, using CastleRock Computing's SNMPc program running on a Windows PC/host, configuration screens you might see are shown below:

Figure 24
editing the RFC1213 MIB

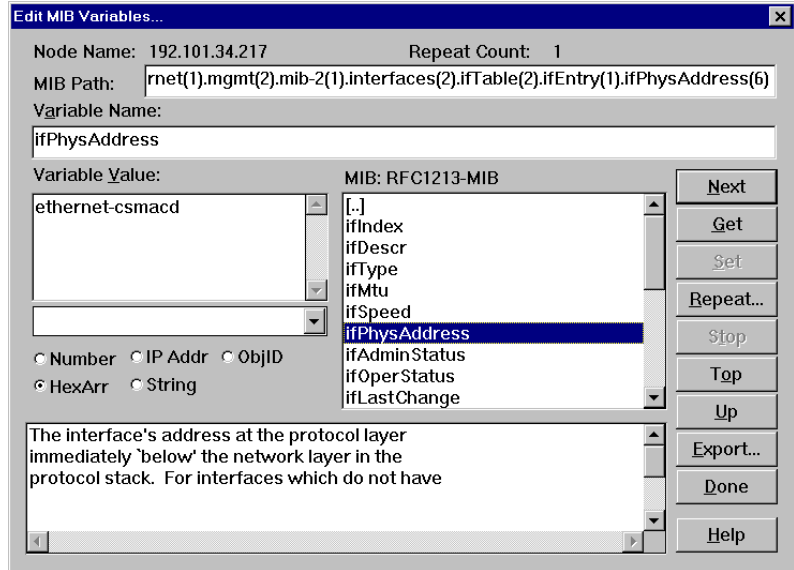


Figure 25
editing the JS8500 MIB

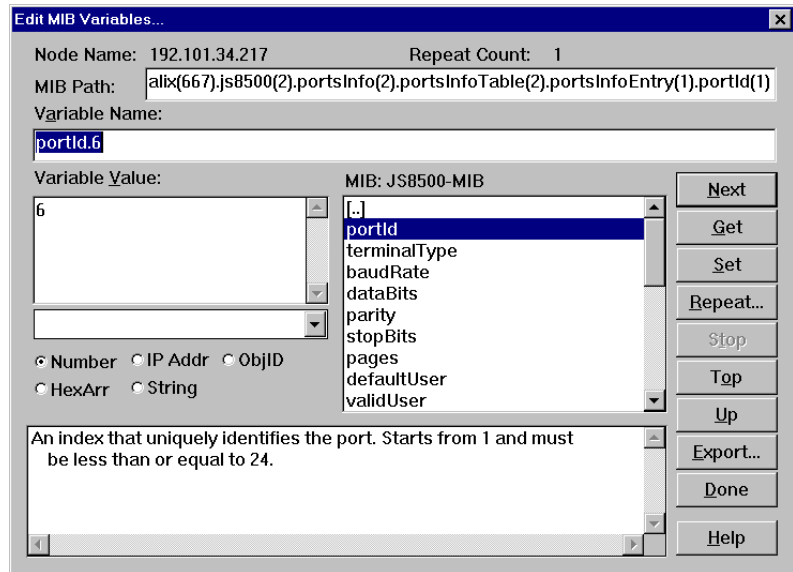


Figure 26
Routing information

192.101.34.217 IpRouteEntry									
Dest	IfIndex	Metric1	Metric2	Metric3	Metric4	NextHop	Type	Proto	Age
0.0.0.0	1	2	-1	-1	-1	192.101.34.222	indirect	rip	2920
127.0.0.0	1	2	-1	-1	-1	192.101.34.198	indirect	rip	2921
158.43.0.0	1	2	-1	-1	-1	192.101.34.222	indirect	rip	2921
192.65.144.0	1	2	-1	-1	-1	192.101.34.222	indirect	rip	2921
192.101.34.192	1	0	-1	-1	-1	192.101.34.217	direct	local	2929
194.131.147.0	1	2	-1	-1	-1	192.101.34.222	indirect	rip	2922

Chapter 7 Guide for Operators on Terminals

Introduction

This chapter explains how to use the JETSTREAM 4000, 8500 or LANSTREAM 2000 (the 'unit') for a user on a terminal. It is provided specifically for users, who do not need to be familiar with system administration matters.

Terminal server connections are described in [Chapter 1 \(Configuring a Line: Terminal Server Connections\)](#)

Chapter contents

It is divided into the following sections:

- Logging in
- Modes of Operation
- Changing your Password
- Changing your Terminal Setup
- Changing your User Environment
- Logging Out
- Running Sessions
- Starting a Session
- Predefining Sessions
- Starting a Predefined Session
- Hot-key Commands
- Resuming a Session
- Killing a Session

Logging in

To be able to log in you must have a login name and password. The system administrator should have set these for you.

- Switch your terminal on and press <return> to call the login prompt.

- Enter your login name and press <return>. If your line has been dedicated to you, your login name will be displayed in brackets automatically, along with the password prompt.
- At the password prompt, enter your password and press <return> (your password will not be displayed as you type it).

When you log in, the unit is in Command Line mode. The cli prompt will be followed by a dollar or pound sign, for example JS_8500\$ (or JS_8500£). The display of a dollar or pound sign will vary according to the characters supported by your terminal.

If you are a restricted user, predefined sessions, set up by the system administrator, may start up automatically. If this is the case, go to Section Starting a Predefined Session.

Logging in via a Modem

Logging in via modem is the same as if you are directly connected to the unit. An additional feature, however, is automatic baud rate detection.

If your terminal is set to a different baud rate to the line into the unit, pressing <return> for the login prompt will display garbled characters or nothing at all. If you send a line break (<break> key) the unit will try the next line speed setting. Send breaks until the login prompt appears. At the slower speeds it may take some time for a response.

Note If you do change the line speed by sending breaks, the following message will be displayed at login:

```
Warning: Baud Rate Changed to new_speed
```

Set the line speed using the 'set line' command, as follows:

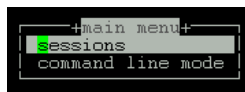
```
set line n speed new_speed  
e.g. set line 6 speed 115200
```

Modes of Operation

The unit has two modes of operation: Full Screen Mode (FSM) - the text-based menu system - and the Command Line Interface (CLI). The CLI is designed for more experienced users. Normal and restricted users may prefer to use the menu system.

Full Screen Mode

Full Screen mode is a menu system, designed for easy access to commands. To enter Full Screen mode, type *screen* and press <return>. The main menu will be displayed (ensure your terminal type is set correctly). For normal and restricted users the main menu contains the following options:



- <Tab> Moves you through fields on the same line, from left to right. The <backspace> key moves you in the opposite direction.
- <PgUp> If the form covers more than one page, you can use the <PgUp> key to display any previous page.
- <PgDn> If the form covers more than one page, you can use the <PgDn> key to display any next page.

Note *On Ansi and VT100 terminals, the <PgUp> and <PgDn> keys won't work unless they are programmed as ^[J and ^[K respectively (where ^[= Escape).*

There are two ways to exit a form:

- <return> Use this key if you want to save the changes made to the form. The following menu will be displayed:

```
Quit Form
Accept And exit Form
```

- <esc> Use this key if you haven't made any changes, or if you don't want to save the changes you have made. If you haven't made any changes to the form, you will be returned to the menu. If you have made changes to the form, the following message will be displayed:

```
Changes Will Be Lost, Proceed? (y/n)
```

Type 'y' to escape, 'n' to return to the form.

Command Line Interface (CLI)

Using the CLI you can enter commands directly rather than through menu options. It is designed for the more experienced user. The Command Line has two features that make it extremely easy to use: context-sensitive help and command abbreviation.

Help

The help key (?) can be pressed at any time to display the options available to you. Look at the following example:

Notice how your original command is always preserved, so that you don't have to type it in again. If you type ? at the CLI prompt, all the commands available to your user level would be listed.

Command Abbreviation

You can use the shortest unambiguous abbreviation of any command. For example, the command:

```
set line 2 termtype wyse60
```

```

JS_8500# set user . ?
password
language
switch                screen switch character
level                 security level
service
ip_host
tcp_port
callback
phone_number
idle_timer
sess_timer
framed_ip
framed_netmask
framed_mtu
framed_compression
session
routing
JS_8500# set user . █

```

could be entered as:

```
se li 2 te w
```

Changing your Password

user level: normal Select the Sessions menu from the main menu. From here, select ‘Set Up User’ and then ‘Set Password’.

cli syntax: You will be asked to enter your old (current) password:

set user

Old Password:

You will then be asked to enter a new password:

Enter Password:

The password can have up to sixteen characters (do not use spaces). Use the key to backspace if necessary. You will be asked to repeat the password:

Re-enter Password:

You will be returned to the Set Up User menu.

Changing your Terminal Setup

user level: normal You are unlikely to need to change your terminal setup, especially while running in Full Screen mode. If you do, remember to make the same changes to your terminal’s setup utility.

cli command:

set user

Changes to your terminal type or the number of video pages supported will take effect immediately. Other changes will take effect the next time you log in.

Don’t change the number of video pages your terminal supports while you have sessions running.

Select ‘Set Up Terminal’ from the Sessions menu. The following form will be displayed.

These are the default settings. In each field, use the <spacebar> to cycle through the available settings, or type ‘L’ to list them.

```

+set up terminal+
speed  terminal  dial  flow  bits  parity  stop  pages
[9600 ] [vt100 ]  [none] [none] [8]  [none]  [1]  [4]

```

Changing your User Environment

Note You must have a user privilege level of ‘normal’ before you can change your user environment (other than access by the systems administrator).

cli syntax: You can change your user environment if
set user

- your screen switch character clashes with an application you are using in one of your sessions, or
- if you wish to have the text menus/cli presented in a different language.

From the main menu select the Sessions menu. From this menu, select the Set Up User menu. Then select ‘Set Environment’.

The following form will be displayed:

```

+user environment+
language  [English ]
screen switch  [1 ]

```

The Language field defaults to ‘English’ but can be set to another language using the ‘customlang’ option. Your system administrator will need to download another language into the unit’s memory. French, German, Italian and Spanish language files are supplied on the supplemental diskette/CD. Switching to another language will change your menus and cli only when you save and exit this form.

The screen switch character must be entered in hex format; see Appendix E (ASCII and HEX conversion tables).

Logging Out

All users To log off the unit, select ‘Logout’ from the Sessions menu. You will be unable to log out if you still have
Command: logout sessions running.

Running Sessions

Sessions are started through the menu option ‘Sessions’ (or through the CLI). You can run multiple sessions simultaneously on the same host or on different hosts. You can switch between different sessions and between sessions and the unit using hot-key commands.

If you are a user with a privilege level of ‘normal’ you can predefine sessions, even configure them to start automatically on login to the unit. If you are a user with a privilege level of ‘restricted’ you can only start sessions predefined for you by the system administrator.

How many sessions can I have?

The actual number of sessions available is four minus the number of predefined sessions set up on your line.

If you have four predefined sessions, you will have no free sessions left. You can get around this by disabling one of your predefined sessions (in the ‘Set Sessions’ form (see Section Predefining Sessions), set the Type field to ‘off’).

Starting a Session

Note You can only predefine sessions if you are a user with a privilege level of ‘normal’ (other than the system administrator).

cli syntax:
telnet, rlogin

1. Select ‘Start telnet/rlogin’ from the Sessions menu. The following form will be displayed:



```
free session
service [telnet]
hostname [
termtype [
username [
echo [off]
mapnl [off]
mode [off]
intr [7f]
quit [1c]
eof [4]
erase [8]
break [d]
```

Complete the fields as follows (using the key to backspace if necessary):

- **Service**- this is the connection protocol you want to use: telnet (default) or rlogin. The relative merits of these protocols are discussed in Chapter 1 (Configuring a Line: Terminal Server Connections).
- **Hostname** - the name or internet address of the machine that you want to access. You must have a login account on this machine. If you want to access a machine in your local network which isn't defined in the host table, you can only use the hostname if it can be resolved by a name server in your network. If you want to access a host outside your local network, it is best to use the internet address.
- **Termtype** - the terminal type you enter here will be passed to the host you are trying to log into. The termtype must be a name recognised by the host. Your system administrator should be able to tell you what to enter.
- **Username** (rlogin only) rlogin will pass your unit's username to the target host. If your username on the target host is different, or if you want to log in as somebody else, enter the required username here.

The fields after ‘Username’ are telnet options only.

2. Set up the session as required and press <return>. You will be connected to the host.
3. Using telnet, you will be prompted for your login name then your password; using rlogin, you will be prompted for your password only. Once you have logged in, you can use the host as if you were directly connected.
4. You can switch to other sessions, and back to the unit, without logging out - see Section Hot-key Commands.
5. To close a session, log out as normal. You will be returned to the unit exactly where you left off.

Predefining Sessions

Note You can only predefine sessions if you are a user with a privilege level of 'normal' (other than the system administrator).

cli syntax: set user

You can predefine up to four sessions. Predefined sessions can be started using the 'Start Predefined Session' menu option, or they can be set up to start automatically. Select 'Set Up User' from the Sessions menu. Select 'Set Sessions' from the Set Up User menu. The Set Sessions form will be displayed:

```

+set sessions+
session 1 2 3 4
service [off] [off] [off] [off]
hostname [pc] [pc] [pc] [pc]
termtype [ ] [ ] [ ] [ ]
auto [off] [off] [off] [off]
echo [off] [off] [off] [off]
mapnl [off] [off] [off] [off]
mode [off] [off] [off] [off]
intr [7f] [7f] [7f] [7f]
quit [1c] [1c] [1c] [1c]
eof [4] [4] [4] [4]
erase [8] [8] [8] [8]
break [1d] [1d] [1d] [1d]

```

These are the default settings. Complete the fields as follows (using the key to backspace if necessary):

- **Service** - this is the connection protocol you want to use: telnet or rlogin. The relative merits of these protocols are discussed in Chapter 1 (Configuring a Line: Terminal Server Connections). Once this field has been set to telnet or rlogin, this session will take up one of your four session slots - whether it is active or not.
- **Hostname** - this is the name of the machine that you want to access. You can only predefine sessions on a host defined in the host table. The first host defined in the host table will be entered as the default. To be able to log in to a machine you must have a login account on it.
- **Termtype** - the terminal type you enter here will be passed to the host you are trying to log into. The termtype must be a name recognised by the host. Your system administrator should be able to tell you what to enter.
- **Auto** - if this field is set to 'off', the session must be started using the 'Start Predefined Sessions' menu option. If the 'Auto' field is set to 'on', the session will start up automatically when the user logs in to the unit. If more than one session is set up like this, session 1 will be displayed first.

The fields after 'Auto' are telnet options only.

Starting a Predefined Session

Note Users with a privilege level of normal and restricted may predefine sessions (as well as the system administrator).

cli syntax: Use this option to start a predefined session.
start

1. Select 'Start Predefined Session' from the Sessions menu. Your predefined sessions will be listed:

```
+predefined sessions+
1: telnet pc
2: telnet Solaris
```

2. Select the session that you want to start.
3. Press <return>. You will be connected to the host. If you are using telnet, you will be prompted for your login name and then your password. If you are using rlogin, you will be prompted for your password only. If you use rlogin, and your unit's login name has been entered in the 'rhost' file of the target login directory, you will be logged straight in. Once you have logged in, you can use the host as if you were directly connected.
4. You can switch to other sessions, and between sessions and the unit, without logging out (see next section).
5. To close a session, log out as normal. You will be returned to the unit exactly where you left off.

Hot-key Commands

All users The commands described in Table 6 can be used to switch between sessions, and to switch between sessions and Full Screen/Command Line mode. The command ^a means hold down the <control> and <a> keys together. This is the screen switch character (or 'hot-key').

Note You can change the screen switch character (^a) if it clashes with a command used by an application you are running in one of your sessions. See Section *Changing your User Environment*.

Table 6 Hot-Key Commands for Session Controls

Function	Hot-key	Description
Switch Sessions	^a n	To switch from one session to another, press ^a and then the required session number. For example, ^a 2 would switch you to session 2. You can also use these commands from the unit to resume sessions. Pressing ^a 0 will return you to the unit.
Display Next Session	^a n	Use this command to display the next session. The current session will remain active. If you use this command from the unit, the lowest numbered active session will be displayed.
Display Previous Session	^a p	Use this command to display the previous session. The current session will remain active. If you use this command from the unit, the highest numbered active session will be displayed.

Function	Hot-key	Description
Return to the unit	^a m	To exit a session and return to the unit, use this command. You will be returned to where you left off. The session will be left running
Redraw Screen	^r	When you switch from a session back to Full Screen Mode, the screen may not be redrawn correctly. If this happens, use this command to redraw it properly.

The functions ‘Display Next/Previous Session’ may not work if your terminal does not allow switching forward and backward between sessions.

Video Pages

You can run four sessions simultaneously. Running the menu system or Command Line counts as a fifth session. If your terminal supports five video pages or more, each session can use a different page. The result of this is that when you switch between sessions their appearance will be maintained, i.e. they will retain their context.

However, if your terminal supports less than five video pages, sessions may have to share pages. Such sessions are termed ‘unpaged’. When you switch to an unpaged session, its context will be lost. The following message will be displayed:

```
[unpaged session n]
```

Similarly, when you switch from an unpaged session to a paged session:

```
[paged session n]
```

Resuming a Session

cli syntax: Select ‘Resume Session’ from the Sessions menu. A list of active sessions will be displayed:
resume

```
Active Sessions
telnet socrates
telnet plato
```

Select the session that you want to resume. It will be resumed where you left off. Alternatively, you can use the hot-key commands described in Table 6.

Killing a Session

cli syntax: This command enables you to kill a session. You cannot log out from the unit while you still have sessions running. Select ‘Kill Session’ from the Sessions menu. A list of your active sessions will be displayed, for example:
kill session

```
Active Sessions
telnet socrates
```

```
telnet plato
```

Select the session that you want to kill. The following prompt will be displayed:

```
Confirm Kill Session 1 (y/n)
```

Type 'y' to kill the session, 'n' to cancel the command.

Chapter 8 Examples of SLIP / PPP connections

Introduction

In Chapter 3 we explained how to configure a JETSTREAM 4000, 8500 or LANSTREAM 2000 (the 'unit') line for a SLIP or PPP connection. Here we take you through examples.

The diagrams show a JETSTREAM 8500 unit. The examples in the diagrams apply equally to other JETSTREAM models and LANSTREAMs.

Chapter contents

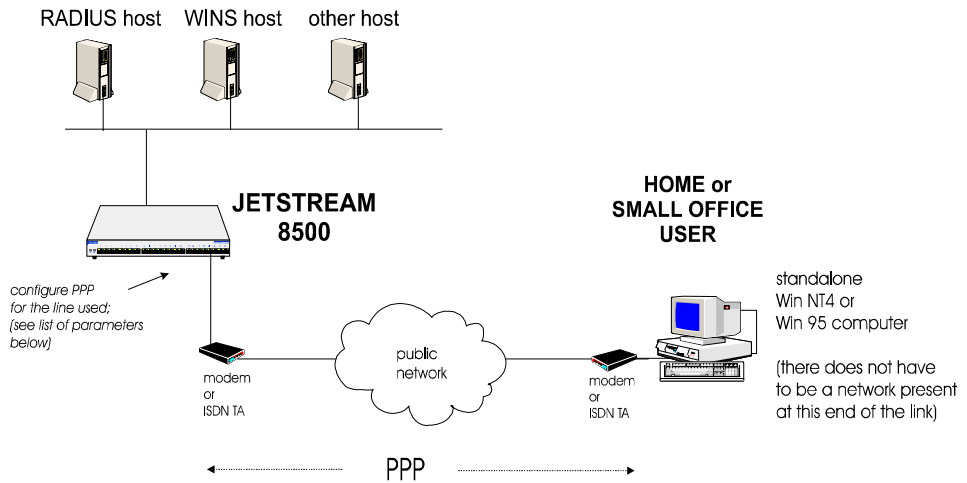
This chapter is divided into the following sections:

- Setting up a Remote User (with PPP)
- Joining together two networks

Setting up a Remote User (with PPP)

This section provides an example of setting up a remote client to the unit, using PPP. The remote client is a single Windows NT4 or 95 computer. Once a successful connection is established to the unit the remote user would be able to use network services (e.g. browsing and using the main file server) as if he/she were connected to the network locally.

Figure 27 typical scenario: a single remote user



The procedure for setting up a remote client depends on the situation, see the following for details:

- [Setting up a remote client on the local network on page 137](#)
- [Setting up a remote client in the unit - on page 137](#)
- [Setting up a remote client in the remote client computer on page 140](#)
- [Setting up a remote client in the main host on the local network on page 141](#)
- [Setting up a remote client in the WINS and/or DNS hosts on the local network on page 141](#)

Setting up a remote client on the local network

1. check if you have a WINS host machine (Windows Internet Name Server) running on your network. A WINS host will allow your remote client to browse; (if you do not have a WINS host, edit the LMHOSTS file on the remote client). Note the ip address of the WINS host machine.
2. check if you have a DNS host machine; note its ip address.

Setting up a remote client in the unit -

1. in the line configuration menu select 'modems' and add your modem and its initialisation string.
2. in the line configuration menu, select 'line settings' and on the line to your remote client configure a minimum of:

line service - set to 'ppp'

modem name - select your modem name

dial parameter - set to 'in'

line speed -set to the highest your modem will accept; e.g 57600

flow (flow control) - set to either 'hardware' or 'software' ('hardware' is preferred)

idle timers and session timers - set to values of your choice; try 600 and 1800 seconds (respectively)

You can leave the other line settings at default; (see Section Setting Up the Line for more information).

The form in the text menu could look like this:

```

+line 8+
service[ppp ]
  speed[9600 ]      terminal[dumb ]
  flow[none]       pages[4 ]
  bits[8]          user[ ]
  parity[none]     hostname[pc ]
  stop[1]          host port[23 ]
  security[off]    JS port[23 ]
  dial[none ]     modem name none ]
  phone number[ ]
  idle timer[ ]   session timer[ ]
  
```

3. configure PPP for the line you are using to connect to the remote computer. Configure a minimum of:
 - local ip address - you allocate this address; an example is shown in Figure 28

remote ip address - it is an ip address for the remote client computer; an example is shown in Figure 28

security - set it to either 'pap' or 'chap'.

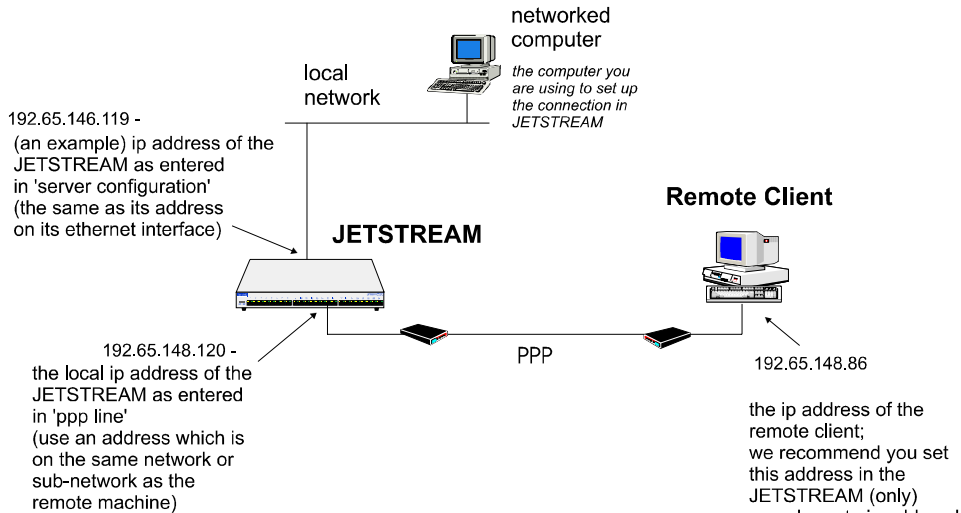
You can leave the other line settings at default; (see Section Configuring PPP for more information).

The form in the text menu would look like this:

```

+ppp line 0+
local ip address[192.65.148.120 ] remote ip address[192.65.148.86 ]
subnet mask[ ] accm[ ]
mru[1500] security[chap]
user[ ] password[ ]
ruser[ ] rpassword[ ]
address_comp[on ] proto_comp[on ]
vj_comp[on ] magic_neg[off]
ipaddr_neg[off]
conf req. to[3 ] term req. to[3 ]
conf req. retries[10 ] term req. retries[2 ]
conf nak retries[10 ] auth_tmout[1 ]
roaming_callback[off] challenge_interval[ ]
  
```

Figure 28 allocating local and remote IP addresses



4. (if you are using PAP or CHAP on the PPP line) add or edit a user account for the user who will be at the remote end; see Section Add a User Account and/or Section Configure a User Account.

5. if you have DNS and/or WINS hosts on your network, enter the IP addresses of these machines - go to the Network Configuration menu; (see the JETSTREAM 4000, 8500, LANSTREAM 2000, Installation Guide, DNS configuration on page 61 and WINS configuration on page 62). The unit will transmit these values to the remote client.
6. 'kill' the line you are using to connect to the remote client computer, then 'restart' it; (in the Line Configuration menu 'kill' line; then, in the command line interface use the 'restart' command).

Setting up a remote client in the remote client computer

1. add and/or configure the modem attached to your computer. Make sure the line settings (baud rate, parity, data bits and stop bits) are the same as the line into the unit. The modem speed you choose is usually not significant; the two modems will negotiate a speed with each other.
2. configure PPP. To help you we have listed below the options which you are related to those in the unit. For both Windows NT4 and Windows 95 you will find these options under 'Dial-up Networking':

Windows NT4 or 95 configuration option	comments
Phonebook entry (NT4) or Connection Properties (W95)	enter the telephone number for the line connected into your unit; select your modem name
Dial-up Server Type	choose 'PPP'
Network Protocol	click on 'TCP/IP'; leave other network protocols (e.g. NetBEUI) unchecked
TCP/IP settings	select 'Server assigned IP address' (the unit will send the ip address to this computer)
TCP/IP settings	select 'Server Assigned name server addresses' . The unit - acting as the 'server' - will send ip addresses of WINS and DNS hosts to the client computer (if you have entered this information in the unit).
TCP/IP settings	select 'use IP header compression'
TCP/IP settings - option 'use default gateway on remote network'	it is not significant whether you select this option
Enable software compression	it is not significant whether you select this option
Log on to network	it is not significant whether you select this option
Enable PPP LCP extensions	check this box if you have selected fixed callback 'on' in the unit (on the first set up of a link, we suggest you leave callback set to 'off')
Scripts	select 'none'

Windows NT4 or 95 configuration option	comments
Security (NT4) or Advanced Options (W95):	
'accept any authentication including clear text'	clicking on this option you can select a security value of 'none' in the unit (under PPP line) or you can select security - 'PAP' or you can select security 'CHAP'
'accept only encrypted authentication' or 'require encrypted password'	if you click on this option, use a security value of 'CHAP' (only) in the unit (under PPP line)
(dialog box presented upon connecting to the unit: name: password: domain name:	enter the same name and password that either the unit or RADIUS is using to authenticate the user do not enter a domain name (i.e.leave blank)
X.25 (NT4 only), Network,	select 'none'

Note Windows NT and 95 provide a dialling capability; there is no need to use separate dialling software.

Setting up a remote client in the main host on the local network

1. If you are not using RIP on this host, add the route to the remote client (which is via the unit).

Setting up a remote client in the WINS and/or DNS hosts on the local network

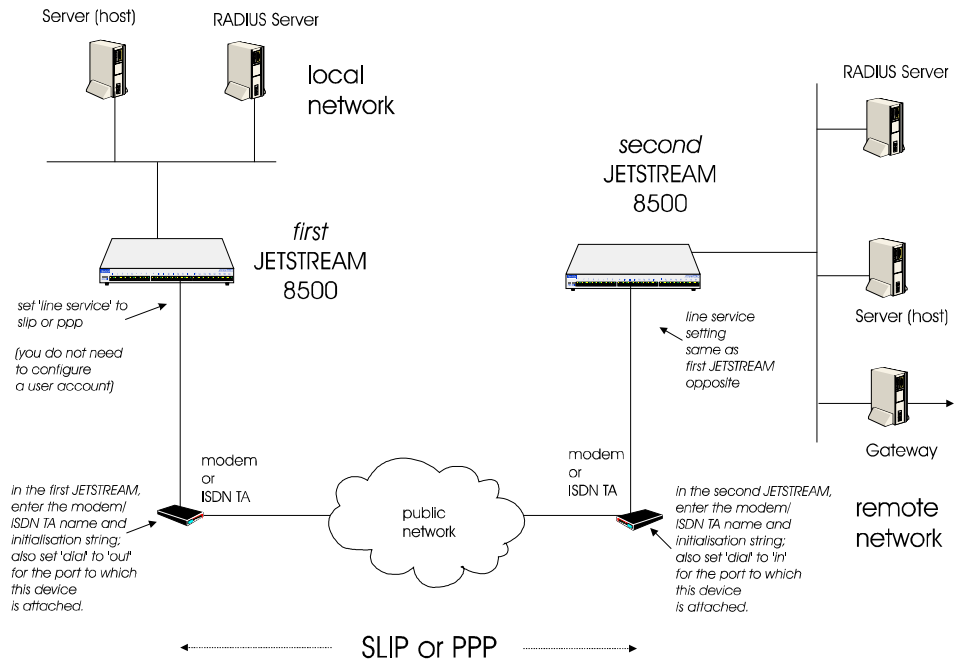
1. If you are not using RIP on this host(s)) add the route to the remote client (which is via the unit).
2. Test your connection by pinging the unit from the remote client (or vice versa). If ok, the user at the remote end of the link should now be able to connect to your local network.
3. Once your remote user can connect successfully to the local network you may also wish to use the security options of PAP or CHAP on the line (see menu option 'PPP line').
4. Once your remote user can connect successfully to the local network you may wish to set up a callback service, either:
 - with a number pre-configured for the user (see fixed callback in Section Configure a User Account), or
 - with the user providing a number for the unit to call him/her back (see roaming callback in Section Configuring PPP).

In either case if your remote user has a Windows NT computer, he/she must change the selection in the 'Dial-up Networking' area, as follows:

Windows NT4 (not W95) configuration option	comments
Phonebook entry - User (or Logon) Preferences - Callback	for 'fixed' callback (in the unit) check the radio button: 'Maybe, ask me during dial when the server offers' for 'roaming' callback (in the unit) check one of the following radio buttons, either: 'Maybe, ask me during dial when the server offers' or: 'Yes, call me back at the number below' (you must enter a number in the field below this option).

Joining together two networks

Figure 29 Joining together two networks

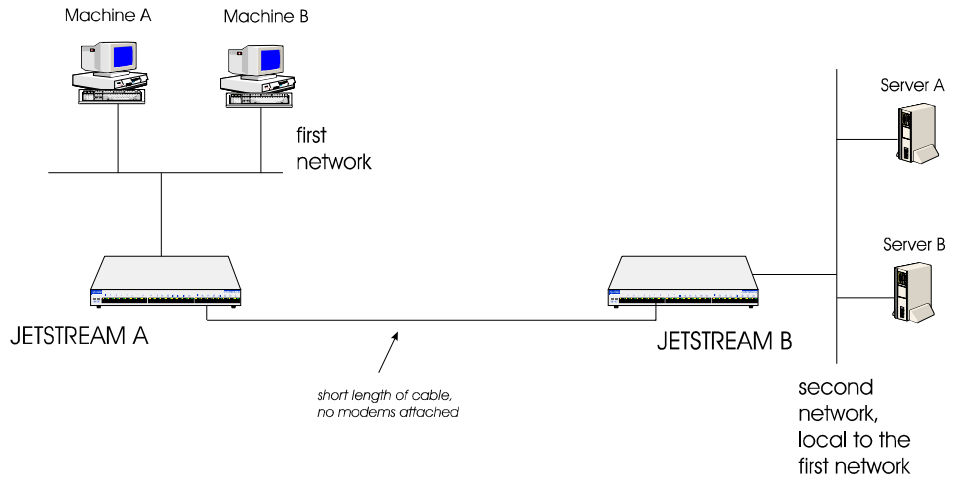


Initial Actions

1. Connect two units located on one site by a short length of (RS232) cable, as shown in Figure 30. Do not connect modems at this stage. Connect each unit to a separate network.

Figure 30

Initial connections



2. Set the ports on both units A and B to either SLIP or PPP (in the menus, use the Line Settings Form; see Section Setting Up the Line. In the cli, use the command `set slip or ppp line`; see Section set ppp line or Section set slip line).
3. Kill the individual line on each unit to make sure the changes have taken effect; (in the menus, go to the Line Configuration Menu, then 'Kill Line'. In the cli, use the kill line command; see kill line on page 163).

4. Connect an RS232 cable between the two ports on the units with the following pin outs:

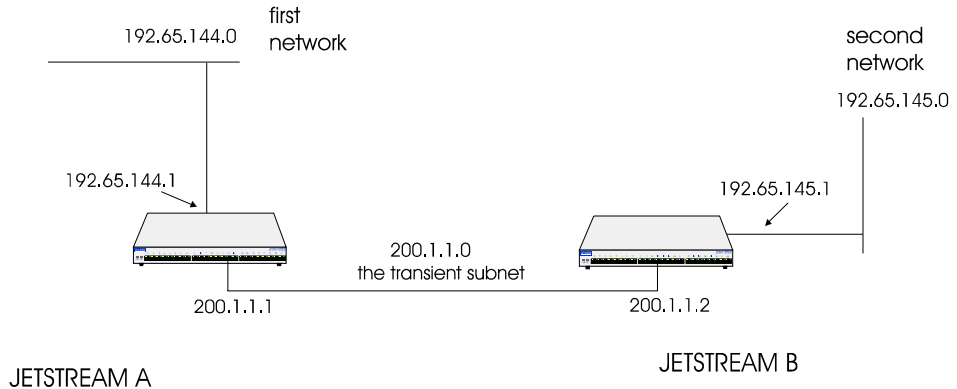
RXD	6	<----	TXD	5	
TXD	5	----->	RXD	6	
RTS	8	<----	CTS	7	(connection only with hardware flow control)
CTS	7	----->	RTS	8	(connection only with hardware flow control)
S/GND	4	----	S/GND	4	

5. Set Dial to NONE on both ports.
6. Set flow control to hardware (SLIP only) or, either hardware or software (for PPP; hardware is preferred).

Setting IP addresses

Refer to Figure 31. To set up the SLIP/PPP link between the two units you must setup a transient subnet (a separate network on the link between the two units which routes packets between the two networks).

Figure 31 IP addresses



To link the two networks (192.65.144.0 and 192.65.145.0) we have created a transient subnet (200.1.1.0) and given the interface at unit A the address 200.1.1.1 and that at unit B to 200.1.1.2.

Looking at Figure 31:

192.65.144.1 is the address of unit A on network 192.65.144.0

200.1.1.2 and 200.1.1.1 are the respective addresses of the units' interfaces on transient subnet 200.1.1.0; the transient subnet is the SLIP/PPP link

192.65.145.1 is the address of unit B on network 192.65.145.0

7. For each SLIP/PPP interface, set the local and remote IP addresses:
 - on unit A, local ip address 200.1.1.1, remote ip address is 200.1.1.2
 - on unit B, local ip address 200.1.1.2, remote ip address 200.1.1.1
8. To complete the setup of the transient subnet, you need to add a gateway to the routing tables in each unit. This gateway tells the unit how to direct packets to the remote network; i.e. unit B needs an entry to tell it to route all packets destined for the 192.65.144.0 network via the interface on unit A 200.1.1.1.

Use the 'Add a Host' menu item (see Adding a Host on page 55) and enter a host. Then select 'Gateway' from the Network Configuration menu. Select 'Add Gateway' and the host table will be displayed; select the host. Note that you can define a host only once as a gateway.

Using the cli, you would make the following entries:

on unit A:

```
add host unitb 200.1.1.2
add gate unitb net 192.65.145.0
```

which means route packets for network 192.65.145.0 through host (interface) on unit B 200.1.1.2 and on unit B:

```
add host unita 200.1.1.1
add gate unita net 192.65.144.0
```

which means route packets for network 192.65.144.0 through host (interface) on unit A 200.1.1.1

9. *(only do this step if you are not using RIP on your network)* Update the routing table in Server A to indicate that the route to machine A is via unit B. Server A in Figure 30 can only send TCP/IP packets to those machines it knows about on its network (like Server B). It cannot see machine A or B directly, so it has to be told how to get to them. To update the routing table, issue the command, at Server A:

```
route add machine_A unitb hopcount
```

If you want to open the route to all machines (not just machine A) on network 192.65.144.0, issue the command:

```
route add 192.65.144.0 unitb hopcount
```

The syntax of this command varies with operating system (os); check your os manual if you are not sure. For example, hopcount is sometimes a number at the end of the command line and sometimes is preceded by -hopcount as in the case of SCO UNIX.

The hopcount between Server A and Machine A is three, as the IP packets are travelling : NETWORK: PPP: NETWORK.

If the unit B had a PC attached running Chameleon the hopcount would only be 2 as the packets are only travelling: NETWORK:PPP.

Once this route is set up the IP packets from Server A will be redirected by unit B to unit A and out onto the network. They will be picked up by Machine A and be seen by this machine to have originated from a server (host) that is not on its network.

10. *(only do this step if you are not using RIP on your network)* The same routing process has to be done on Machine A to get the response back to Server A; i.e.:

```
route add Server_A unita hopcount
```

Likewise, if you want to open the route to all machines (not just server A) on network 192.65.145.0, issue the command:

```
route add 192.65.145.0 unita hopcount
```

This needs to be set up in Machine A to redirect the IP packets back to the Server A or the other network, as appropriate.

11. To test your setup, go to Machine A and ping or telnet Server A (or vice versa). You should have a successful connection. If you have problems, refer to Appendix B (Troubleshooting).

An overview of RIP is given in Appendix D (RADIUS & Networking) of the 8500 Installation Guide.

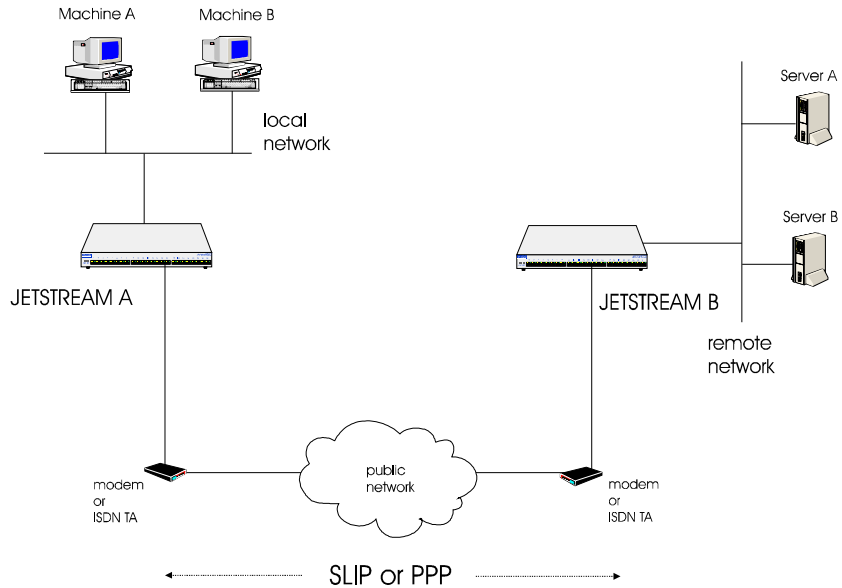
Final actions

Tip we recommend you have successful communication between the two units, without modems, before starting this section.

12. Connect modems or ISDN TAs to the two units, and connect in turn to the public network.

Figure 32

Full configuration



13. Cable each unit to its modem with the following pin outs:

unit			MODEM or ISDN TA		
RJ45			DB25		
RXD	6	<-----	RXD	3	
TXD	5	----->	TXD	2	
RTS	8	<-----	CTS	5	(connection only with hardware flow control)
CTS	7	----->	RTS	4	(connection only with hardware flow control)
DSR	2	----->	DTR	20	
S/GND	4	-----	S/GND	7	
DCD	1	<-----	DCD	8	
DTR	3	<-----	DSR	6	

14. Configure the modems as follows:

on unit A enter the modem name and initialisation string; set Dial to 'in'

on unit B enter the modem name and initialisation string; set Dial to 'out'; enter a 'phone number for unit B to dial.

15. To test communication through the modems and public network, go to Machine A and ping or telnet Server A (or vice versa). You should have a successful connection. If you have problems, refer to Appendix B (Troubleshooting).
16. Set the idle and session timers for the line on unit A. Repeat on unit B.

The two networks should now be able to communicate with each other; the units are acting as routers and are effectively transparent to the machines and servers on the respective local and remote networks.

Chapter 9 The CLI commands

Introduction

This chapter contains a description of each Command Line Interface (CLI) command in the JETSTREAM 4000, 8500 or LANSTREAM 2000 (the 'unit'). The commands are described in alphabetical order and each section includes the user level required to use the command. Most but not all CLI commands have menu equivalents. [Table 7](#) plots the menu options against their equivalent CLI commands.

Table 7
Menu Option/
CLI command
Equivalents

MENU	MENU OPTION	EQUIVALENT CLI COMMAND(S)
Sessions	Set Up Terminal. Set Up User Options Kill Session Logout Resume Session Start Predefined Session Start Telnet/Rlogin Become Admin User	set line, show line set user, show user kill line logout resume start telnet, rlogin admin
Users	Add User Change User Set Sessions Delete User - Set Password	add user set user, show user set user, show user, set telnet, show telnet delete user reset user set user, show user
Line Configuration	Line Port Settings SLIP PPP Parallel Port Settings Modems <i>(when quitting the 'line port settings' form)</i> <i>(when quitting the 'parallel port settings' form)</i> Kill line Kill parallel	set line, show line set slip line, show slip line set ppp line, show ppp line set parallel, show parallel add modem, delete modem, show modems reset line reset parallel kill line kill parallel

MENU	MENU OPTION	EQUIVALENT CLI COMMAND(S)
Server configuration	servername internet address broadcast address subnet mask domain name ip_host authentication dhcp gui access	set server, show server
	banner OEM mode <i>(the version of software running is displayed at the top of any menu screen)</i> - <i>(on exit from the Main menu when going to the cli)</i> -	version netload, netsave save debug
Radius Configuration	Add authentication host Delete authentication host Add accounting host Delete accounting host Change radius settings (‘authentication’ - this is a sub-item in the ‘server configuration’ menu)	add radius delete radius add radius delete radius set radius, show radius set server, show server
Network Configuration	reset snmp tftp host table (options) DNS (options) WINS (options) gateway (options) -	reset factory add community, add trap, delete community, delete trap, set contact, set location, show snmp set server add host, set host, delete host, show hosts add DNS, delete DNS, show server add WINS, delete WINS, show server add gateway, set gateway, delete gateway, show gateways show routes

MENU	MENU OPTION	EQUIVALENT CLI COMMAND(S)
	security reboot	set server reboot

add community

user level: This command enables you to define up to four SNMP communities.
admin

Syntax

```
add community community_name inetaddress
             none | readonly | readwrite
```

Where:

community_name is an arbitrary name assigned to the community.

inetaddress is the internet address that identifies the host(s) in the community.

none | readonly | readwrite defines the access permissions for the community.

See also

[add trap](#), [delete community](#), [set contact](#), [set location](#), [show snmp](#)

add DNS

user level: This command enables you to define the DNS (Domain Name Service) host or hosts in your network. You can enter the addresses two DNS hosts in the unit; one will be referred to as the primary host, the other a secondary host. The DNS hosts do not have to be the same hosts as entered in your unit's host table.

On a remote access connection the unit will transmit these addresses to a dial-up Windows NT/95 client. Therefore, your remote user does not have to configure DNS parameters in his/her computer.

For more information on DNS see the Installation Guide, [Section](#) .

Syntax

```
add DNS internet_address
```

Note 'DNS' must be entered in upper case. Also:

internet address is the internet address of your machine providing the DNS; enter the address in dot decimal notation.

Menu equivalent

Network Configuration - DNS - Add DNS

See also

[delete DNS](#), [add WINS](#), [show server](#)

add gateway

user level:
admin

This command enables you to define the gateways in your network. You can add up to twenty gateways and these must be hosts that you have defined in the host table.

Syntax

```
add gateway hostname type [inetaddress]
```

Where:

hostname is the name of the host that you want to define as a gateway

type is the gateway type: default, host or network. The types are:

- **Default** - this is a gateway which provides general access beyond your local network.
- **Host** - this a gateway reserved for accessing a specific host external to your local network.
- **Network** - this is a gateway reserved for accessing a specific network external to your local network.

inetaddress if you define the type as host or network, you must define the internet address of the target host or network.

Your gateway by default is 'active'; you can change it to 'passive'; see the command `set gateway`.

Menu equivalent

Network Configuration - Gateway - Add Gateway

See also

[delete gateway](#), [set gateway](#)

add host

user level:
admin

This command enables you to add the details of the other hosts in your network. These will be added to the host table. You can also add hosts accessed frequently not in your LAN.

Syntax

```
add host hostname inetaddress
```

Where:

hostname is the name of the host (14 characters maximum).

inetaddress is the internet address of the machine.

Menu equivalent

Network Configuration - Host Table - Add Host

See also

[delete host](#), [set host](#)

add modem

user level:
admin

Use this command to add modem details to the unit. You will want to add modems which you want the unit to control.

Syntax

```
add modem name init_string
```

Where:

<code>name</code>	is the name of your modem, e.g. <code>usrobotics28.8</code> , or a name you wish to use, e.g. <code>modem4</code> . Do not enter spaces in the name; use the underscore <code>_</code> character; e.g. <code>us_robotics_28.8</code>
<code>init_string</code>	is the initialisation string of the modem; see your modem's documentation.

Menu equivalent

Line Configuration - Modems - Add Modem or Change Modem

See also:

[delete modem](#), [show modems](#)

Note *To change modem details in the cli you must 'delete' the modem, then 'add' it again, with the changed details.*

add radius

user level: Use this command to add RADIUS authentication and accounting hosts to the unit.
admin

Syntax

```
add radius host type host name secret
```

Where:

<code>host type</code>	is either <code>authentication_host</code> or <code>accounting_host</code>
<code>hostname</code>	is the name of the RADIUS host
<code>secret</code>	is the secret (password) shared between the unit and the RADIUS host.

Note *You must have the host already entered in the unit's host table; see [Section add host](#). If not you will see a message saying that no host is configured.*

Menu equivalent

radius configuration - radius settings

See also:

[delete radius](#), [set radius](#), [set server](#), [show radius](#)

add trap

user level:
admin

Use this command to define communities which will receive trap messages generated by the unit. Note that the unit does not generate any enterprise-specific traps. Up to four trap communities may be defined.

Syntax

```
add trap trap_name inetaddress
```

Where:

trap_name is an arbitrary name assigned to the community.

inetaddress is the internet address that identifies the host(s) in the community.

See also

[add community](#), [delete trap](#), [set contact](#), [set location](#), [show snmp](#)

add user

user level:
admin

This command enables you to add a new user to the system. You will be prompted to enter a password (maximum sixteen characters). You must also set the user's level using the `set user` command.

Syntax

```
add user username
```

Where *username* is the required login name (maximum sixteen characters).

Menu equivalent

Users - Add User

See also

[delete user](#), [set user](#), [show user](#)

add WINS

user level:
admin

This command enables you to define the WINS (Windows Internet Naming Service) host or hosts in your network. You can define a maximum of two hosts. If you wish, it/they can be the same address(es) as a machine(s) already entered in the unit host table.

Syntax

```
add WINS internet_address
```

Note 'WINS' must be entered in upper case. Also:

internet address is the internet address of your machine providing the WINS; enter the address in dot decimal notation.

Menu equivalent

Network Configuration - WINS - Add WINS

See also

[delete WINS](#), [add DNS](#), [show server](#)

admin

user level:
normal

If you are a normal user, this command enables you to enter Admin mode. But only if you know the admin password. This will give you full access to the unit's commands. The unit's prompt will change to a hash or pound sign (JS_8500# or JS_8500£) to indicate that you are in admin mode. You must log out and back in again to revert to your original mode.

Syntax

```
admin
```

Menu equivalent

Sessions - Become Admin User

debug

level of user:
admin

This command will send debug information to the screen. You can be connected to either the Admin port or a front-mounted port. Use this command only when instructed by your Technical Support.

Syntax

```
debug
```

Menu equivalent

(none available)

See also

-

delete ARP

This command enables you to delete the ARP table. This is useful for diagnostic and debugging purposes. This command is only available from the CLI.

Syntax

```
delete arp
```

See also

[*show ARP*](#)

delete community

user level: This command enables you to delete SNMP communities defined using the `add community` command.
admin

Syntax

```
delete community 1 | 2 | 3 | 4
```

Communities are numbered according to the order they are created in. You can list them using the `show snmp` command.

See also

[add community](#), [delete trap](#), [show snmp](#)

delete DNS

user level: This command enables you to delete the DNS (Domain Name Service) host or hosts in your network.
admin

Syntax

```
delete DNS internet_address
```

Note 'DNS' must be entered in upper case. Also:

internet address is the internet address in dot decimal notation. If you cannot remember the address type a space and then a question mark after DNS; e.g. `del DNS ?`
The unit will list the ip addresses of DNS machines entered in its DNS table. Type the ip address.

Menu equivalent

Network Configuration - DNS - delete DNS

See also

[add DNS](#), [delete WINS](#), [show server](#)

delete gateway

user level: This command enables you to delete a gateway. The host will not be deleted from the host table.
admin

Syntax

```
delete gateway hostname
```

Menu equivalent

Network Configuration - Gateways

See also

[add gateway](#), [set gateway](#), [show gateways](#)

delete host

user level: This command enables you to delete a host from the host table. If the host is referenced by any predefined telnet or rlogin session, or is defined as a gateway, DNS or WINS host, the message <in use> will be displayed and it will not be deleted.
admin

Syntax

```
delete host hostname
```

Menu equivalent

Network Configuration - Host Table

See also

[add host](#), [set host](#)

delete modem

user level: Use this command to delete modem details from the unit.
admin

Syntax

```
delete modem modem_name
```

If you cannot remember the name of the modem, key the first few significant letters or type ?

Menu equivalent

Line Configuration menu - modems - delete modem

See also:

[add modem, show modems](#)

Note *To change modem details in the cli you must 'delete' the modem, then 'add' it again, with the changed details.*

delete radius

user level: Use this command to delete RADIUS authentication and accounting hosts from the unit.
admin

Syntax

```
delete radius host type host name
```

Where:

<i>host type</i>	is either <code>authentication_host</code> or <code>accounting_host</code>
<i>hostname</i>	is the name of the RADIUS host

Menu equivalent

radius configuration - radius settings

See also:

[add radius](#), [show radius](#)

delete trap

user level: This command enables you to delete SNMP trap communities defined using the `add trap` command.
admin

Syntax

```
delete trap 1 | 2 | 3 | 4
```

Communities are numbered according to the order they are created in. You can list them using the `show snmp` command.

See also

[add trap](#), [delete community](#), [show snmp](#).

delete user

user level: This command enables you to delete a user. You cannot delete the following: the default admin user, users that are logged in or users whose line is dedicated to them.
admin

Syntax

```
delete user username
```

Menu equivalent

Users - [delete user](#)

See also

[add user](#), [set user](#), [show user](#)

delete WINS

user level: This command enables you to delete the WINS (Windows Internet Naming Service) host or hosts in your network.
admin

Syntax

```
delete WINS internet_address
```

Note 'WINS' must be entered in upper case. Also:

internet address is the internet address in dot decimal notation. If you cannot remember the address type a space and then a question mark after WINS; e.g. del WINS ?
The unit will list the ip addresses of WINS machines entered in its WINS table. Type the ip address.

Menu equivalent

Network Configuration - WINS - delete WINS

See also

[add WINS](#), [delete DNS](#), [show server](#)

heap

user level: This command tells you how much free memory currently exists and the largest available fragment.
admin

Syntax

```
heap
```

help

all users The *help* command displays a brief description of how to use the Command Line:

```
Type ? at any time to list possible options  
(e.g. set user?)
```

Syntax

```
help
```

kill line

user level:
admin

This command can be used to kill the processes on a *serial* line.

Syntax

```
kill line n
```

Where *n* is the line that you want to kill.

Menu equivalent

Line Configuration - Kill Line

See also

[kill session](#), [reset line](#), [restart](#), [kill parallel](#)

kill parallel

user level:
admin

This command can be used to kill the processes on a parallel line.

Syntax

```
kill parallel n
```

Where *n* is the line that you want to kill.

Menu equivalent

Line Configuration - Kill Line

See also

[kill session](#), [reset parallel](#), [restart](#), [kill line](#)

kill session

all users This command enables you to kill a session.

Syntax

```
kill session n
```

Where *n* is the session that you want to kill. To see how your sessions are numbered, use the `show sessions` command.

Menu equivalent

Sessions - Kill Session

See also

[kill line](#), [logout](#), [resume](#), [show sessions](#)

logout

user levels: This command logs you off the unit. You won't be allowed to log out if you still have sessions running.
all users

Syntax

```
logout
```

Menu equivalent

Sessions - Logout

See also

[kill line](#), [kill session](#)

netload

user level: This command allows you to download a file over a network from a host using TFTP. The file can be one of several types; e.g. a configuration file of another unit. The list of file types is shown below.
admin

Syntax

```
netload [nowrite] filetype hostname filename
```

where you replace the word 'filetype' with one of the following words:

customlang	a language file either supplied or translated; see Section Language of your choice
configuration	a configuration file of a unit
term1	the first of your extra terminal definition files
term2	the second of your extra terminal definition files
term3	the third of your extra terminal definition files
software	a new version of a unit's software

and where:

hostname	is one from the list of hosts defined in the unit's host table. Type ? to show the host table entries. Select a host by typing its name, e.g. aristotle.
filename	must include the path to the file e.g. /etc/jetstream/config/... The path/filename must start with the 'forward slash' / character; do <i>not</i> specify a drive letter. For terminal definition files, the unit will refer to your filename (after downloading) as either 'term1' 'term2' or 'term3'.
nowrite	is an optional parameter which allows you to put the downloaded file into RAM without a write to FLASH memory. You must type the word 'nowrite' immediately after 'netload' (separated by a space). Subsequently you can save the file to FLASH by re-using the netload command <i>without</i> the 'nowrite' option.

During and/or after download you will see status messages at the command line, e.g.

```
TFTP: transfer succeeded
```

Note you can configure TFTP in the unit; see the command set `server`.

The downloaded files will take effect as follows:

customlang	see Section Language of your choice
configuration	immediately after successful download. When you continue to use the cli or menus, you will be using the new configuration
term1, term2 and term3	see Section Downloading Terminal Definitions
software	when you reboot the unit. See Section reboot

If you have used the 'nowrite' option and you now wish to discard this file in RAM and revert to the original file in FLASH, you must reboot the unit. Use the cli command `reboot`.

Menu equivalent

(none available)

See also

[netsave](#), [reboot](#), [set server](#)

netsave

user level:
admin

This command enables you to save two types of information to a file on a remote host: the configuration of your unit and crash details.

Configuration information

The following information will be saved:

- User Profiles, including passwords

- Port Configuration

- Host Table

- Gateways

- RADIUS details

- Modems

- SNMP

Information unique to this unit (name, ip address) will not be saved. Make sure you have write permission to the file. You can use this configuration file to configure other units. The configuration can subsequently be reloaded using the `netload` command.

Crash information

When the unit has rebooted after a crash you can save crash information to a file on a remote host. This information will be diagnostic data for use by Technical Support personnel.

Syntax:

```
netsave type hostname filename
```

where you replace the word 'type' with one of the following words:

configuration	the configuration of your unit
crash	information associated with the last crash of the unit

and where

hostname	is one from the list of hosts defined in the unit host table. Type ? to show the host table entries. Select a host by typing its name, e.g. aristotle.
filename	must include the path to the file e.g. /etc/jetstream/config/...

Menu Equivalent:

(not available)

See Also:

[netload](#), [save](#)

ping

all users

If you are having trouble accessing a host, try the *ping* command. This tries to elicit a response from the specified host. If successful, a report similar to the following will be generated:

```
# ping socrates

PING socrates (192.101.34.1): 100 data bytes
108 bytes from 192.101.34.1: icmp.seq=0. time=15. ms
108 bytes from 192.101.34.1: icmp.seq=1. time=12. ms

- - - socrates PING statistics - - -
10 packets transmitted, 10 packets received, 0% packet loss
round-trip (ms) min/avg/max = 12/12/15
```

You can interrupt the process by pressing any key.

If the hostname cannot be resolved, the following message will be displayed:

```
Ping: hostname: Host not found
```

If the host has been resolved, but the network it is on is unreachable, the following output will be generated:

```
ping hostname/inetaddress 100 data bytes

ping: t_rcvudata: ENETUNREACH - Network is
unreachable
```

If the host has been resolved, but it isn't answering, the following will be displayed:

```
ping hostname/inetaddress 100 data bytes

10 packets transmitted, 0 packets received,
100% packet loss.
```

Syntax

```
ping hostname/inetaddress [packet_size] [packets_sent]
```

Where:

<i>hostname/ inetaddress</i>	is the hostname or internet address of the machine that you want to ping.
<i>packet_size</i>	is the size of packet sent (default = 100 bytes).
<i>packets_sent</i>	is the number of packets sent (default = 10).

reboot

user level:
admin

This command will reboot the unit. You will be asked to confirm the reboot with the following prompt:

```
save config to flash ROM y/n
```

If you press 'y' the unit will save your configuration, close all connections and then reboot. If you press 'n' the unit will prompt you:


```
confirm reboot unit y/n
```

Press 'y' to reboot, 'n' to cancel.

For more information on how the unit reboots, see BOOTP, [Section Overview](#).

Rebooting does not reset the unit to factory default settings.

Syntax

```
reboot
```

Menu equivalent

Network Configuration - Reboot

See also

[show server](#)

reset factory

user level: This command will reset the unit to its default values. The unit will save the factory default settings to FLASH memory; this saving will take a few seconds. After this period you will be logged out and presented with a new login prompt.
admin

Syntax

```
reset factory
```

Menu equivalent

Network Configuration - Reset

See also

[reboot](#)

reset line

user level: This command will reset the specified serial line(s) to the default line configuration.
admin

Syntax

```
reset line ./n/*
```

Where:

.	specifies the current line.
<i>n</i>	is a specific serial line number.
*	specifies all serial lines.

Menu equivalent

Line Configuration - Line Settings - Quit form

See also

[kill line](#), [restart](#), [show line](#), [set line](#), [reset parallel](#)

reset parallel

user level: If you have parallel port(s) fitted to your unit, this command will reset the specified parallel line(s) to the default line configuration.
admin

Syntax

```
reset parallel n/*
```

Where:

<i>n</i>	is a specific parallel line number.
*	specifies all parallel lines.

Menu equivalent

Line Configuration - Parallel Port Settings - Quit form

See also

[kill parallel](#), [restart](#), [show parallel](#), [set parallel](#)

reset user

user level: This command will reset the specified user(s) to the default user settings. This sets the user level to 'normal' and the screen switch character to '1'. Any predefined sessions are switched off. The default admin user will not be reset.

admin

Syntax

```
reset user ./*/username
```

Where:

.	specifies the current user.
<i>username</i>	is the name of a specific user.
*	specifies all users.

See also

[reboot](#)

restart

user level:
admin

When there is insufficient free memory to start a login or virtual circuit on a line, that line will appear dead and you will be unable to restart it. You must wait until sufficient memory is available and then restart all such lines using this command. You can enter the command on any active serial line. The execution of the command will affect halted processes on all lines, both serial and parallel.

Syntax

```
restart
```

Menu equivalent

(none available)

See also

[heap](#), [kill line](#), [kill parallel](#)

resume

user level:
all users

The resume command enables you to resume any session that you have left running. You will be returned to your last position in a session.

Syntax

```
resume n
```

Where *n* is the session you want to resume.

Menu equivalent

Sessions - Resume Session

See also

[kill session](#), [start](#)

rlogin

user level:
admin, normal

This command will establish a connection with a host using the rlogin protocol. Rlogin passes your login name to the host, so you are prompted for your password only. If your unit's login name exists in the 'rhost' file of the target login directory, you won't be prompted for a password. You will be logged straight in.

Syntax

```
rlogin hostname/inetaddress [termttype termttype] [user  
username]
```

Where:

<i>hostname/ inetaddress</i>	is the hostname or internet address of the machine you want to log into.
<i>termttype</i>	is your terminal type. By default a dumb terminal type is passed to the host. When connecting to a UNIX host, you must define the termttype in accordance with its UNIX TERM variable.
<i>username</i>	is your login name on the target host if different to your unit's login. You can also use this argument to log in as someone else.

Menu equivalent

Sessions - Start telnet/rlogin

See also

[kill session](#), [resume](#), [show line](#), [start](#), [telnet](#)

save

user level:
admin

This command enables you to save the configuration information of your unit to FLASH (permanent, non-volatile) memory. Note that the save command does not apply to language files or any other files downloaded into RAM using the netload command. The writing to FLASH will take a few seconds and during this time the unit will not respond to user input.

WARNING

do not turn the power on/off while the unit is writing to FLASH memory.

Syntax:

```
save
```

See also

netload, netsave

screen

all users This command will change you from Command Line mode to Full Screen mode (on supported terminal types only).

Syntax

```
screen
```

set contact

user level: This command enables you to configure the SNMP sysContact object.
admin

Syntax

```
set contact contact_name
```

Where *contact_name* is a string representing your contact name; it cannot contain spaces (e.g. john.smith, john_smith or johnsmith)

See also

[*set location*](#), [*show snmp*](#)

set date

user level: This command enables you to set the date in the unit. The date is used by the real-time clock. For more information on the real-time clock see JETSTREAM 4000, 8500, LANSTREAM 2000, Installation Guide, [Setting Date and Time on page 55](#).
admin

Syntax

```
set date dd/mm/yyyy
```

for example; set date 05/12/2000

Menu equivalent

Main Menu - hardware

See also

[set time](#)

set ethernet interface RJ45

user level: This command enables you to select the RJ45 10/100Base-T interface.
admin

Syntax

```
set ethernet interface RJ45
```

See also

[set ethernet interface AUI](#), [show hardware](#)

set ethernet interface AUI

user level: This command enables you to select the AUI interface.
admin

Syntax

```
set ethernet interface AUI
```

See also

[set ethernet interface RJ45](#), [show hardware](#)

set ethernet speed

user level: This command enables you to select the speed of the Ethernet RJ45 interface.
admin

Syntax

```
set ethernet speed speed-value
```

Where:

speed-value can be set to one of the following:

- Auto:** auto-sense the speed of the ethernet interface (default)
- 10M:** set speed to 10 Mbps
- 100M:** set speed to 100 Mbps

See also

[*set ethernet interface RJ45, show hardware*](#)

set gateway

user level: This command enables you to redefine a gateway.
admin

Syntax

```
set gateway hostname type [inetaddress] [status]
```

Where:

<i>hostname</i>	is the name of the gateway.
<i>type</i>	is one of 'default', 'host' or 'network'.
<i>inetaddress</i>	is the internet address of the target host or network.
<i>status</i>	is one of: 'active' or 'passive'.

For definitions of active and passive see the Installation Guide [Gateways on page 63](#).

Menu equivalent

Network Configuration - Gateway - Change Gateway

See also

[add gateway](#), [delete gateway](#), [show gateways](#)

set host

user level: Use this command if you need to change the internet address of one of the hosts in your host table.
admin

Syntax

```
set host hostname inetaddress
```

Menu equivalent

Network Configuration - Host Table - Change Host

See also

[add host](#), [delete host](#), [show hosts](#)

set line

user levels:
admin, normal

Use this command to configure lines on the front-mounted RJ45 ports only. The command cannot set:
the Admin Port line configuration; this is fixed - see the Installation Guide, *The Admin Port on page 37*.
the parallel port line configuration; see the command `set parallel`.

An admin user can change the setup of any line; a normal user can change their own line only. On login connections, changes to the terminal type or number of video pages will take effect immediately. Other changes will take effect when a user next logs in on the line.

Syntax

```
set line line_number
[speed speed]
[parity parity]
[stop stop-bits]
[data data-bits]
[flow flow-control]
[pages pages]
[termttype term-type]
[dial dial-status]
[user user-name]
[nouser]
[service line_service]...followed by (optionally)
    [raw/telnet] [hostname] [js_port] [host_port]
[phone_number phone-number]
[modem_name modem-name]
[idle_timer i-timer value]
[session_timer s-timer value]
[routing routing]
[security security]
```

Where:

- line_number* may also be specified as '*' for all lines or '.' for the line currently being used.
- speed, parity, stop-bits, data-bits, flow control* are standard line settings
- pages* (for 'jslogin' line service) is the number of video pages the terminal supports.
- term-type* is the type of terminal attached to this line; e.g. ansi. Note this value will be ignored if you have set a termttype value using the command telnet.

<i>dial-status</i>	use when a modem is attached to a port; set to 'in' or 'out' (default none). Note that 'dial-status' is unrelated to the User 'callback' parameter.
<i>user-name</i>	(for <code>jslogin</code> line service) can be used to dedicate the line to a specific user. Only this user will be able to log in on this line and they won't need to enter their login name - just their password.
<i>nouser</i>	(for <code>jslogin</code> line service) nullifies the user argument; it enables any user to log in on this line.
<i>line-service</i>	<p>select from one of: <code>jslogin</code>, <code>direct</code>, <code>silent</code>, <code>reverse</code>, <code>printer</code>, <code>bidir</code>, <code>slip</code> or <code>ppp</code>.</p> <p>for remote access connections, see Section Setting Up the Line, subsection Service.</p> <p>when you select 'direct', 'silent' or 'reverse', you must specify whether the line service is 'raw' or 'telnet'; e.g. <code>silent telnet</code>.</p> <p>when you select 'direct', 'silent' or 'bidir', you must enter the target host name; e.g. <code>sophocles</code>.</p> <p>when you select 'direct raw', 'silent raw' or 'bidir', you must specify the TCP port assigned on the target host to listen for the incoming connection.</p> <p>when you select 'reverse raw' or 'bidir', you must specify the TCP port assigned to the unit's port (that is the JETSTREAM 4000, 8500 or LANSTREAM 2000 TCP port number). TCP/IP hosts will use this TCP port to establish a connection with the unit.</p>
<i>phone-number</i>	a number which the unit will dial on that line, when 'dial' is set to 'out'. Enter the number without spaces. To change the phone number overwrite the previous entry.
<i>modem-name</i>	is the name of the attached modem; e.g. <code>usrobotics28.8</code> , or a name you wish to use, e.g. <code>modem 1</code> . Do not enter spaces in the name; use the underscore <code>_</code> character; e.g. <code>us_robotics_28.8</code> . You can enter a total of nineteen alphanumeric characters (including spaces).
<i>i-timer value</i>	<p>enter a period in seconds for which the idle timer will run. Use this timer to close a connection because of inactivity. When the idle timer expires, if there has been no exchange of data, the unit will end the connection. The default value is 0 (zero), meaning that the idle timer will not expire (the connection is open permanently).</p> <p>This idle timer will be overridden by the idle timer which you can configure for a user; i.e. the user idle timer takes precedence.</p>

s-timer value	enter a period in seconds for which the session timer will run. Use this timer to forcibly close the session (connection). When the session timer expires the unit will end the connection. The default value is 0 (zero), meaning that the session timer will not expire (the session is open permanently, or until you kill the line or you/the user log(s) out). This session timer will be overridden by the session timer which you can configure for a user; i.e. the user session timer takes precedence.
Routing	determines whether RIP packets are sent over SLIP/PPP connections. Can be set to None (off), send, listen or send & listen.
security	This may be set to on or off to enable login/password authentication on reverse telnet and other reverse type connections. The unit's stored user database is always used for this authentication. The default setting is off .

Any number or combination of the arguments can be used.

Examples:

```
set line 6 service silent telnet plato
set line 3 service reverse raw 1000
set line 9 speed 38400 modem in service bidir
homer 1000 900
```

You can set all lines to the same parameters by using the * asterisk character, e.g.

```
set line * speed 38400 dial in
```

will set all lines to this speed and dial values.

Menu equivalent

Line Configuration - Line Settings

See also

[show line](#), [add modem](#), [set parallel](#)

set location

user level: This command enables you to configure the SNMP sysLocation object.
admin

Syntax

```
set location location
```

See also

[set contact](#), [show snmp](#)

set parallel

user levels: If parallel port(s) are fitted to your unit use this command to configure lines on the parallel port(s).
admin

Syntax

```
set parallel  
line_number  
[service line_service]... followed by (optionally)  
[raw] [hostname] [js_port] [host_port]
```

Where:

<i>line_number</i>	may be specified as '*' for all parallel lines or '.' for the line currently being used.
<i>line-service</i>	select from one of: printer.

Any number or combination of the arguments can be used.

Examples:

```
set par 1 service printer
```

Menu equivalent

Line Configuration - Parallel Port Settings

See also

[show parallel](#), [reset parallel](#), [kill parallel](#)

set ppp line

user level: Use this command to configure PPP on a line.
admin

syntax

```
set ppp line line_number parameter
```

where: *line_number* may also be specified as * for all lines, or . for the current in-use line.

parameters are any from the list below:

parameter syntax	parameter name
lipaddr	local ip address
ripaddr	remote ip address
subnet	subnet mask
accm	asynchronous character control map
mru	maximum receive unit
security	security
user	user
password	password
ruser	remote user
rpassword	remote password
ac_comp	address/control compression
proto_comp	protocol compression
vj_comp	VJ compression
magic_neg	magic number negotiation
ipaddr_neg	ip address negotiation
cr_tmout	'configure request' timeout
tr_tmout	'terminate request' timeout
cr_retry	'configure request' retries
tr_retry	'terminate request' retries
nak_retry	'configure nak' retries

parameter syntax	parameter name
auth_tmout	authentication timeout

The meanings and values of these parameters are explained in the Configuration Guide [Section Configuring PPP](#).

You can include multiple parameters in one line of syntax.

Menu equivalent

Line Configuration - Line Settings

See also

[show ppp line](#)

set radius

user level: Use this command to set RADIUS settings of the unit:
admin

Syntax

```
set radius <parameter>
```

The parameters are detailed in JETSTREAM 4000, 8500, LANSTREAM 2000, Installation Guide, [Section RADIUS configuration](#). Type a question mark ? at the command line prompt to see a list of the parameters. You can enter multiple parameters on one line.

Menu equivalent

radius configuration- radius settings

See also

[add radius](#), [show radius](#), [set server](#)

set server

user level: Use this command to configure the home setup of the unit.
admin

Syntax

```
set server

[name server-name]
[internet inet-address]
[subnet subnet]
[broadcast broadcast]
[domain domain]
[ip_host user-iphost]
[authentication auth-method]
[tftp retry retry-value]
[tftp timeout timeout-value]
[security security-status]
[gui_access gui-status]
[banner banner-status]
[OEM-mode mode-flags]
```

Where:

<i>server-name</i>	set or change the name of the unit. The name can be a maximum of 14 characters. After this action, you must reboot the unit; use the command <code>reboot</code> .
<i>inet-address</i>	set or change the internet address of the unit. After this action, you must reboot the unit afterwards; use the command <code>'reboot'</code> .
<i>subnet</i>	set or change the subnet mask of your network. For information on the subnet mask parameter, see Section Initial Configuration.
<i>broadcast</i>	set or change your broadcast address. Once you have entered an IP address and subnet mask, the broadcast address will default to the IP address with the host part(s) set to 255. After this action, you must reboot the unit; use the command <code>reboot</code> .
<i>domain</i>	set or change your domain name. After this action, you must reboot the unit; use the command <code>reboot</code> .
<i>user-iphost</i>	the default ip host for all users who login to the unit. Enter an internet address in dot decimal notation; e.g. 192.101.34.202. The IP address entered here does not affect any line configuration.

<i>auth-method</i>	set the authentication method for users, when they login to the unit; the method is 'local', 'both' or 'radius'. For an explanation of these types, see JETSTREAM 4000, 8500, LANSTREAM 2000, Installation Guide, Section Initial Configuration .
<i>retry-value</i>	is the number of times the unit will attempt to transfer (using tftp) a file to/from a host. Enter a value between 0 and 255. The default value is 5. A value of 0 means that the unit will not attempt a retry should tftp fail.
<i>timeout-value</i>	is the time in seconds the unit will wait for successful transmit or receipt of tftp packets before retrying a tftp transfer. Enter a value between 1 and 255. The default value is 3.
<i>security-status</i>	By enabling security, you restrict certain types of incoming connections (reverse and printer line types and remote configuration) to the hosts or devices defined in the host table. The values are 'on' and 'off'; the default is 'off' (security disabled).
<i>gui-status</i>	use this parameter to control access to the unit's graphical configuration programme, JETset . The default is 'off'. When set to 'on' the user with username 'admin' can access the JETset program from a Web browser, using the unit's internet address. Entry to the programme is controlled by password. If you are not using JETset to configure the unit, we suggest you set this parameter to 'off'; access will be denied any person trying to connect to the unit.
<i>banner-status</i>	this parameter concerns the banner information (product name/ software version). This banner information is presented to a user with a login prompt. For security reasons you may wish to turn off the display of this information. The choices are ON or OFF. The default is OFF. This parameter does not affect logins using Telnet/Rlogin or the Admin Port; in both these cases the banner information shall always be displayed.

OEM-mode

A 16-bit store allowing 16 independent items of OEM functionality to be enabled or disabled. It is set as a hexadecimal number in the range 0000 to FFFF.

Currently 2 options are available;

OEM Menu Mode - (OEM_mode 0001), this replaces the standard "login" prompt with the text from the "OEM1" string in the custom language.

The OEM1 string can be replaced by a formatted character string of up to 300 characters. When OEM_mode has bit 0001 set and the custom language is loaded the contents of the OEM1 string are displayed as the login prompt.

This facility is useful for creating a simple user definable single level menu system.

See [Section Language support](#) and [Section netload](#) for information on configuration of the custom language.

Password Disable Mode - (OEM_mode 0002), password entry (prompt) is bypassed for users with no password set.

Setting this bit will cause the password prompt to be bypassed when no password is set for the user. It can be used in conjunction with OEM_mode 0001 to enable a simple menu system.

Any combination of the arguments can be used. Examples:

```
set server name stimp  
set server name stimp tftp retry 2  
set server internet 192.101.34.202 broadcast 255.255.255.254 ip_host  
72.96.0.2
```

Menu equivalents

server configuration

network configuration

See also

[show server](#), [set date](#), [set time](#), [show hardware](#), [reset factory](#)

set slip line

user level: Use this command to configure SLIP on a line.
admin

syntax

```
set slip line line_number parameter
```

where:

line_number may also be specified as * for all lines, or . for the current in-use line.

parameters are any from the list below:

parameter syntax	parameter name
lipaddr	local ip address
ripaddr	remote ip address
subnet	subnet mask
mtu	maximum transmission unit
priority	interactive priority
transmit_parameters	transmit parameters
icmp_suppress	suppress icmp
vj_comp	VJ compression

The meanings and values of these parameters are explained in [Section Configuring SLIP](#).

You can include multiple parameters in one line of syntax (up to a maximum of 100 characters).

Menu equivalent

Line Configuration - Line Settings

See also

[show slip line](#)

set telnet

user levels: Use this command to set telnet parameters on a line. It is available for line service types of:
admin

Direct telnet
Silent telnet

This command also sets default telnet values when you telnet to a host using the cli command `telnet`.

Syntax

```
set telnet

[line line_number]
[termtyp terminal-type]
[echo value]
[mapnl value]
[mode value]
[intr value]
[quit value]
[eof value]
[erase value]
[break value]
```

Where:

<i>line_number</i>	is the serial line number connected; for example 3
<i>terminal type</i>	is your terminal type; for example wyse60. Note this value will be ignored if you have set a <code>termtyp</code> value using the command <code>telnet</code> .
<i>echo</i>	on or off
<i>mapnl</i>	on or off
<i>mode</i>	on or off
<i>intr</i>	<hexadecimal>
<i>quit</i>	<hexadecimal>
<i>eof</i>	<hexadecimal>
<i>erase</i>	<hexadecimal>
<i>break</i>	<hexadecimal>

Note:

`echo`, `mapnl`, `mode`, `intr`, `quit`, `eof`, `erase` and `break` are telnet options.

Menu equivalent

not available in the text menus

See also

[show telnet](#), [telnet](#)

set time

user level: This command enables you to set the time in the unit. The time is used by the real-time clock. For more information on the real-time clock see JETSTREAM 4000, 8500, LANSTREAM 2000, Installation Guide, [Setting Date and Time on page 55](#).
admin

Syntax

```
set time hh:mm [:ss]
```

for example; set time 11:23

Optionally you can specify the number of seconds; e.g. set time 11:23.30

Menu equivalent

Main Menu - hardware

See also

[set date](#), [show time](#)

set user

user levels: This command enables you to modify a user's setup, including predefined sessions. An admin user can change any user's setup. A normal user can only change certain elements of their own setup, e.g. password and language.
admin, normal

Syntax

```
set user username/ .  
  
[language language-name]  
[password]  
[level user-level]  
[switch switch_character]  
[service user-service]  
[ip_host iphost-address]  
[tcp_port t-port number]  
[callback callback-flag]  
[phone_number phone-number]  
[idle_timer i-timer value]  
[sess_timer s-timer value]
```

```
[framed_ip f-ip address]
[framed_netmask f-netmask]
[framed_mtu f-mtu value]
[framed_compression f-compression value]
[session n .....]
```

Where:

<i>language-name</i>	is either english or customlang (a language of your choice, either supplied or translated; see Section Language of your choice).
<i>password</i>	if you include this argument you will prompted to enter a new password.
<i>user-level</i>	is 'admin', 'normal', 'restricted' or 'menuing'. For an explanation of these terms see Section User Levels .
<i>switch-character</i>	is the hex value of the 'hot-key' used for switching sessions. The default is 1 (^a). See the ascii code chart in Appendix E (ASCII and HEX conversion tables) .
<i>user-service</i>	select one of: jsprompt, telnet, rlogin, tcp_clear, slip or ppp. For more information on these user services see Section Configure a User Account .
<i>iphost-address</i>	(use only when you have selected a service of 'telnet' or 'rlogin'); select: 0.0.0.0 for the unit to select the default host set for all users; see Section set server . 255.255.255.255 for the unit to prompt the user for the ip address or name of the host to which he/she wishes to connect n.n.n.n (where n is a number) for any other ip address of your choosing (as system administrator); e.g 192.65.144.6
<i>t-port number</i>	(use only when you have selected a user-service of 'telnet') enter the TCP port number of the host with which the unit should start the service. The default port is 23; in most cases you can use the default value.
<i>callback-flag</i>	whether the unit calls the user back when he/she connects to the unit (a security feature). Set either 'on' or 'off' (default is 'off'). When 'on', enter a phone number (see below).
<i>phone-number</i>	a number which the unit will dial to callback the user (you must have set 'callback' to 'on'). Enter the number without spaces. To change the phone number, overwrite the previous entry.

<i>i-timer value</i>	enter a period in seconds for which the idle timer will run. Use this timer to close a connection because of inactivity. When the idle timer expires, if there has been no exchange of data, the unit will end the connection. The default value is 0 (zero), meaning that the idle timer will not expire (the connection is open permanently). The maximum value is 2^{32} seconds. The idle timer (here) will override the idle timer which you can configure for a line.
<i>s-timer value</i>	enter a period in seconds for which the session timer will run. Use this timer to forcibly close a user's session (connection). When the session timer expires the unit will end the connection. The default value is 0 (zero), meaning that the session timer will not expire (the session is open permanently, or until the user logs out). The maximum value is 2^{32} seconds. The session timer (here) will override the session timer which you can configure for a line.
<i>f-ip address</i>	use only when the user service field is set to 'slip' or 'ppp'; for more information see Section Configure a User Account , sub-section framed ip .
<i>f-netmask</i>	ignore this parameter; it is reserved for future use.
<i>f-mtu value</i>	use only when the user service field is set to 'slip' or 'ppp'; for more information see Section Configure a User Account , sub-section framed mtu .
<i>f-compression value</i>	use only when the user service field is set to 'slip' or 'ppp'; for more information see Section Configure a User Account , sub-section framed compression .
<i>session</i>	use this argument to predefine sessions for the user. You can predefine one specified session (<i>n</i>), or all sessions (*). It takes the arguments defined below:

Session arguments

```
... session n/* type telnet/rlogin host hostname [termtyp  
termtyp] [auto on/off] [echo on/off] [mapnl on/off] [mode  
on/off] [intr <hex>] [quit <hex>] [eof <hex>] [erase  
<hex>] [break <hex>]
```

You must specify the type and hostname. The other arguments are optional. The arguments after `auto` are telnet options.

You can use any number or combination of the arguments. Use the ? command to list the options for each one. An example is given below:

```
set user julie level normal switch 02 session*  
type telnet host socrates termtype wyse60
```

This command has set up four predefined telnet sessions on host socrates for user 'julie'.

Notes

1. You can set all users to the same parameters by using the * asterisk character, e.g.

```
set user * language french
```

will set all users to this language value.

Menu equivalent

Users - Change User/Set Password

See also

[add user](#), [netload](#), [show user](#), [delete user](#), [show telnet](#)

show ARP

This command is used to display the current ARP table. This is useful for diagnostic and debugging purposes.

This parameter is only accessible from the unit's CLI.

Syntax

```
show arp
```

See also

[delete ARP](#)

show date

user levels: This command enables you to show the date in the unit; e.g.
admin, normal `date2/2/1999`

Syntax

```
show date
```

Menu equivalent

Main Menu - hardware

See also

[set date](#), [set time](#), [show time](#), [show hardware](#)

show gateways

user levels: Use this command to list the gateways you have defined. The list will be displayed in the following format:
admin, normal

Hostname	Type	Internet Address	Status
socrates	default		Active
plato	host	192.65.144.4	Passive

If you have not entered gateway information your command will be ignored; you will be presented with the unit prompt once more.

Syntax

show gateways

Menu equivalent

Network Configuration - Gateways - Change Gateway

See also

[add gateway](#), [delete gateway](#), [set gateway](#)

show hardware

user level: This command displays the hardware configuration of your unit. An example display is:
admin, normal

```
JS_8500# show hardware
mac address      0080ba60330c
board id         JS4300076R1.5
processor        80386
uarts            3 * Serial ASIC
flash rom        1 x 1MB
ram              2 x 2MB
battery ram      32kB
serial ports     24
ethernet interface auto
ethernet speed   10M
date             13/5/2003
time             14:16:17
JS_8500#
```

Syntax

```
show hardware
```

Menu equivalent

Main Menu - Hardware

See also

[set date](#), [set time](#), [show line](#), [show parallel](#)

show hosts

user levels: Use this command to list the contents of the host table:
admin, normal

```
JS_8500# show hosts
hostname          internet address
pc                172.16.28.100
Solaris           172.16.0.2
router312        172.16.1.2
sco               172.16.113.115
JS_8500#
```

Syntax

```
show hosts
```

Menu equivalent

Network Configuration - Host Table - Change Host

See also

[add host](#), [delete host](#), [set host](#)

show interfaces

This command will show all lines with active SLIP or PPP links. It is useful for monitoring the status of dial-up lines. This parameter is only accessible from the unit's CLI.

Syntax

```
show interfaces
```


show line

user levels: This command can be used to display the configuration of a single line or all lines, of the front-mounted serial RJ45 ports only. Admin users can show all lines, normal users can only display the configuration of their own line. The command does *not* show :

- the Admin Port line configuration; this is fixed - see the Installation Guide, [The Admin Port on page 37](#).
- the parallel port line configuration; see the command `show parallel`.

For a single line the display will look similar to this:

```
JS_8500# show line 14
speed                9600
terminal             dumb
dial                 none
flow                 none
bits                 8
parity               N
stop                 1
pages                4
phone number
modem name           none
idle timer           0
session timer        0
routing              none
service              jslogin
hostname             pc
host port            23
JS port              23
current user
JS_8500#
```

If you specify all lines, the display will look similar to this:

```
JS_8500# sh li *
line speed service
1 9600 jslogin nouser
2 9600 jslogin nouser
3 9600 jslogin nouser
4 9600 jslogin nouser
5 9600 jslogin nouser
6 9600 jslogin nouser
7 9600 jslogin nouser
8 9600 ppp nouser
9 9600 jslogin nouser
10 9600 jslogin nouser
11 9600 jslogin nouser
12 9600 jslogin nouser
13 9600 jslogin nouser
14 9600 jslogin nouser
15 9600 jslogin nouser
16 9600 jslogin nouser
17 9600 jslogin nouser
18 9600 jslogin nouser
19 9600 jslogin nouser
20 9600 jslogin nouser
21 9600 jslogin nouser
22 9600 jslogin nouser
< hit any key >
23 9600 jslogin nouser
24 9600 jslogin nouser
JS_8500#
```

Note that the user shown in the right-hand column is the ‘current user’ i.e. the user currently logged in on that line. ‘Nouser’ means there is not a user currently logged in.

Syntax

```
show line line_number
```

Where *line_number* is :

.	the current line.
<i>n</i>	a specific line number.
*	all lines

Menu equivalent

Line Configuration - Line Settings

See also

[*set line, show user, show parallel*](#)

show modems

user levels: Use this command to show modem details held by the unit.
admin, normal

Syntax

```
show modem
```

This will show (for example):

name	initialisation string
Hayes	
US Robotics	
Courier	

Menu equivalent

Line Configuration - Modems - Change Modem

See also:

[add modem](#), [delete modem](#), [show line](#)

Note *To change modem details in the cli you must 'delete' the modem, then 'add' it again, with the changed details.*

show parallel

user levels: If you have a parallel port(s) fitted, this command can be used to display the configuration of a single parallel line or all parallel lines.
admin

For a single line the display will look similar to this:

```
js 8500# sh pa 1

service           printer
hostname          plato
host port         23
JS port           23
```

If you specify all lines (and you have more than one parallel port fitted), the display will look similar to this:

```
js 8500# sh pa *

line  service    hostname    host port    JS port
1     printer     homer      23           23
2     rev raw      sophocles  23           23
```

Syntax

```
show parallel line_number
```

Where *line_number* is :

.	the current line.
<i>n</i>	a specific line number.
*	all lines

Menu equivalent

Line Configuration - Parallel Port Settings

See also

[set parallel](#), [reset parallel](#), [kill parallel](#), [show hardware](#)

show ppp line

user levels:
admin,
normal

Use this command to show the PPP configuration of a line. Admin users can show all lines; users with normal level privileges can only display the configuration of their own line.

syntax

```
show ppp line line_number
```

where:

line_number may also be specified as * for all lines, or . for the current in-use line.

parameters are any from the list below:

parameter syntax	parameter name
lipaddr	local ip address
ripaddr	remote ip address
subnet	subnet mask
accm	asynchronous character control map
mru	maximum receive unit
security	security
user	user
password	password
ruser	remote user
rpassword	remote password
ac_comp	address/control compression
proto_comp	protocol compression
vj_comp	VJ compression

parameter syntax	parameter name
magic_neg	magic number negotiation
ipaddr_neg	ip address negotiation
cr_tmout	'configure request' timeout
tr_tmout	'terminate request' timeout
cr_retry	'configure request' retries
tr_retry	'terminate request' retries
nak_retry	'configure nak' retries
auth_tmout	authentication timeout

The meanings and values of these parameters are explained in [Section Configuring PPP](#).

Menu equivalent

Line Configuration - Line Settings

See also

[set ppp line](#)

show radius

user levels: Use this command to check the RADIUS settings of the unit:
admin, normal

Syntax

```
show radius
```

The output of this command are the RADIUS settings of the unit (e.g.):

```
primary authentication host plato
secondary authentication host homer
primary accounting host plato
secondary accounting host homer
retry 3
timeout 1
auth_port 1645
acct_port 1646
acct_authenticator on
accounting on
session id d0000000
```

For details of these parameters, see JETSTREAM 4000, 8500, LANSTREAM 2000, Installation Guide, [Section RADIUS configuration](#).

Menu equivalent

radius configuration - radius settings

See also

[add radius](#), [set radius](#), [set server](#)

show routes

user levels: Use this command to give you a better understanding of your network. It will also show a single passive gateway configured using bootp. Below is an example:
admin, normal

Destination	Gateway	Flags	Refs	Use	Interface
192.101.35.192	192.101.35.217	U	1	1	1e0
0.0.0.0	192.101.35.217	UG	0	0	1e0

Syntax

```
show routes
```

Menu equivalent

there is no menu equivalent

Note *this command is synonymous with the 'netstat -r' command on most Unix systems. See the manpages (type "man netstat" on your Unix system for more information).*

See also

-

show server

user levels: This command displays the base configuration of the unit, for example:
admin, normal

```
servername                stimpv
internet address          192.65.144.91
subnet mask                255.255.255.0
broadcast address         192.65.144.255
domain name                perle.com
ip_host                   191.243.221.254
DNS
  primary                  192.165.144.5
  secondary                192.165.144.7
WINS
  primary                  192.101.34.211
  secondary                192.101.34.213
tftp retry                 5
tftp timeout              255
security                   off
authentication             local
gui_access                 off
banner                     off
```

Fields which are unconfigured will not appear in the list on your screen.

Syntax

```
show server
```

Menu equivalent

server configuration

See also

[set server](#), [show hardware](#)

show sessions

user levels: This command lists your active sessions (including active predefined sessions), for example:

admin normal 1 telnet socrates

Syntax

```
show sessions
```

Menu equivalent

User - Set Up User - Set Sessions

See also

[resume](#)

show slip line

user levels: Use this command to show the SLIP configuration of a line. Admin users can show all lines; users with normal level privileges can only display the configuration of their own line.
admin, normal

syntax

```
show slip line line_number
```

where

:*line_number* may also be specified as * for all lines, or . for the current in-use line.

parameters are any from the list below:

parameter syntax	parameter name
lipaddr	local ip address
ripaddr	remote ip address
subnet	subnet mask
mtu	maximum transmission unit
priority	interactive priority
transmit_parameters	transmit parameters
icmp_suppress	suppress icmp
vj_comp	VJ compression

The meanings and values of these parameters are explained in [Section Configuring SLIP](#).

Menu equivalent

Line Configuration - Line Settings

See also

[set slip line](#)

show snmp

user levels:
admin, normal

This command shows the configuration of the unit for SNMP support; for example:

```
snmp contact          miked
snmp location         x235
snmp communities:    1. homer 192.65.144.78 read/write
                    2. local 192.65.144.2.55 read only
snmp traps:          1. local 192.65.144.255
```

Syntax

```
show snmp
```

Menu equivalent

network configuration - snmp

See also

[add community](#), [add trap](#), [set contact](#), [set location](#)

show telnet

user levels: Use this command to show telnet parameters on a line. Note that telnet parameters shown here apply only to line service types of:

admin, normal

Direct telnet

Silent telnet

The command also shows telnet parameters entered using the command `set telnet`.

```
JS_8500# show telnet line *
line echo mapnl mode intr quit eof erase break terminal
1 off off off 7f 1c 04 08 1d vt100
2 off off off 7f 1c 04 08 1d vt100
3 off off off 7f 1c 04 08 1d vt100
4 off off off 7f 1c 04 08 1d vt100
5 off off off 7f 1c 04 08 1d vt100
6 off off off 7f 1c 04 08 1d vt100
7 off off off 7f 1c 04 08 1d vt100
8 off off off 7f 1c 04 08 1d vt100
9 off off off 7f 1c 04 08 1d vt100
10 off off off 7f 1c 04 08 1d vt100
11 off off off 7f 1c 04 08 1d vt100
12 off off off 7f 1c 04 08 1d vt100
13 off off off 7f 1c 04 08 1d vt100
14 off off off 7f 1c 04 08 1d vt100
15 off off off 7f 1c 04 08 1d vt100
16 off off off 7f 1c 04 08 1d vt100
17 off off off 7f 1c 04 08 1d vt100
18 off off off 7f 1c 04 08 1d vt100
19 off off off 7f 1c 04 08 1d vt100
20 off off off 7f 1c 04 08 1d vt100
21 off off off 7f 1c 04 08 1d vt100
< hit any key >
22 off off off 7f 1c 04 08 1d vt100
23 off off off 7f 1c 04 08 1d vt100
24 off off off 7f 1c 04 08 1d vt100
JS_8500#
```

Syntax

```
show telnet line line_number
```

Where:

line_number is the serial line number connected

Menu equivalent

not available in the text menus

See also

set telnet

show time

user levels: This command enables you to show the time as measured by the real-time clock in the unit; e.g.
admin, normal time11:04:32

Syntax

```
show time
```

Menu equivalent

Main Menu - hardware

See also

[set date](#), [set time](#), [show date](#), [show hardware](#)

show user

user levels: Use this command to display a user's setup, including predefined sessions. The admin user can show details of any user, a normal user can only view their own details:

```
JS_8500# show user julie
username          julie
language          english
screen switch    01
level            normal
service          jsprompt
ip_host          0.0.0.0
tcp port         23
callback         off
phone number
idle timer       0
session timer   0
framed ip       255.255.255.254
framed netmask  0.0.0.0
framed mtu      1500
framed compression on
routing         none
  type      hostname  auto echo mapnl mode  intr quit  eof  erase  break terminal
1 telnet   pc          off  off  off  off  7f  1c   04  08   1d
2 telnet   Solaris    off  off  off  off  7f  1c   04  08   1d
JS_8500#
```

Syntax

```
show user ./username
```

Where:

`.` specifies the current user.
`username` is the name of a specific user.

Menu equivalent

Admin user: Users - Change User/Set Sessions.

Normal user: Sessions - Set Up User/Set Sessions

See also

[set user](#)

start

all users

Use this command to start a predefined session. This is a particularly important command for restricted users who can only start sessions predefined for them by system administrator. If you are using telnet, the target host will prompt you for your login name. If you are using rlogin, the host will prompt you for your password. If you are using rlogin and your unit's login name is entered in the 'rhost' file of the target login directory, you will be logged straight in.

Syntax

```
start n
```

Where *n* is the predefined session that you want to start.

Menu equivalent

Sessions - Start Predefined Session

See also

[resume](#)

telnet

user levels:
admin, normal

This command will establish a connection with another host on the network using the telnet protocol. You must specify the target host but the other arguments (such as echo, mapnl, mode, etc.) are optional. If you do not specify the other arguments the line telnet values will be used (values set/shown in `set telnet` or `show telnet`)

If you do specify arguments such as echo, mapnl, mode, etc. the values you enter will override the line telnet values. Note that your values (specified here using the `telnet` command) expire when your telnet session is finished; values set/shown in `set telnet` or `show telnet` can be saved permanently.

When the connection is made you will be prompted for your login name.

Syntax

```
telnet hostname/inetaddress [termttype termttype] [echo on/off] [mapnl on/off] [mode on/off] [intr <hex>] [quit <hex>] [eof <hex>] [erase <hex>] [break <hex>]
```

Where:

<i>hostname/ inetaddress</i>	is the name or internet address of the machine you want to log into
<i>termttype</i>	is your terminal type. This argument enables you to pass your terminal type to the host. When connecting to a UNIX host, you must define the termttype in accordance with its UNIX TERM variable. The termttype argument overrides a termttype value entered into the unit when using the <code>set line</code> or <code>set telnet</code> commands.
echo, mapnl, etc.	these are telnet options. They set values once only, for the duration of a single telnet connection. See comments under Section telnet above.

Menu equivalent

Users - Set Sessions (*to set default values*)

or

Sessions - Start telnet (*to use or override default values*)

See also

[kill session](#), [resume](#), [rlogin](#), [set telnet](#), [show sessions](#), [show telnet](#), [start](#)

version

user levels: This command tells you what version of software your unit is running.
admin, normal

Syntax

```
version
```

Menu equivalent

Version of software is displayed at the top of any menu display, e.g. :

```
user [admin]   JETSTREAM 2.00 i.1           telnet 1
```

The text in the middle of the line (JETSTREAM) will display the name of your product.

Appendix A Summary of Line Service Types

When you are configuring a line on the JETSTREAM 4000, 8500 or LANSTREAM 2000 (the 'unit') you will find a parameter for a line called 'service'. The detail of types of line service available are shown below.

Note do not confuse line 'service' with user 'service'. User 'service' is a completely different parameter from line 'service' and is used by the unit in different ways.

Line Service Type	Description/Uses	Example	How to setup
Bidir	Allows a bidirectional modem connection on a port	A UUCP connection for batch file transfer and printing.	Section Host to host: bidirectional Modem Connections
Direct telnet or rlogin	When using the unit as a Terminal Server, to bypass the unit and allow users to login straight into a specific host. <i>These are non-permanent connections</i>	Users on terminals.	Section Login direct to host
Direct Raw	Enables external non-login devices to access TCP/IP servers via the unit. No authentication will take place. The connection is set up from the unit to a TCP/IP network host (the opposite of Reverse Raw). <i>These connections are established by pressing <return>.</i>	On dialin connections: user applications for devices such as bar code readers and smart cards.	in the same way as a 'silent raw' connection; see Section External host: Dialin Modem Connections
jslogin	The default connection. The unit presents a login on that line.	<ul style="list-style-type: none"> a) System administrator to do unit configuration b) Users to starting the unit's sessions to hosts. c) Providing authentication of a user before starting a user 'service' of SLIP 	for b) Section Login for Sessions for c) Section Setting Up the Line

Line Service Type	Description/Uses	Example	How to setup
PPP	a) Remote access connection b) Using the unit as a router (two units back-to-back)	A mobile employee Joining together two networks	Section Setting Up the Line and Section Configuring PPP
Printer	Using the unit as a printer server	Remote printing using LPD or RCP	Section Remote Printing using LPD and Section Remote Printing Using RCP
Reverse Raw	Simple pipe between a TCP/IP host and a machine/device attached to a port on the unit. The connection is set up from the TCP/IP host on the local network to the unit (the opposite of Direct Raw and Silent Raw).	To access printers or dialout modems (with separate host-based print/modem handling software).	Section Remote Printing Using Host-Based Print Handling Software see also: Local host: Dialout Modem Connections on page 44
Reverse Telnet	Enables a TCP/IP host to establish a login connection on an external machine attached to a port	To access machines like protocol converters or statistical multiplexors.	Section Reverse Telnet connection
Silent telnet or rlogin	When using the unit as a Terminal Server, to bypass the unit and allow users to login straight into a specific host. <i>These are permanent connections, therefore consume system resources</i>	Users on terminals.	Section Login direct to host

Line Service Type	Description/Uses	Example	How to setup
Silent Raw	Enables external non-login devices to access TCP/IP hosts via the unit. The connection is set up from the unit to a TCP/IP network host on the local network (the opposite of Reverse Raw). <i>These connections are established automatically;</i> they are suitable for computer to computer communications.	Dialin connection from an external host machine.	Section External host: Dialin Modem Connections
SLIP	a) Remote access connection b) Using the unit as a router (two units back-to-back)	A mobile employee Joining together two networks	Section Setting Up the Line and Section Configuring PPP

Appendix B Troubleshooting

Introduction

This appendix contains solutions for problems that may arise while using the JETSTREAM 4000, 8500 or LANSTREAM 2000 (the 'unit').

- if you bought your unit from a registered Perle Supplier, you must contact their Technical Support department; they are qualified to deal with your problem.
- if you are a registered Perle Supplier, and bought your unit from Perle, please contact the Technical Support department of your nearest Perle office. The addresses and telephone numbers of your nearest Perle office are contained in [Appendix F \(Contacting Perle\)](#).

Contents

- [General communication matters](#)
- [BOOTP/DHCP problems](#)
- [Callback problems](#)
- [Host problems](#)
- [Hub problems \(LANSTREAM only\)](#)
- [JETset problems](#)
- [Language problems](#)
- [Login problems](#)
- [Modem problems](#)
- [MTSD problems](#)
- [PPP problems](#)
- [Printing problems](#)
- [Saving to FLASH memory](#)
- [Telnet/Rlogin problems](#)
- [Problems with terminals](#)
- [Emergency Recovery](#)

General communication matters

General communication checks and practices are as follows:

- ping your host; if you cannot ping at all, check the cabling between the unit and your network. If you can ping but packet loss is reported, ping another host/device on the same network. You will appreciate whether the problem is specific to a host/device or general to the network. If there is a problem with the network check the state of the network, including number of nodes.
- after entering or changing ip information for your unit (internet address, broadcast address, subnet mask) *reboot the unit* (does not apply when using BOOTP or DHCP). Once the unit has rebooted other network devices can communicate with it (ping, telnet, etc.). Also, protocols such as ARP and proxy-ARP will work properly

If you don't reboot unit the ip information you have entered/changed will not be recognised by other network devices.

- use the *show routes* command (command line only). See if there a route to the host?
- implement load-balancing in your network by distributing the processing. For example, try not to cluster devices on the unit which require high throughput.
- ensure routes to/from your host are as direct as possible; e.g. ensure the unit is on the same network as your host so that bridges/routers do not act as bottlenecks.
- if your network is congested, subnet it with a bridge; however, bear in mind the recommendations in the previous paragraph.

BOOTP/DHCP problems

Messages: "host name too long" or "filename too long"

- the unit can only accept hostnames or filenames of the same maximum length as permissible in the text menus or cli.

Problem: DHCP or BOOTP have been set up to configure my unit but does not seem to have done anything.

Check: Check that the server dhcp parameter is set to on, if not set it to on and reboot.

If your unit is brand new or has been factory reset, you may see the message:

INIT: Attempting Rarp

This means that you have no active BOOTP or DHCP servers on your network.

Check that your BOOTP server is configured for your unit or that your DHCP server has an active lease pool (scope) with at least 1 free IP address.

Problem: You observe TFTP errors when the unit boots, for example:

TFTP: File not found : filename

TFTP: Timed out

This has a number of causes, including:

- The filenames you specified to BOOTP/DHCP do not exist or are in the wrong place.
- DHCP has previously leased bootfile information to the unit (which it has stored for the duration of the lease), but you have since changed the location or name of the bootfile.
- Your DHCP/BOOTP server has no TFTP server running and/or the server for any of the downloadable files in your bootfile has no TFTP server running.

Check: Ensure that lease data in your DHCP server manager is correct.
 Reset or restart the DHCP server.

If this does not resolve the problem, the DHCP lease can be restarted by resetting the unit to factory defaults and rebooting. We recommend that you store your unit's configuration before doing this. It can then be reloaded when the unit is booting from DHCP correctly.

Callback problems

fixed callback is on but the unit is not calling the user back

other factors: you have a phone number configured for that line.

- enter a phone number *for the user*. The unit will only callback using the number configured for that user; this is a different 'number' parameter from the number you can configure for a line.
- check the modem at the user's end is set to 'auto-answer'.

Host problems

Cannot access a host by name

- if using DNS or if DNS is required, ensure a nameserver is configured on your unit and is accessible (ping it).
- if not using DNS, ensure the host is configured in the host table. Check access to the host by pinging it using the host's IP address.

Cannot access a host on a local network

ensure:

- the network address is correct.
- the subnet mask is set correctly and reflects the network configuration.
- the broadcast address is set correctly and reflects the network configuration.

Cannot access a host on a remote network

- use the *show route* command to verify that there is a route to the remote host. If no gateway is specified, ensure a default gateway is specified. Ping the default gateway to check if it is working.
- Consider the situation beyond the gateway; e.g. are intermediate gateways and the remote host available? Also, check the messages returned by the *show route* command; e.g. that a particular host or gateway is unreachable.

Gateways added into the gateway table are ignored by the unit

- have you used BOOTP and entered a single static gateway in the bootptab file entry? If yes, the other gateways will be ignored. See 8500 Configuration Guide [How to setup BOOTP on page 102](#) for more information

Access to host lost after a few minutes

- If the route to this host goes through routers, make sure those routers are all sending RIP packets across the networks.

You see a message saying your host is in use.

- delete your host as either, a DNS or WINS host, or a gateway, then retry the 'delete host' command/menu item. You may have configured your host as a DNS or WINS host, or a gateway.

The connection fails when the user 'ip_host' parameter is set to 0.0.0.0

other factors: several hosts are entered in the unit's host table

- check the host ip address entered in the server configuration; it is this ip address - and not hosts in the host table - which the unit will use when a user's ip_host is set to 0.0.0.0

Hub problems (LANSTREAM only)

You have a connection into the 10BaseT 'uplink' port (on rear panel), but you cannot communicate to your connected device.

- On the 'uplink' port check if the green 'Link OK' LED is on. If the LED is off you have a bad link. This is probably caused by the switch marked 'HUB - UPLINK'(next to the port) being in the wrong position. Move the switch to the opposite position. Now see whether the 'Link OK' LED is on (steady green); if the LED is on you have a good link.
- Check that the Receive and Transmit signal pairs are connected as follows:

Connected device	direction of signal	LANSTREAM
Receive pair	<—————	Transmit pair
Transmit pair	—————>	Receive pair

JETset problems

Trying to access JETSET you see an 'alert' dialog box, e.g. :

Figure 33



- change the parameter 'gui_access' to 'on'.

Problems with JETstart

- Problem:** I can't save the configuration generated with JETstart.
Check: You need to set up JAVA applet security before you can save a file to your hard disk.
- Problem:** I need to use the scroll bars to see the whole applet.
Solution: Drag the frame bar dividing the title frame from the applet frame to the top of the browser window.
- Problem:** JETstart applet doesn't load.
Check: Check your browser version against the list of supported versions.
- Problem:** Can't see all the text in an error message.
Solution: Click OK and cause the error to re-occur. The text will then be visible.

Language problems

in a customised language, the text strings appear in the wrong place in the text menus and cli.

- check the original ascii text file you used to translate to your customised language. The sequence of lines must be maintained; so if 'set line' appeared on the 60th line in the original file, the translation of 'set line' in your custom language must appear on the 60th line in your language file.

Login problems

For login problems see also '[Section Telnet/Rlogin problems](#)'

User is waiting up to 60 seconds before login is accepted or denied

other factors: authentication is set to 'both' or 'RADIUS'. User has entered username and password, and has pressed <return> key.

- check RADIUS configuration of primary and secondary authentication/accounting hosts specified, and you have retry and timeout values greater than the default, the unit will be spending time trying each of these hosts and keeping the user waiting.
- adjust RADIUS configuration: specify just one host, reduce timeout and retry values to the default or less than default.

You cannot progress beyond the 'login' and 'password' prompts (when authentication is set to either 'both' or 'RADIUS')

- check the setting of 'account_authenticator' flag is the same in the unit and the RADIUS host; either they should both check or both ignore the authenticator field. If you are not sure, change the setting in the unit; see if this fixes the problem.
- on the RADIUS host check the secret (password); you should see it displayed in clear text in the RADIUS clients file. If you are unsure whether it is the same secret which you entered in the unit, go to the unit and re-enter a new secret.
- on the RADIUS host check there is only one entry for a particular user; do not have multiple entries of the same username (although passwords may be different).

You cannot obtain a login on *any* of the front-mounted ports

- Connect via the Admin port and check the settings of the front-mounted ports; they have probably been set to 'direct' or 'silent' telnet/rlogin.

You have lost or don't know your password (as 'admin' user)

- you must reset the unit to its factory default settings using the 'reset' switch on the rear panel. There is no procedure to access the unit without a password.

Using a terminal, you see garbled characters or no characters at all

other factors: you are connecting to the unit from a terminal via a modem

- your terminal is set to a different baud rate to the line into the unit. Send a line break (<break> key) and the unit will try the next line speed setting. For more information see [Section Logging in](#).

Error message: 'Warning: Baud Rate Changed to new_speed'

other factors: you are connecting to the unit from a terminal via a modem

- you will see this message after sending a line break (<break> key); the unit has tried the next line speed setting. Your action is acceptable: your terminal is set to a different baud rate to the line. For more information see [Section Logging in](#).

Modem problems

the unit is not initializing the modem

- check your line service is set to jslogin, slip or ppp. If your line service is set to any other type, the unit will not initialize a modem. You will need to configure the modem manually.

see also [Login problems](#)

MTSD problems

MTSD works erratically

- On some operating systems, the system timeouts used to establish and break network connections can disrupt the operation of MTSD. To avoid this, check the arguments you are using with MTSD commands. Type `mtsd -help` and see the applicability of each command.
- Include or take-out arguments which you feel are appropriate.

see also [Printing problems](#)

PPP problems

the link fails on start-up (problem #1)

other factors: there are remote ip addresses set for both a user ('framed ip' value) and a line ('remote IP address').

- check the IP address set for the user; this is used in preference to the ip address set for a line. If there is a problem with the user's IP address, negotiation will fail; the unit will *not* use the line's IP address as an alternative.

the link fails on start-up (problem #2)

other factors: security (either PAP or CHAP) is enabled on the line.

- check the remote client/device has the same setting; i.e. PAP if the unit is using PAP. The unit does not perform negotiation with the remote end over PAP or CHAP.

at the remote end the client software locks up

other factors: security (CHAP) is enabled on the line.

- disable CHAP re-challenge parameter (`challenge_interval`) in the unit. Some PPP client software does not work when receiving CHAP re-challenges.

Printing problems

the print job fails to print on the device attached to the serial or parallel ports

- on the line where the printer is attached, set line service to `printer`. Print jobs will not print when the line service is set incorrectly.

**when using RCP, the network host receives a rejection message from the Perle unit.
The result is that the print job does not take place.**

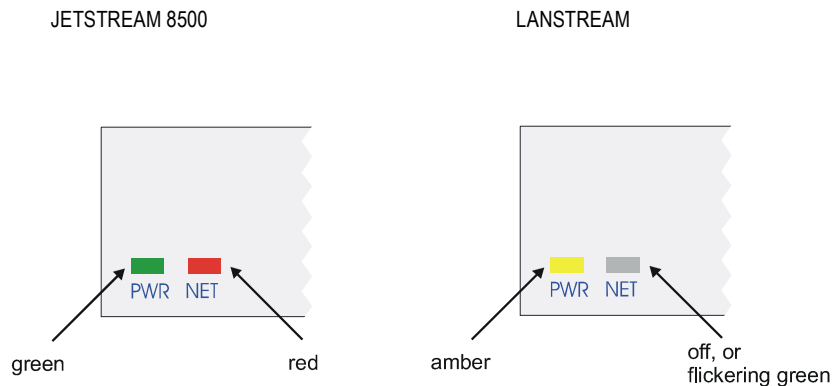
- print using LPD, *or*
- modify the printer interface scripts on the network host to overcome this weakness of RCP. The modification will force the network host to continue trying to send the print job when the unit's printer port is busy.

Saving to FLASH memory

The POWER and NETWORK LEDs display the following colours:

(as shown in [Figure 34](#))

Figure 34 LED display: failure of load to FLASH



The Network LED flickers green if network traffic is identified on the network ports.

- If you were loading a new version of software try again using the Admin Port. The save to FLASH has failed.

Telnet/Rlogin problems

For login problems see also '[Section Login problems](#)'

Message 'unauthorised client' when using telnet (or rlogin) to access the unit via a network port:

- check the 'security' feature. Security may be 'on' in the unit and you are trying to access the unit via an unauthorised host.

Message 'no pseudo devices available' when using telnet (or rlogin) to access the unit via a network port:

- there are already the maximum number of telnet/rlogin sessions connecting to the unit via its network port. Close down one of the other sessions.

Problems with terminals

see also: [Section Login problems](#).

The following section concerns problems with the appearance of data on your terminal screen:

The unit logs me out after a few minutes

- Change the idle timeout value set for the user. The idle timeout for all users is set to 300 seconds (5 minutes) by default, because the unit is designed for remote access connections (using SLIP or PPP).

Corrupt data

- check your line settings (baud rate, stop bits, etc.)

Missing data

- ensure the same type of flow control is set in both your terminal and on the unit's port.

Error message 'not permitted on a dumb terminal' after typing the cli command 'screen'

- set your line to 'termtype' VT100, ansi or Wyse60 (or other form of terminal emulation, if you have downloaded one). The default line type in the unit is 'dumb' which does not support the graphics characters necessary to view the text-based menus.

Screen corruption when using the text-based menu system

- check that the terminal setup in the unit matches your terminal.
- check that entries in the term file match your terminal setup.

- if using a PC/computer, ensure the type of terminal emulation selected in your application matches those supported by the unit. If you still have the problem, you may be suffering with poorly written terminal emulation in your application. Instead use the command line mode; if you have a web browser use JETset.

When using the function keys on your keyboard, nothing happens or your sessions keep swapping.

- Change your screen switch character. The function keys on the keyboards of some terminals (e.g. Wyse 60) send character sequences which begin with ^a; unfortunately, ^a is also the default screen switch character, or 'hot-key', which you use to switch between sessions. A valid alternative would be ^b (hex=02).

If you are the system administrator, you can change any user's screen switch character.

When using a downloaded terminal definition, you are having problems using arrow keys.

- Use Ctrl-K, Ctrl-J, Ctrl-H and Ctrl-L for up, down, left and right respectively.

When switching from a session back to the text menus, both screen images are superimposed.

- Press ^r to redraw the screen.

INIT: Error in terminal file <filename>

- This error indicates that you have exceeded the 80 character limit for one or more of the terminal capabilities defined in the reported file.

INIT: Error on line *n* in terminal file <filename>

- You have omitted the '=' sign from the reported line.

Problems with Framed Routing

- Problem:** My SLIP/PPP link is running but I am not seeing any routing information propagated to my dial up clients.
- Check:** Make sure that SLIP/PPP links are configured for route broadcasts, see section 9.1. Wait for 30 seconds before checking again for new routes, routes are broadcast every 30 seconds.
- Problem:** I can talk to my dial-up clients, but not any other machine on the network it is attached to.
- Check:** Make sure that your dial-up client is configured to pass on RIP (routing) packets to it's other network interfaces. This may involve installing additional routing software on some operating systems.
- Problem:** I have configured framed routing for a SLIP/PPP link but routing does not work.

Check: Both Remote IP Address and Local IP Address need to be configured with valid IP addresses for framed routing to remote clients to operate.

Emergency Recovery

Problem:

You have a unit already configured and,

- you do know your password, but
- have lost, misconfigured or don't know the IP address of the unit, and
- you cannot obtain a login on any port (including the console port)

The emergency recovery method is to use BOOTP (see [Section BOOTP](#)).

- Setup a host machine on your network to run BOOTP. Using the ethernet address of the unit (printed on the base of the product) BOOTP will assign the unit a known IP address.
- Now, you should be able to telnet into the unit and change its IP address.

Using BOOTP to recover access to your unit in this manner will preserve all configuration settings - apart from the IP address.

Appendix C SLIP and PPP overview

Introduction

This appendix describes the main features of SLIP and PPP.

SLIP

Overview

The Serial Line Interface Protocol (SLIP) is a simple but crude protocol for transporting IP datagrams over serial links; (a datagram is defined as a number of bytes of user information sent from the sender to the receiver). It is an old protocol dating back to the mid-nineteen eighties. It is specified in RFC 1055; see Appendix D (References).

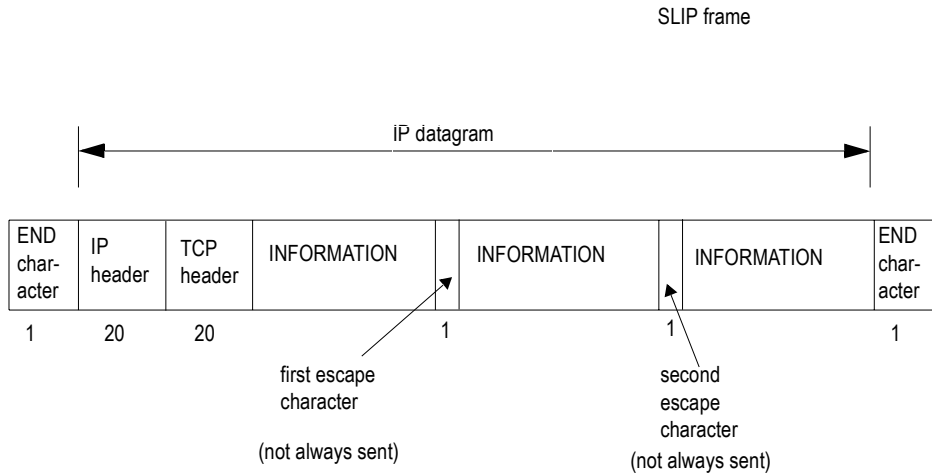
SLIP has two forms: SLIP and compressed SLIP (C-SLIP). The unit supports both SLIP and C-SLIP; the default version is C-SLIP. See C-SLIP on page 237 for more information on C-SLIP.

The way SLIP encapsulates IP datagrams is shown in Figure 35. The datagram is terminated by a special character called END. Most applications also transmit an END character at *the beginning of* a datagram, to prevent line noise being interpreted as part of the datagram.

There may be one or two ESCAPE characters, depending on the content of bytes in the information fields. Therefore the ESCAPE characters are not always transmitted. In our example the number of bytes in the SLIP frame is the length of the IP datagram plus an overhead of 4 bytes.

SLIP has a number of deficiencies which are discussed in Deficiencies on page 236. Despite these deficiencies SLIP is a popular protocol, still widely used; however, PPP is becoming more popular than SLIP.

Figure 35 SLIP framing



1 this figure denotes the size of the field, in bytes

Deficiencies

1. You cannot use software flow control; therefore, you must use hardware flow control. Software flow control uses xon/xoff characters, which SLIP is unable to escape to the datastream.
2. SLIP can lead to errors since there is no checksum in the SLIP frame. If a noisy phone line corrupts a datagram being transferred by SLIP, the upper layers must detect them. This problem is less serious with TCP/IP (where upper layers provide a checksum) but more serious with UDP (where upper layers optionally provide a checksum).
3. The remote client cannot obtain an IP address from the server, so the remote end must obtain an IP address another way (e.g. a script).
4. SLIP is often used for interactive traffic such as Telnet or Rlogin, where small numbers of characters are sent in a datagram (e.g. a word of only a few letters, such as 'help'). Telnet and Rlogin both use TCP so the IP datagram is accompanied by a TCP/IP header, 40 bytes in length. This header is a large overhead for a small datagram; i.e. the word 'help' is 4 bytes; it would occupy $40 + 4 = 44$ bytes with the TCP/IP header. This overhead leads to poor performance with interactive traffic.

To overcome these problems, a newer version of SLIP has been developed called compressed SLIP or C-SLIP; see C-SLIP on page 237.

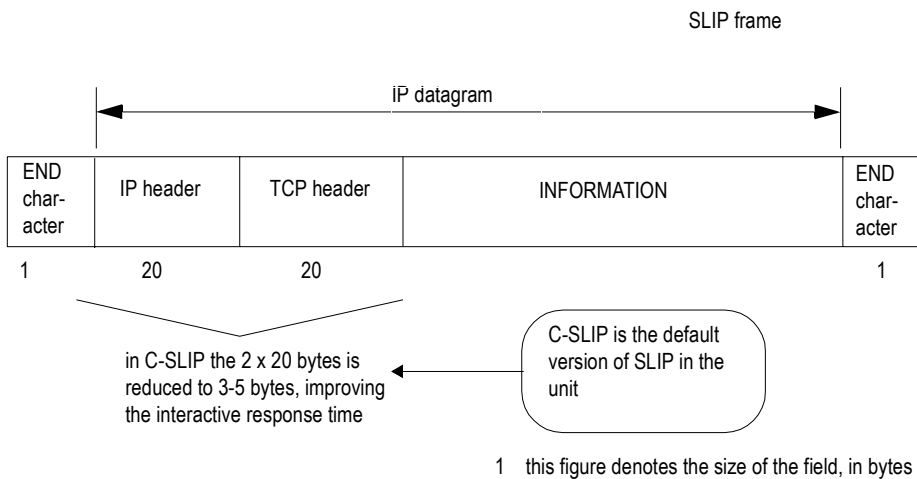
5. SLIP supports only the IP protocol; it cannot transmit multiple network protocols over the same single serial line.

C-SLIP

A newer version of SLIP was developed called compressed SLIP (or C-SLIP), to overcome the performance problems of SLIP. This is specified in RFC 1144 (see Appendix D (References)). C-SLIP reduces the 40 byte TCP/IP header to 3 or 5 bytes, greatly improving interactive response time; see Figure 36.

C-SLIP is the default version of SLIP in the unit and is represented by the SLIP parameter called 'VJ Compression' (for Van Jacobson compression); when turned 'on' the TCP/IP header is compressed and you are therefore running C-SLIP over your link. VJ compression is 'on' by default; Section Configuring SLIP shows you where to find this parameter in the text menu and cli.

Figure 36 Compressed SLIP (C-SLIP)



ESCAPE characters are not shown here (see Figure 35)

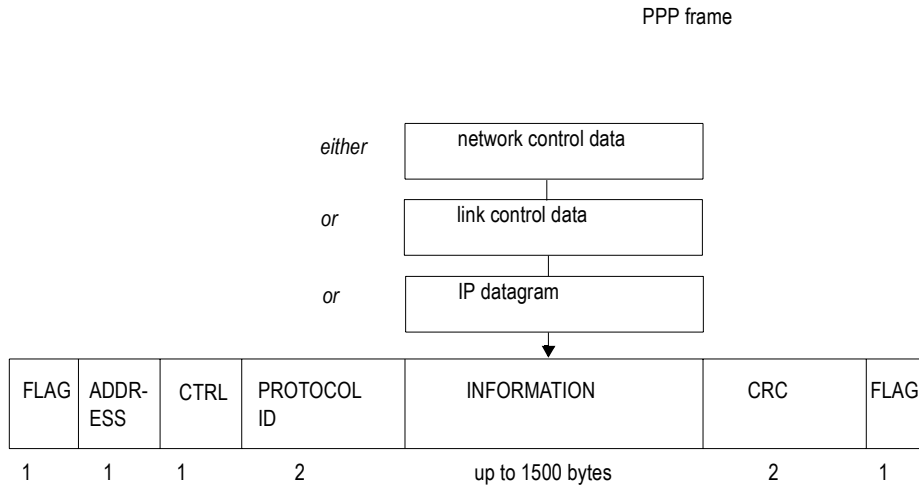
PPP

Overview

The Point-to-Point Protocol (PPP) is a modern and reasonably sophisticated protocol for transporting IP datagrams over serial links; (a datagram is defined as a number of bytes of user information sent from the sender to the receiver). It is specified in RFC 1055; see Appendix D (References).

The way PPP encapsulates IP datagrams is shown in Figure 37. The format of PPP frames resembles the ISO HDLC (high-level data link control) standard.

Figure 37 PPP framing



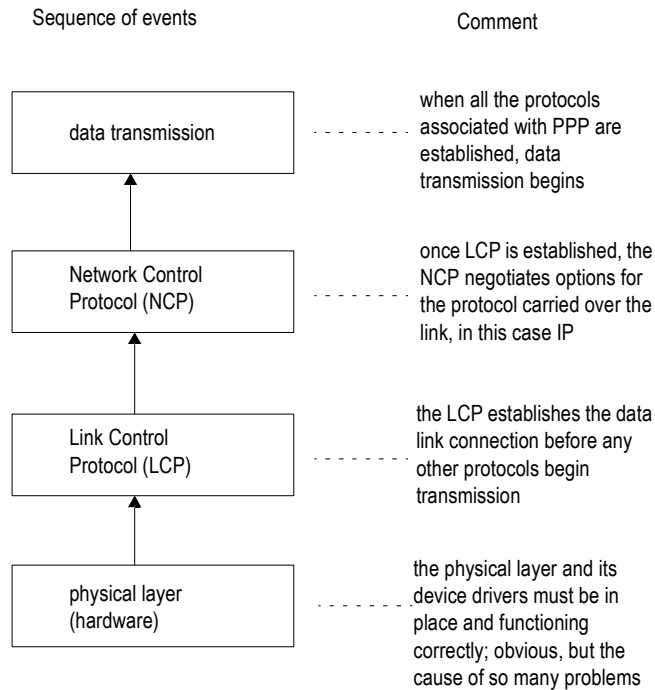
1 this figure denotes the size of the field, in bytes

Each frame begins and ends with a FLAG byte. This byte is followed by ADDRESS and CONTROL bytes. Next is a PROTOCOL field which indicates the content of the INFORMATION field; e.g. whether the information field is an IP datagram, link control data or network control data. The CRC field (or FCS, meaning 'Frame Check Sequence') is a cyclic redundancy check, to detect errors in the frame.

How PPP works

Once the hardware of the link is connected and is operational, PPP operates using a Link Control Protocol (LCP) and a family of Network Control Protocols (NCPs). This operation - which happens in a very specific order - is explained in Figure 38.

Figure 38 Operation of PPP



The NCP for IP is IPCP (IP Control Protocol); in the unit the only networking layer datagrams you are sending over your link are IP datagrams.

Implementations of PPP are becoming more widely available and so the number of users of PPP is growing. PPP is probably now used more than SLIP.

Advantages

1. You can use either hardware or software flow control.
2. You should experience less errors since there is a checksum on every frame.
3. The remote client can obtain an IP address from the server - i.e. there is dynamic negotiation of the IP address (of each end).

4. There is TCP/IP header compression (similar to SLIP) where the 2 x 20 byte header is reduced to 3 or 5 bytes (see Figure 36). This compression is represented by the PPP parameter called 'VJ Comp' (for VJ Compression); when turned 'on' the TCP/IP header is compressed. VJ compression is 'on' by default; Section Configuring PPP shows you where to find this parameter in the text menus and cli. VJ compression increases performance with interactive traffic.
5. Security on the link is provided by the protocols PAP and CHAP. PAP operates at start-up of the link, authenticating the remote user. CHAP operates at start-up of the link and at regular intervals. The regular frequency of CHAP ensures that a link remains secure during a session.

The default security protocol in the unit is CHAP. Also, you can configure the interval with which CHAP re-challenges the remote end during a session.
6. PPP supports multi-protocols over a single serial line.
7. PPP transmits data over both synchronous and asynchronous lines; in the unit support for PPP is for asynchronous lines only.

Appendix D References

This appendix lists the RFC (Request for Comment) documents to which reference is made in this Guide.

Reference Number	Name of Document
RFC 791	Internet Protocol. September 1981.
RFC 792	Internet Control Message Protocol. September 1981.
RFC 793	Transmission Control Protocol. September 1981.
RFC 826	Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48.bit Ethernet address for transmission on Ethernet hardware. November 1982.
RFC 854	Telnet Protocol Specification. May 1983.
RFC 855	Telnet options specifications. May 1983.
RFC 951	Bootstrap protocol. September 1985.
RFC 1034	Domain names - concepts and facilities. November 1987.
RFC 1035	Domain names - implementation and specification. November 1987.
RFC 1055	A Nonstandard for Transmission of IP Datagrams Over Serial Lines: SLIP. June 1988.
RFC 1058	Routing Information Protocol. June 1988.
RFC 1144	Compressing TCP/IP headers for Low-Speed Serial Links. February 1990.
RFC 1155	Structure and identification of management information for TCP/IP based networks. May 1990.
RFC 1157	Simple Network Management Protocol. May 1990.
RFC 1213	Management Information Base for Network Management of TCP/IP based networks; MIBII. March 1991.
RFC 1258	BSD Rlogin. September 1991.
RFC 1332	The PPP Internet Protocol Control Protocol. May 1992.
RFC 1334	PPP Authentication Protocols. October 1992.
RFC 1350	The TFTP Protocol (Revision 2). July 1992.
RFC 1548	The Point-to-Point Protocol (PPP). December 1993.
RFC 1662	PPP in HDLC-like Framing. July 1994.

Reference Number	Name of Document
RFC 1877	PPP Internet Protocol Control Protocol Extensions for Name Server Addresses. December 1995.
RFC 1994	PPP Challenge Handshake Authentication Protocol (CHAP). August 1996.
RFC 2058	RADIUS Authentication. January 1997.
RFC 2059	RADIUS Accounting. January 1997.
RFC 2068	Hypertext Transfer Protocol -- HTTP/1.1. January 1997.

Appendix E ASCII and HEX conversion tables

Introduction

This appendix contains the following:

- Section ASCII to Decimal and Hex Conversion Chart
- Section Binary to Hex Conversion Chart

ASCII to Decimal and Hex Conversion Chart

ASCII	DEC	HEX
NUL (^@)	000	00
SOH (^A)	001	01
STX (^B)	002	02
ETX (^C)	003	03
EOT (^D)	004	04
ENQ (^E)	005	05
ACK (^F)	006	06
BEL (^G)	007	07
BS (^H)	008	08
HT (^I)	009	09
LF (^J)	010	0A
VT (^K)	011	0B
FF (^L)	012	0C
CR (^M)	013	0D
SO (^N)	014	0E
SI (^O)	015	0F
DLE (^P)	016	10
DC1 (^Q)	017	11
DC2 (^R)	018	12

ASCII	DEC	HEX
DC3 (^S)	019	13
DC4 (^T)	020	14
NAK (^U)	021	15
SYN (^V)	022	16
ETB (^W)	023	17
CAN (^X)	024	18
EM (^Y)	025	19
SUB (^Z)	026	1A
ESC	027	1B
FS	028	1C
GS	029	1D
RS	030	1E
US	031	1F
SP	032	20
!	033	21
"	034	22
#	035	23
\$	036	24
%	037	25

ASCII	DEC	HEX
&	038	26
'	039	27
(040	28
)	041	29
*	042	2A
+	043	2B
,	044	2C
-	045	2D
.	046	2E
/	047	2F
0	048	30
1	049	31
2	050	32
3	051	33
4	052	34
5	053	35
6	054	36
7	055	37
8	056	38

ASCII	DEC	HEX
9	057	39
:	058	3A
;	059	3B
<	060	3C
=	061	3D
>	062	3E
?	063	3F

ASCII	DEC	HEX
Q	081	51
R	082	52
S	083	53
T	084	54
U	085	55
V	086	56
W	087	57

ASCII	DEC	HEX
i	105	69
j	106	6A
k	107	6B
l	108	6C
m	109	6D
n	110	6E
o	111	6F

ASCII	DEC	HEX
@	064	40
A	065	41
B	066	42
C	067	43
D	068	44
E	069	45
F	070	46
G	071	47
H	072	48
I	073	49
J	074	4A
K	075	4B
L	076	4C
M	077	4D
N	078	4E
O	079	4F
P	080	50

ASCII	DEC	HEX
X	088	58
Y	089	59
Z	090	5A
[091	5B
\	092	5C
]	093	5D
^	094	5E
-	095	5F
`	096	60
a	097	61
b	098	62
c	099	63
d	100	64
e	101	65
f	102	66
g	103	67
h	104	68

ASCII	DEC	HEX
p	112	70
q	113	71
r	114	72
s	115	73
t	116	74
u	117	75
v	118	76
w	119	77
x	120	78
y	121	79
z	122	7A
{	123	7B
	124	7C
}	125	7D
~	126	7ES
DEL	127	7F

Binary to Hex Conversion Chart

Binary	Hex
0000	0
0001	1
0010	2
0011	3
0100	4
0101	5
0110	6
0111	7
1000	8
1001	9

Binary	Hex
1010	A
1011	B
1100	C
1101	D
1110	E
1111	F

Notes:

To represent two letters/two numbers flow binary numbers sequentially, so :

0F is 0 followed by F, i.e. 0000 followed by 1111.

0F is therefore 00001111 in binary.

Likewise, the binary digits 10110100 would equate to:

1011 followed by 0100, which is B followed by 4;

therefore 10110100 is B4 in hex.

Appendix F Contacting Perle

You need to read this appendix if you want to... You need to read this appendix if you want to contact Perle for technical support or any other queries about this product.

appendix if you want to... This appendix includes the following sections;

- **Making a technical support query** on page **248**
- **Repair procedure** on page **251**
- **Feedback about this manual** on page **252**
- **Perle support centres worldwide** on page **253**

Internet access

Click here to access the our website at the following URL:
<http://www.perle.com>

Email

Click here to email Perle at the following address;
Email: support@perle.com

Making a technical support query

This section contains the following information about making a query;

- [Who to contact](#) on page **248**
- [Information needed when making a query](#) on page **249**
- [Making a support query via the Perle web page](#) on page **250**

Who to contact

If you bought your product from a registered Perle supplier, you must contact their Technical Support department; they are qualified to deal with your problem.

If you are a registered Perle supplier, and bought your product from Perle, contact Perle Technical Support at the offices listed below.

Information needed when making a query

When you make a technical support enquiry please have the following information ready;

Hint
Print out this page and fill in the table provided with the basic information you need.

Item	Write details here
Product name and version	
Problem description	
Operating system version	
Driver version	
Details of any other cards installed in your system	
Your name	
Company Name	
Country	
Phone number	
Fax number	
Email address (if available)	

Making a support query via the Perle web page

If you have an internet connection, please send details of your problem to Technical Support using the email links provided on the Perle web site in the 'Support' area.

See also [Perle support centres worldwide](#) on page 253 for email links and other contact details for the Perle technical support centres.

[Click here to access our website at the following URL:
http://www.perle.com](http://www.perle.com)

Repair procedure

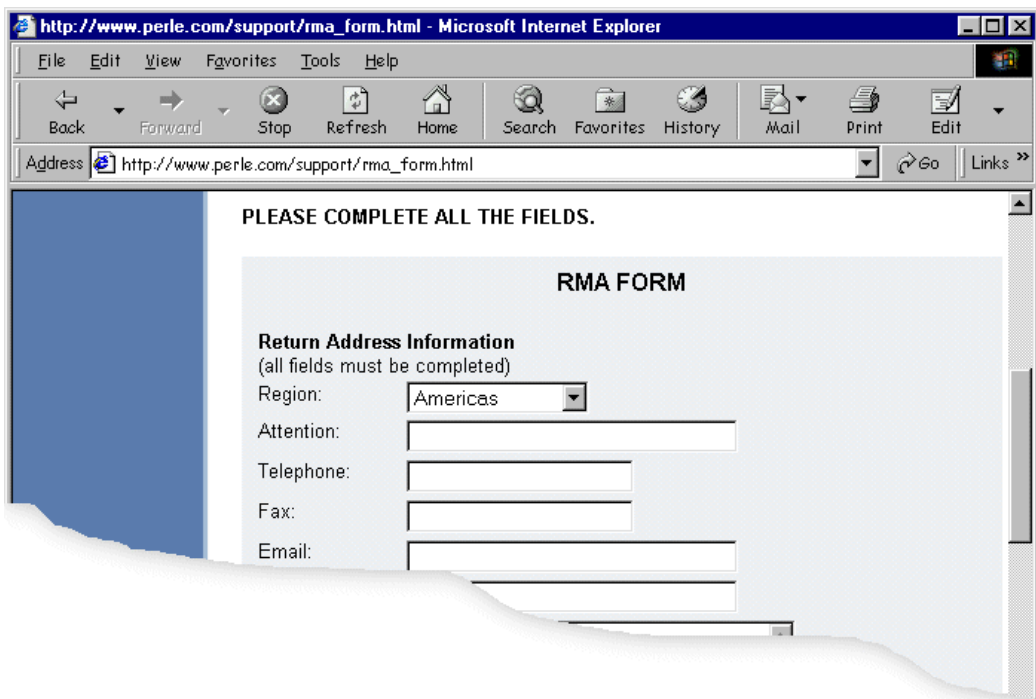
Before sending a unit for repair, you must contact your Perle supplier. If, however, you bought your product directly from Perle you can contact directly. See [Perle support centres worldwide](#) on page 253 for contact information.

Customers who are In Europe, Africa or Middle East can submit repair details via a website form shown in the next picture. This form is on the Perle website, www.perle.com, in the **Support** area.

[Click here to access our web site at the following URL:
http://www.perle.com/support/rma_form.html](http://www.perle.com/support/rma_form.html)

In the USA and Asia contact the office shown in the Technical Support section.

Website RMA (Return Material Authorisation) Form



The screenshot shows a Microsoft Internet Explorer browser window displaying the RMA Form at http://www.perle.com/support/rma_form.html. The browser's address bar shows the URL. The page content includes a blue sidebar on the left and a main content area with the following text and form fields:

PLEASE COMPLETE ALL THE FIELDS.

RMA FORM

Return Address Information
(all fields must be completed)

Region:

Attention:

Telephone:

Fax:

Email:

Feedback about this manual

If you have any comments or suggestions for improving this manual please email Perle using the following address;

docfeedback@perle.com

Please include the *title*, *part number* and *date* of the manual (you can find these on the title page at the front of this manual).

Perle support centres worldwide

Note

Perle offers free technical support to Perle Authorised Distributors and Registered Perle Resellers.

To access technical support please visit the Perle website at www.perle.com/support.

If you are unable to find the information you require, please feel free to contact our technical support teams by email using the addresses shown in the next table.

Country	Address	Email
North America	Perle Systems Ltd. 60 Renfrew Drive Markham Ontario Canada L3R OE1	<i>Email: ptac@perle.com</i>
Europe	Perle Systems Europe Ltd. 3 Wintersells Road Byfleet Surrey KT14 7LF UK	<i>Email: ptac@perle.com</i>
Asia	Perle Asia Pacific (Pte) Ltd. 190 Middle Road #19-05 Fortune Centre Singapore 188979	<i>Email: ptac@perle.com</i>
Worldwide	Perle Systems Ltd. 60 Renfrew Drive Markham Ontario Canada L3R OE1	<i>Email: ptac@perle.com</i>

Index

- A
- Access Restrictions 111, 188
- account authenticator flag, troubleshooting 228
- ACSII code chart 243–244
- add community* 151
- add DNS* 151
- add gateway* 152
- add host* 153
- add modem* 153
- add radius* 154
- add trap* 155
- add WINS* 156
- Adding users 81, 155
- Admin user 87
- admin*, cli command 156
- Authentication
 - and RADIUS 79
 - of username 'admin' 78
 - on Rlogin/Telnet into the unit 20
- Automatic baud rate detection 124
- B
- Baud rate 18, 22, 25, 64
- Bi-directional modem connections 44, 219
- Binary to Hex Chart 244
- BOOTP 99–109
- BOOTP file, *see* BOOTPTAB file
- BOOTPTAB file 102
- Broadcast address 209
- C
- Callback
 - fixed 84
 - roaming 72
 - setting up in a remote Win NT machine 141
- Callback Control Protocol (CBCP) 73
- Change environment 87, 128
- Change password 88, 127
- Change terminal setup 127
- Change user 82
- CHAP 240
- CLI commands 149–217
- cli commands and menu equivalents 149
- cli prompts 87, 124
- CLI, *see* Command Line Interface
- Command abbreviation 126
- Command Line Interface 126
- contacting Perle Systems
 - email 247
 - for technical support 248
 - internet 247
- C-SLIP,
 - overview 237
- customlang feature, *see* Language Support
- D
- debug* 157
- Default settings
 - Line 170
 - Line, parallel 54
 - Line, serial 27, 53, 74
 - PPP line 67
 - SLIP line 65
 - Users 82, 171
- delete community* 158
- delete DNS* 158
- Delete gateway 159
- Delete host 159
- delete modem* 160
- delete radius* 160
- delete trap* 161
- Delete user 89, 161
- delete WINS* 162
- Dial parameter
 - and line service types 74
- Dialin modem connections 43
- Dialout modem connections 44

- Direct line service type
 - raw 219
 - rlogin 219
 - telnet 23, 219
- DNS 159
- Domain name 209
- Downloadable terminal definitions 96–98
- E
- email 247
- Emergency Recovery 233
- Environment 87, 128
- Error messages, *see* Troubleshooting
- Ethernet 5
- Examples
 - LPD configuration 35
 - RCP configuration 41
 - SLIP/PPP connections 135
- F
- Factory reset
 - software 110
- FLASH memory 27, 54, 75, 93, 165, 168, 173, 230
- Flow control 18, 22, 25, 64
- Forms 125
- FSM, *see* Full Screen Mode
- Full Screen Mode 124
- G
- Gateway
 - configuring using bootp 103
- Global replace 26, 53, 74
- H
- HDLC 237
- heap* 162
- Help 126, 162
- Hex Code Chart 244
- Hex to Binary Chart 244
- Host Table
 - Show host table 199
- Hot-keys 131–132
- Hunt group
 - Bidirectional modems 45
 - Dialout modems 44
 - Printers 42
 - Reverse Telnet 29
- I
- ICMP 66
- Idle timer, *see* Timers 22
- Initialisation string parameter
 - and line service types 74
- Internet address
 - Show internet address 209
- IP 235–240
- IP Host
 - (default for all users) 187
 - (setting for a user) 84, 194
- IPCP 239
- ISDN Terminal Adaptors 74
- J
- Joining together two networks
 - see* Router
- jslogin? line service type 219
- K
- kermit, application 45
- kill line* 163
- kill parallel* 163
- Kill session 132
- kill session* 164
- L
- Language Support 89
 - language of your choice 90
 - supplied languages 89, 128, 194
 - translation guidance 91
- Language support
 - effect of Software upgade on ascii Language Files 92
- Language Support, customlang, 89, 128, 194
- Line service
 - .v.User service 219

- summary of types 219–221
- Line service types
 - Bidirectional 44, 219
 - Direct raw 219
 - Direct rlogin 23, 219
 - Direct telnet 23, 219
 - jslogin 219
 - Printer 34–37, 38–40, 220
 - Reverse raw 42, 220
 - Reverse telnet 220
 - Silent raw 221
 - Silent rlogin 23, 220
 - Silent telnet 23, 220
- Logging on 123
 - to remote hosts, *see* Sessions
- Logging out 128, 164
 - from sessions 130
- Lost password 114
- lp, application 45
- LPD 33–37
- M
- Menu system 124
- Menuing 87
- Menus
 - cli command equivalents 149
- MIB definitions 116, 117–120
- MIB used by LANSTREAM 115
- Modem name parameter
 - and line service types 74
- Modems
 - Automatic baud rate detection 74, 124
 - Bidirectional 44
 - configurable features - summary 74
 - Dialin 43
 - Dialout 44
 - Logging on via 124
 - Modem handling 45–53
- MTSD 45–53
 - command options 51–53
- Multiple printer connections, *see* Hunt group
- N
 - netload* 90, 91, 165
 - netload*, and the 'save' cli command 173
 - Normal user level 87
 - Nouser 181
- P
- PAP 240
- Parallel port, configuration
 - see* LPD or RCP
 - see* set/show parallel (cli commands)
- Parity 18, 22, 25, 64
- Password
 - changes with upgraded software 96
 - Changing a user's password 88
 - effect of a new configuration file 105, 114
 - lost 114
 - Setting a user's password 81
 - users changing their own password 127
- phone number
 - when 'dial' is set to 'out' 74
- ping* 167
- PPP,
 - advantages of 239
 - and RADIUS 59
 - configuring for a line 67–72
 - default line settings 67
 - overview 237
 - use PPP or SLIP? 62
- Predefined sessions 131
 - for other users 87
- Predefining sessions 130
- Print handling (using MTSD) 45–53
- Printer line service type 220
- Printing
 - Using LPD 33–37
 - Using MTSD 45
 - Using RCP 38–40
- Privilege levels, *see* User level

- product repair form 251
- Prompts, *see* cli prompts
- Q
- queue types, using LPD 37
- R
- RADIUS
 - and telnet/rlogin 20
 - and user accounts 78
 - class attribute size 81
 - line, SLIP and PPP parameters supported 62
 - providing SLIP or PPP 59
- RADIUS, example user file
 - PPP service 61
 - telnet service 81
- RAM 165
- RCP 38–40
- Reboot* (cli command) 168
- Rebooting 110
- References 241
- Remote client
 - setting up using PPP 136
- Remote configuration 111
- Remote printing
 - Using LPD 33–37
 - Using RCP 38–40
- Remote printing (using MTSD) 45
- repair procedure 251
 - product repair form 251
 - RMA form 251
- reset factory* 169
- reset line* 170
- reset parallel* 170
- Reset to defaults
 - Line, parallel 54, 170
 - Line, serial 27, 53, 74, 170
 - Unit 110
 - Users 171
- restart* 172
- Restricted user level 87
- resume* 172
- Resume session 132
- Reverse raw 42, 44, 220
- Reverse telnet 28–29, 220
- RFCs, *see* References
- RIP 146
- Rlogin 23, 129–130, 173, 236
- Rlogin,
 - and RADIUS 20
 - from the unit 17
 - into the unit 16
- RMA form 251
- Router
 - using the unit as a router 58, 74, 143
- Routes, *see* *show routes*
- RS232 signals 74
- S
- Sample terminal definition files 96
- Save configuration
 - cli, to a file on a host 166
 - menus 27, 54, 75, 92
 - to a file on a host 113
 - to internal memory 173
- save*, cli command 173
- screen* 175
- Screen switch character 131
 - Changing a user's 82
- Security 111
- Serial port, configuration
 - see* Host Control of Ports and Printing Chapter 31
 - see* SLIP and PPP Chapter 57
 - see* Terminal Server Chapter 15
- Server (JETSTREAM or LANSTREAM) base unit configuration 209
- Server (JETSTREAM or LANSTREAM) name 209
- service, user .v. line 83, 219
- Session timer, *see* Timers 23

- Sessions 87–88, 128–133
 - set contact* 175
 - set date* 176
 - set gateway* 179
 - set host* 179
 - set line* 181
 - set location* 183
 - set parallel* 184
 - set radius* 186
 - set server* 187
 - set telnet* 190
 - set time* 193
 - set user* 90, 91, 193
- Setting a user's password 81
 - show date* 197
 - show gateways* 198
 - show hardware* 199
 - show hosts* 199
 - show interfaces* 200
 - show line* 201
 - show modem* 203
 - show parallel* 204
 - show radius* 207
 - show routes* 208
 - show serverinfo* 209
 - show sessions* 210
 - show snmp* 212
 - show telnet* 213, 216
 - show time* 214
 - show user* 214
- Silent raw 43, 221
- Silent rlogin 20–23, 220
- Silent telnet 20–23
- SLIP,
 - and RADIUS 59
 - configuring for a line 65–67
 - default line settings 65
 - deficiencies 236
 - overview 235
 - use SLIP or PPP? 62
- SNMP 115–122
 - add community* 151
 - add trap* 155
 - delete community* 158
 - delete trap* 161
 - JS8500 Private MIB 116, 117–120
 - set contact* 175
 - set location* 183
- start* 215
- System administration 95–114
- T
- TCP 236
- TCP clear, User service 83
- TCP/IP 5, 236, 237, 240
- technical support 248
 - centres worldwide 253
 - queries, information needed for 249
 - via the internet 250
 - who to contact 248
- Telnet 16–29, 129–130, 216, 236
 - direct 219
 - reverse 28–29, 220
 - silent 20–23, 220
- Telnet,
 - and RADIUS 20
 - from the unit 17
 - into the unit 16
 - remote sessions - limit on 111
- Term1/2/3 96
- Terminal definitions 96
- Terminal setup 127
- Terminal type 25, 96, 127
- TFTP 90, 96, 113
- TFTP configuration 98
- Timers
 - and logins direct to a host 22
 - and Reverse Telnet connections 29
 - and Telnet/Rlogin *from* the unit 19

- changing for Terminal Server type connections 15
- effect on JETSTREAM or LANSTREAM sessions 88
- idle timer, for a line 19, 22, 25, 27, 64, 74
- idle timer, for a user 83
- on Telnet/Rlogin *into* the unit 16
- session timer, for a line 19, 23, 26, 65
- session timer, for a user 83
- Translating a language file, *see* Language Support
 - language of your choice 90
- Traps 116
- Troubleshooting 223–233
- tty interfaces
 - and MTSD 45
- U
- UDP 236
- UNIX 5
- Unix SVR4
 - dialin under 49
- Unpaged (session) 132
- Upgrading software 96
 - effect on ascii Language Files 92
- User administration 77–89
- User level 87
- User name 81
- User service
 - .v. Line service 83, 219
 - TCP clear 83
 - tcp clear 81
- User type, *see* User level
- Users
 - default settings 82
- uucp, application 45
- V
- version*, cli command 217
- Video pages
 - Paged sessions 132

W
WINS 159

