BLACK BOX®
NETWORK SERVICES

16 and 24 port Console Servers

User Guide

Normas Oficiales Mexicanas (NOM) Electrical Safety Statement
INSTRUCCIONES DE SEGURIDAD

1. Todas las instrucciones de seguridad y operación deberán ser leídas antes de que el aparato eléctrico sea operado.

2. Las instrucciones de seguridad y operación deberán ser guardadas para referencia futura.

3. Todas las advertencias en el aparato eléctrico y en sus instrucciones de operación deben ser respetadas.

4. Todas las instrucciones de operación y uso deben ser seguidas.

5. El aparato eléctrico no deberá ser usado cerca del agua-por ejemplo, cerca de la tina de baño, lavabo, sótano mojado o cerca de una alberca, etc.

6. El aparato eléctrico debe ser usado únicamente con carritos o pedestales que sean recomendados por el fabricante.

7. El aparato eléctrico debe ser montado a la pared o al techo sólo como sea recomendado por el fabricante.

8. Servicio-El usuario no debe intentar dar servicio al equipo eléctrico más allá a lo descrito en las instrucciones de operación. Todo otro servicio deberá ser referido a personal de servicio calificado.

9. El aparato eléctrico debe ser situado de tal manera que su posición no interfiera su uso. La colocación del aparato eléctrico sobre una cama, sofá, alfombra o superficie similar puede bloquea la ventilación, no se debe colocar en libreros o gabinetes que impidan el flujo de aire por los orificios de ventilación.

10. El equipo eléctrico deber ser situado fuera del alcance de fuentes de calor como radiadores, registros de calor, estufas u otros aparatos (incluyendo amplificadores) que producen calor.

11. El aparato eléctrico deberá ser connectado a una fuente de poder sólo del tipo descrito en el instructivo de operación, o como se indique en el aparato.

12. Precaución debe ser tomada de tal manera que la tierra fisica y la polarización del equipo no sea eliminada.

13. Los cables de la fuente de poder deben ser guiados de tal manera que no sean pisados ni pellizcados por objetos colocados sobre o contra ellos, poniendo particular atención a los contactos y receptáculos donde salen del aparato.

14. El equipo eléctrico debe ser limpiado únicamente de acuerdo a las recomendaciones del fabricante.

15. En caso de existir, una antena externa deberá ser localizada lejos de las lineas de energia.

16. El cable de corriente deberá ser desconectado del cuando el equipo no sea usado por un largo periodo de tiempo.

17. Cuidado debe ser tomado de tal manera que objectos liquidos no sean derramados sobre la cubierta u orificios de ventilación.

18. Servicio por personal calificado deberá ser provisto cuando:

    a. El cable de poder o el contacto ha sido dañado; u
    b. Objectos han caído o líquido ha sido derramado dentro del aparato; o
    c. El aparato ha sido expuesto a la lluvia; o
    d. El aparato parece no operar normalmente o muestra un cambio en su desempeño; o
    e. El aparato ha sido tirado o su cubierta ha sido dañada.

FEDERAL COMMUNICATIONS COMMISSION
AND
CANADIAN DEPARTMENT OF COMMUNICATIONS
RADIO FREQUENCY INTERFERENCE STATEMENTS

This equipment generates, uses, and can radiate radio frequency energy and if not installed and used properly, that is, in strict accordance with the manufacturer's instructions, may cause interference to radio communication. It has been tested and found to comply with the limits for a Class A computing device in accordance with the specifications in Subpart J of Part 15 of FCC rules, which are designed to provide reasonable protection against such interference when the equipment is operated in a commercial environment. Operation of this equipment in a residential area is likely to cause interference, in which case the user at his own expense will be required to take whatever measures may be necessary to correct the interference.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This digital apparatus does not exceed the Class A limits for radio noise emission from digital apparatus set out in the Radio Interference Regulation of the Canadian Department of Communications.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la classe A prescrites dans le Règlement sur le brouillage radioélectrique publié par le ministère des Communications du Canada.

CE **Caution:** the Console Server is approved for commercial use only.

About this Guide

Purpose of this manual

This manual tells you how to install, configure and use the Console Server and associated utility software.

Who this manual is for

This manual is aimed at users who want to communicate directly via the serial port to networked devices (such as routers, servers and so on) in order to perform system administration tasks.

This manual requires a working knowledge of using personal computers and associated operating systems, as well as experience in installing host cards and peripherals.

Fast Contents

Contents

Chapter 1 Introduction

You need to read this chapter if you want to...

You need to read this chapter if you want an overview of the Console Server product.

This chapter provides introductory information about the Console Server, its associated components, software and configuration utilities.

This chapter includes the following sections

- About the Console Server on page 18

- Typical applications summary on page 20

- Console Server front and rear views on page 21.

For details of installation procedures, see Chapter 2 Installation.

For information about performing system administration tasks with your Console Server, see Chapter 3 System administration.

For information on using your Console Server as a console server, see Chapter 4 Using your Console Server.

About the Console Server

The Console Server is a console server which allows you to communicate directly via the serial port to networked devices (such as routers, servers and so on) in order to perform system administration tasks.

The Console Server allows system administrators to diagnose and fix from anywhere on the LAN/WAN or via a modem thus saving on administrator's time and costs to keep system disruption to a minimum.
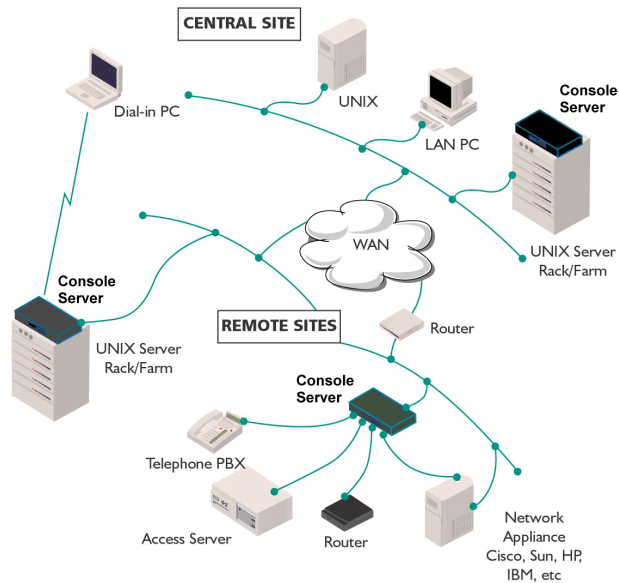
Typically, you use the Console Server when a server or network device fails at a remote site or if you want to perform administration tasks from home. Using a Console Server you can access the unit over the LAN/WAN or via dial-in.

The Console Server is available in the following variants;

- 16 port
- 24 port

See also Typical applications summary on page 20 and Console Server front and rear views on page 21.

Typical applications summary

Managing devices over the LAN/WAN

The Console Server allows the administrator to Telnet to the appropriate port on the console server. With the Console Server in band management functionality, administrators can gain access to attached devices from anywhere on the LAN/WAN provided they know the IP addresses. The Console Server also allows access to multiple devices simultaneously.

Managing devices without accessing the LAN/WAN

In the event of a network failure, the Console Server allows the administrator access via a modem attached to one of the serial ports on the unit to access attached devices.

Network security

Console Server provides a comprehensive suite of security features to allow an organization to implement robust security planning to prevent unauthorized access. These include SLIP and PPP Remote User dial-in and support for RADIUS.

For a secure LAN connection, the Console Server supports SSH version 1 and version 2 protocol. Remote server connections with SSH protocol uses an encrypted data channel with support for password and other authentications.

Management and diagnostics

Independent tests have proved Console Serverextremely easy to configure and install. A comprehensive array of software tools allows the Console Server to be configured, managed and upgraded either locally or remotely over the network and even via the Internet.

These tools include JETset, for complete port management from any location via a Web browser, and easy downloads of software upgrades to the unit's flash memory. Command line and menu interfaces are included, as is a separate local management port, plus industry standard control and management facilities - SNMP, BOOTP, DHCP and DNS.

Console Server front and rear views

The Console Server is a network access server with front-mounted RJ45 serial ports. It is designed for use in a rack. The serial ports are RS232. The product has 10/100BaseT and AUI network connections and an Administration port for system management. The next picture shows the front view of a 24 port unit.

Console Server front view

PWR NET

Power and network LEDs

Sixteen or twenty four serial ports
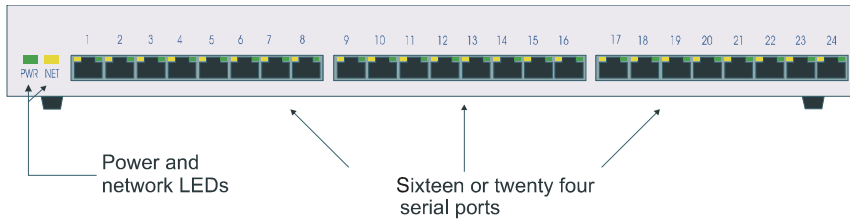
You can mount the Console Server in a 19 inch rack, on a wall or on a desk.

Console Server rear panel

Power Connector

Admin Port

10/100 Port

MAC address label

Ethernet Address

110 - 240V
0.5 - 1 A
50 - 60 Hz
AC (~)
25W

ADMIN

FACTORY

10 BASE T

AUI

RESET

ON/OFF switch

Factory Reset Recessed Switch

AUI Port
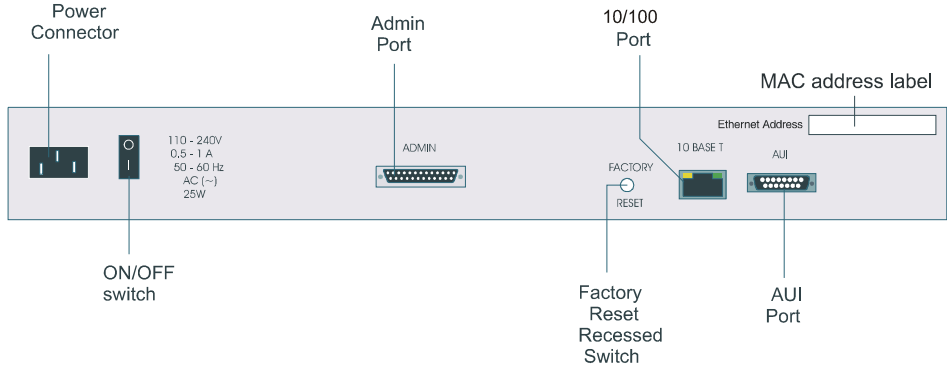
Chapter 2 Installation

You need to read this chapter if you want to... You need to read this chapter if you want install the Console Server.

This chapter provides task oriented information about installing the Console Server, its associated components, software and configuration utilities.

This chapter includes the following sections;

General installation procedure

The general procedure for installing and setting up your Console Server is as follows;

1. Install your Console Server in a rack or on a desktop as required using the procedures described in Rack mounting your Console Server on page 25 and Desk mounting your Console Server on page 27.

Note   *If you are stacking multiple units on a desktop see* Multiple stacking your Console Server on page 28 *for the maximum advisable units to stack.*

2. Connect your Console Server to the network. See Appendix A Cabling information.

3. If required, select the interface type you want. See Selecting AUI or 10/100 Base T interface on page 32.

4. Set up your IP address using the procedures given in Setting up an IP address on page 33.

5. Access the Console Server configuration software using the procedures given in Accessing the Console Server configuration software on page 45

6. Set up your network parameters using the procedure given in Setting up your network parameters on page 46.

You can now use the unit. For information on using the Console Server for system administration purposes. See Chapter 3 System administration for further details.

For information on using your Console Server as a console server, see Chapter 4 Using your Console Server.

Rack mounting your Console Server

To mount a single Console Server into a 19 inch rack, use the two mounting brackets and four screws provided with the unit.

Caution   **When mounting several Console Server units in a 19" rack, you must not stack more than 3 units without leaving an air gap between them.**

Caution   **Observe maximum ambient operating temperatures within a rack; you may have to use forced air cooling.**

mounting
bracket

Console Server

holes for
rack
mounting

side

rear

front
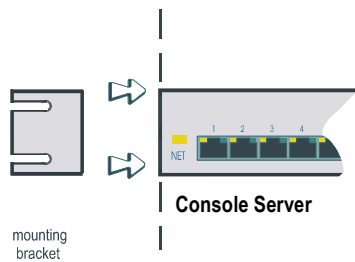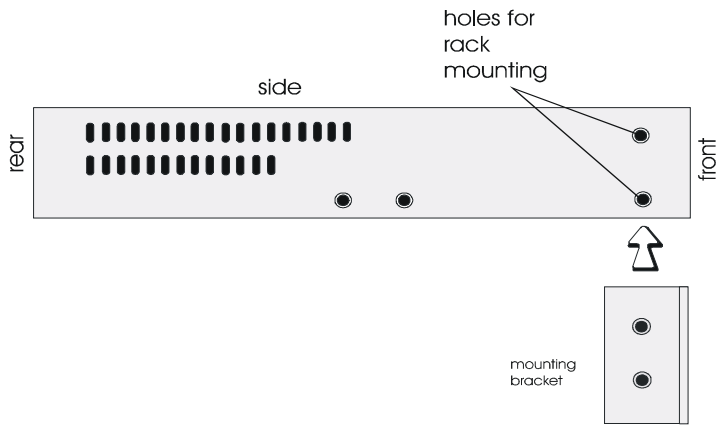
mounting
bracket

Desk mounting your Console Server

To prepare the Console Server for use on a desk use the four self-adhesive rubber feet provided with the unit. Stick the four feet to the underside of the unit, one in each corner, approximately one inch from each adjacent edge.
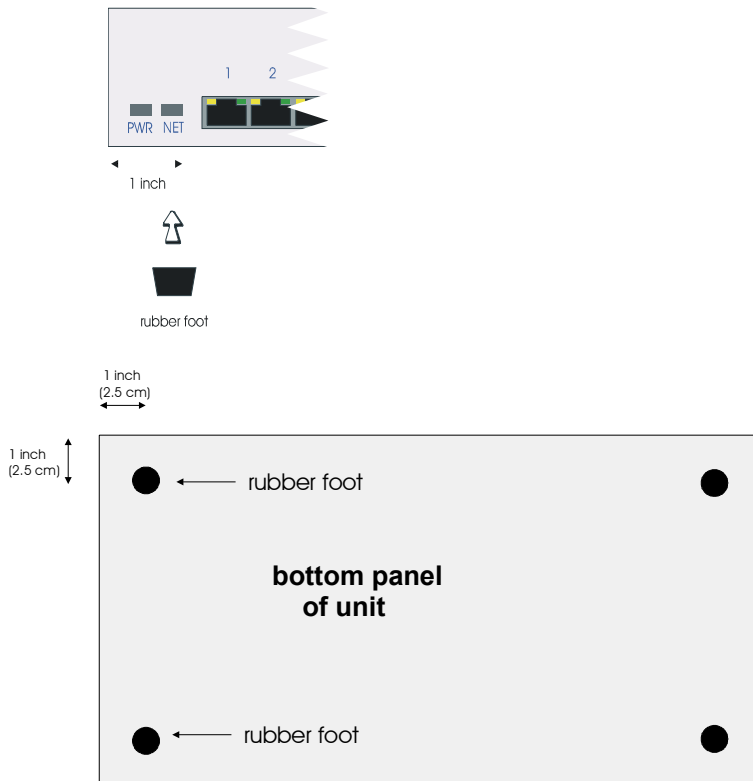
Multiple stacking your Console Server

When stacking your unit on a desk we recommend that you stack no more than three units high in a 0 to 40 degrees centigrade environment.This precaution ensures that you keep within the maximum operating temperatures of the units.

Caution   ***When desk mounting multiple Console Server units, make sure you fit the rubber feet to all units before stacking to assist ventilation.***
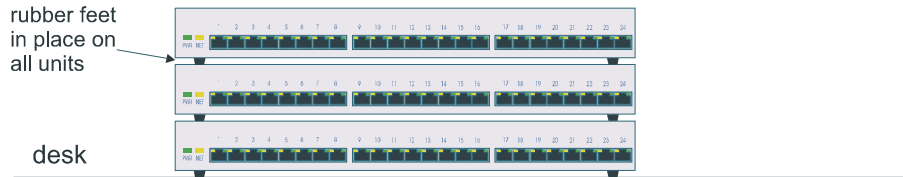
rubber feet in place on all units

desk

Caution   ***When mounting several Console Server units in a 19" rack, you must not stack more than 3 units without leaving an air gap between them.***

Caution   ***Observe maximum ambient operating temperatures within a rack; you may have to use forced air cooling.***

LED guide

During bootup you should see power and network LEDs display the following colours.

Power and network LEDs

Console Server during bootup

flickering:
green then yellow

flickers green,
or yellow if reply
received from
bootp server,
or red, if network
is not connected
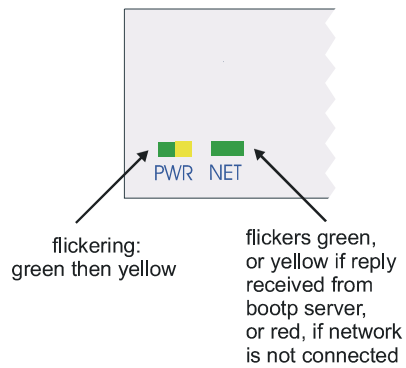
Once power is on and the network is connected, the power and network LEDs will display the following colours:

Console Server
during normal operations

PWR   NET

green,
permanently
lit

flickers:
green for transmit
yellow for receive
red for network error
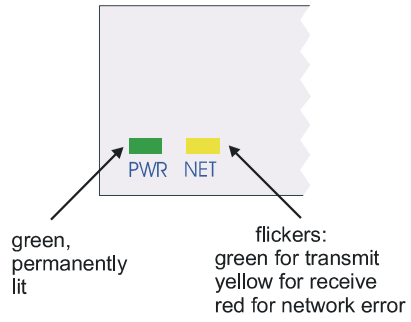
RJ45 LEDs   There are bi-colour LEDs on the RJ45 connectors on both the front and rear panels. These LEDs flicker briefly during bootup and then display the following colours,

Transmit   Receive   Speed   Link Status
LED   LED   LED   LED

(yellow)   (green)   (yellow)   (green)

RJ45 front   RJ45 rear
(Serial port)   (10/100Base T)
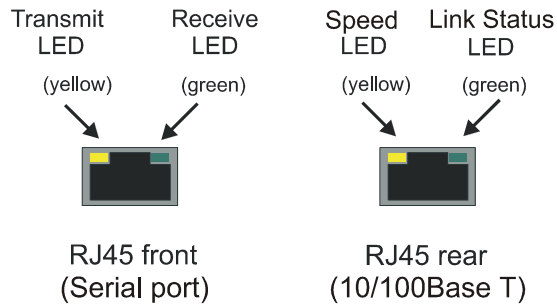
Selecting AUI or 10/100 Base T interface

Before performing the initial configuration of your Console Server unit, you need to select the type of interface you want to use from either AUI or 10/100Base-T (Default setting is 10/100Base-T). To do this proceed as follows;

Note   *To display the currently selected interface type, at the command prompt, type* ***show hardware*** *and press the* ***Enter*** *key. The resulting display will include the currently selected hardware type.*
You only need to use these commands on revision 2 Console Server boards.

1.   Login to your unit and display the command prompt.

2.   At the command prompt, type one of the commands listed in the next table to select the interface type you want to use.

To set this type of interface	Use this command
10/100Base-T	`set ethernet interface RJ45`
AUI	`set ethernet interface AUI`

You can now perform the initial configuration of the unit.

Setting up an IP address

Setting up an IP address automatically using DHCP

This section includes the following;

- Set up procedure on page 33
- About DHCP on page 35

Set up procedure

To set up an IP address automatically using DHCP proceed as follows;

Note   *For details of the BOOTP/DHCP tags (client information items) that are supported by both BOOTP and DHCP see* Appendix F BOOTP. *In addition on Microsoft Windows NT, DHCP allows for the configuration of WINS server names.*
If automatic configuration of Console Server 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 Console Server clients unless you are very familiar with the potential interactions that may result.
For information on BOOTP see Appendix F BOOTP.

1. Set up your DHCP server as required.
   See your system documentation for details of configuring the DHCP service on your server's operating system.

either:
the DHCP server
finds a matching
ethernet address
and sends a
reply to the unit

DHCP server

if there is a
DHCP reply

CS9000

or:
the DHCP server
does not find a
matching ethernet
address;
it does not
reply to the unit

DHCP request
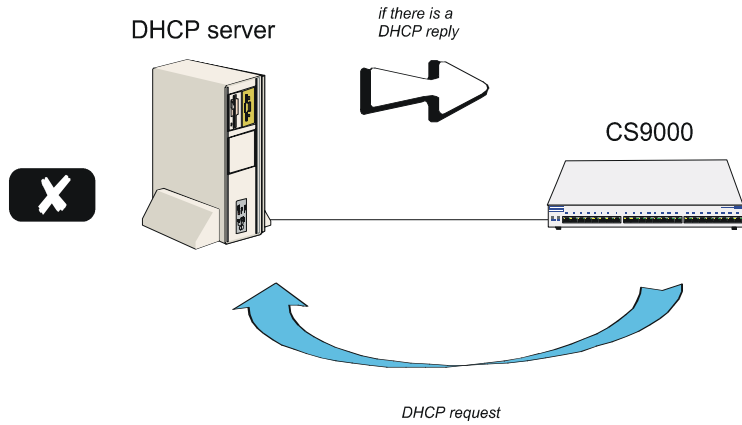
2. Connect your Console Server to the network and turn on the unit.

The IP address and any other configuration information will now be set up automatically.For more information see About DHCP on page 35.

About DHCP

You can use DHCP to perform the following actions on a single or multiple Console Server (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)

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

Another advantage of DHCP 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 DHCP process.

The the unit's implementation of DHCP is compatible with RFC 951.

On bootup or power-up, the unit will send a broadcast request to the DHCP 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 DHCP request and response on page 35.

You can stop the DHCP server from replying to the unit; see Appendix F BOOTP

DHCP request and response

either:
the DHCP server finds a matching ethernet address and sends a reply to the unit

if there is a DHCP reply

DHCP server

CS9000

or:
the DHCP server does not find a matching ethernet address;
it does not reply to the unit

DHCP request
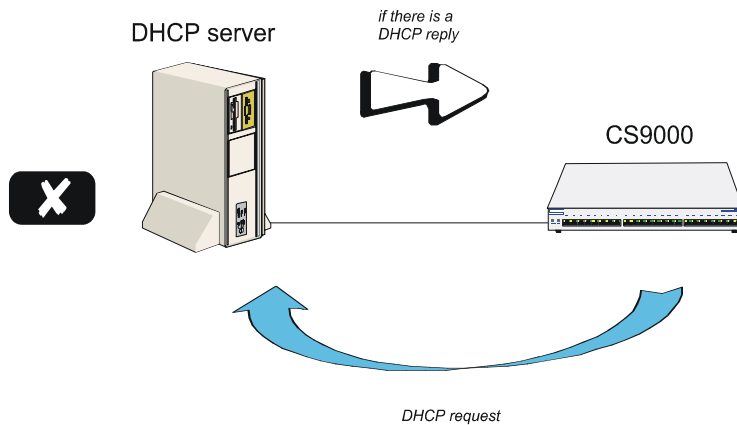
The DHCP server checks the ethernet address and looks for a matching address in its DHCP tables:

- if a matching ethernet address is found the DHCP server will reply to the unit; the reply will contain network configuration information. This information is listed in the DHCP tables 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 DHCP server does not reply; the unit boots from internal memory.

Refer to DHCP request and response on page 35 for an explanation of the following text:

the DHCP 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 DHCP 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 DHCP 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.

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 favour of BOOTP as it is supported on a wide range of network operating systems, however to ensure compatibility with existing installations, the Console Server 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 Console Server 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.

Manually setting up an IP address

This section includes the following;

Set up procedure

To manually set up an IP address proceed as follows;

1. Set up a terminal or PC running terminal emulation. For examples of connection pinouts see Appendix A Cabling information.

   If you connect via the Admin Port you will see a display of diagnostic and bootup messages.

   Note that if you cannot emulate VT100, you will have to use the Command Line Interface (cli); *(the cli commands are described in full in* Appendix B The CLI commands*).*

2. At the console, with the login prompt displayed, type *admin* and press <return>.

3. At the password prompt, now displayed type *superuser* and press <return>. This is the default admin user password.

   The command line prompt will now be displayed:

4. At the command prompt type *screen* and press <return> to enter Full Screen mode.

   The main menu is now displayed:

```
┌──────┤main menu├──────┐
│ sessions              │
│ users                 │
│ line configuration    │
│ server configuration  │
│ radius configuration  │
│ network configuration │
│ hardware              │
│ command line mode     │
└───────────────────────┘
```

5. At the main menu, select 'server configuration'. (alternatively, use the cli command set server)

   The server form will be displayed as shown in the next picture:

```
                      +server+
         servername[           ]
   internet address[172.16.1.32    ]
  broadcast address[172.16.255.255 ]
       subnet mask[255.255.0.0   ]
       domain name[                          ]
    authentication[both(local+radius)]
              dhcp[on ]
      ssh protocol[both(ssh-1+ssh-2)]
        gui access[off]
            banner[off]
          OEM_mode[    ]
```

6. Within the server form, complete the fields by moving between the fields using the arrow keys. Use the <del> key to backspace if necessary.

For a description of the fields in this form see Server form field descriptions on page 42.

Example settings for all the Console Server configuration fields are shown in the next picture:

```
                      +server+
         servername[           ]
   internet address[172.16.1.32    ]
  broadcast address[172.16.255.255 ]
       subnet mask[255.255.0.0   ]
       domain name[                          ]
    authentication[both(local+radius)]
              dhcp[on ]
      ssh protocol[both(ssh-1+ssh-2)]
        gui access[off]
            banner[off]
          OEM_mode[    ]
```

7. When you have completed the form, press <return>.

You will be presented with the following display:

8. Accept the form; you will be returned to the Main Menu.

    You may want to save your configuration changes permanently; see Saving
    configuration changes on page 62

9. Reboot the unit. Rebooting will ensure that other network devices can
    communicate with it.

Note   *If you set the port to authenticate by RADIUS only, users will not be able to dial in
          and connect if the network connection is down (no access to RADIUS server).*

Tip   *If you are not using the RADIUS service, you can leave authentication set to 'both'.
          You will have entered users in the Console Server's user table. The unit will
          authenticate users via its own user table and, provided user names and passwords
          are valid, should not need recourse to a RADIUS host.*

Server form field descriptions

The server form fields are described in the next table. You can use this information to assist with setting values in .

Parameter	Description
servername (also known as hostname or alias)	The familiar name for your Console Server.
Internet Address (IP Address)	The Console Server's unique address in the network.
Broadcast Address	The address used by the Console Server for sending information to all hosts on your network simultaneously. 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.
Subnet Mask	Allows interconnected local networks to coexist with the same network ID. This hides complicated local environment and routing information from external hosts and gateways. If you want the Console Server to belong to the same subnet as other hosts, give it the same subnet mask as them.We recommend you set a subnet mask on initial configuration
Domain Name	Unique name which describes your domain - your location in the global network. Like Hostname, it is a symbolic rather than a numerical identifier.
Authentication	You can authenticate all users connecting to the Console Server in one of three ways:

Parameter	Description
	both - (the default) firstly with the unit's own user table. If the username is found in unit but the password is incorrect, an authentication request is sent to the RADIUS host. If the username is not found in the unit, authentication is passed up to the RADIUS host. (The exception is the 'admin' user; if you supply an incorrect password, the unit will not go to the RADIUS host; it will fail the authentication).
	When the unit uses the RADIUS host, it will try firstly the primary RADIUS host and then - if one is specified - the secondary RADIUS host; (see RADIUS configuration on page 51).
	local - with the unit's user table (only)
	RADIUS - with the RADIUS host's user table (only); does not apply to username 'admin' who is always authenticated locally.
DHCP	You can use the auto configuration method for configuring the Console Server from a DHCP server. You must turn on this feature by selecting 'on' and disable this feature by selecting 'off'. Default is 'off' or DHCP is disabled.
SSH protocol	In order to provide a secure connection from the LAN to a device on the Console Server, you must enable the appropriate SSH protocol version. By default, ssh protocol is 'disabled'. To support SSH version 1, select 'ssh-1'. To support SSH version 2 only, select 'ssh-2'. To enable both version of ssh support, select 'both (ssh-1+ssh-2)'. If you are configuring ssh for the first time, you will be prompted to generate the appropriate encryption keys used for negotiating a secure connection. This key generation process could take several minutes. Once generated, the Console Server will then support the ssh protocol selected.

Parameter	Description
gui access	this parameter controls access to the Console Server's graphical configuration programme JETset.
	The default is 'off'. When set to 'on' the admin user can access the JETset from a Web browser, using the unit's internet address. Entry to the programme is then controlled by password.
	If you are not using the JETset to configure the unit, we suggest you set this parameter to 'off'; access will be denied to any person who tries to connect to the unit from their browser.
	How to access the JETset is described in Appendix G JETset.

Accessing the Console Server configuration software

Logging onto your Console Server

1. From your host, telnet to Console Server. For example, telnet 192.65.1434.15

2. A login prompt is now displayed.

3. At the console, with the login prompt displayed, type *admin* and press <return>. At the password prompt, type *superuser* and press <return>. This is the default admin user password. The command line prompt will be displayed: <product name (abbreviated)> e.g. xxxxxx, followed by the hash # sign, indicating that you are now logged in as the system administrator.

4. To enter Full Screen mode (the text-based menus), type *screen* and press <return>. The main menu will be displayed:

```
┌─────main menu─────┐
│ sessions          │
│ users             │
│ line configuration│
│ server configuration│
│ radius configuration│
│ network configuration│
│ hardware          │
│ command line mode │
└───────────────────┘
```

Setting up your network parameters

Setting up the host table

The Console Server needs to know the hostnames and internet addresses of the other hosts in the network (or any hosts anywhere on the Internet) which you want to communicate with on a regular basis. For example, gateways, RADIUS, servers and so on. These hostnames are added to the unit's Host Table. You can add up to twenty hosts. To do this;

1. From the Main menu, select 'Network Configuration'.

   The Network Configuration menu is now displayed.

2. Within the Network Configuration menu, select 'Host Table';
   The Host Table menu will be displayed:

```
┤network configuration├
 reset
 snmp
 tft┌host table├
 hos│ add host
 DNS│ change host
 WIN│ delete host
 gat
 security
 reboot server
```

You can now add (Adding a Host on page 46), change (Changing a Host on page 48)or delete (Deleting a host on page 49) a host as required.

Adding a Host

To add a host (cli syntax add host):

1. Within the Host Table menu, select 'Add Host' from the Host Table menu; this option enables you to add the *hostname* of a host to the host table.

   You will be asked to enter the hostname:

```
          ┌network configuration┐
          │reset                │
          │snmp                 │
          │tft┌host table┐─┐
  enter host name:  █
          │gat└──────────┘
          │security
          │reboot server
```
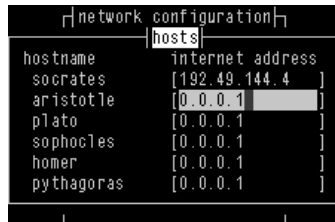
2.   Type in the name of the host (14 characters maximum) and press <return>.

Changing a Host

This option enables you to add or change a host's internet address:

To change a host (set host, show host):

1. Within the Host Table menu, Select 'Change Host' from the Host Table menu;

> This form will list all hosts added to the host table. The default internet address is 0.0.0.1.

2. Enter the correct internet address of each host. Use the <del> key to backspace if necessary.

Deleting a host

This option enables you to delete an entry from the host table. If a host is referenced by a pre-defined session, or is defined as a gateway or name server, you won't be allowed to delete it.

To delete a host (cli command delete host)

1.   Within the Host Table menu, When you select 'Delete Host', the host table will be displayed:

```
┤network configuration├
reset
snmp ┌─┤hosts│
tft ┌ │socrates
hos │ │aristotle       ▐  ▌
DNS │ │plato
WIN │ │sophocles
gat ┘ │homer
secu  │pythagoras
rebo
```

2.   Select the host that you want to delete and press <return>.

You will be asked to confirm the deletion:

```
        ┤network configuration├
        reset
        snmp ┌─┤hosts├
        tft │ socrates

confirm delete host 'sophocles' (y/n)

        gat ┘ homer
        secu  pythagoras
        rebo
```

3.   Type 'y' to delete the host, 'n' to cancel the command.

Changing the Admin Password

cli syntax:
set user
password

To change the Admin password proceed as follows;

1. Within the Users menu, select 'Set Password'.

2. From the list now displayed, select 'admin' user.

    You will be prompted to enter a password. This can be up to sixteen characters. Use the <del> key to backspace if necessary.

3. At the prompt, enter the password and press <return>.

    You are now prompted to enter the password a second time to confirm your choice.

4. At the prompt, re-enter the password and press <return>.

The password change will take effect next time you log in.

Note   *The factory default password is **superuser.***

RADIUS configuration

This section includes the following:

-

-

Set up procedure

To configure how the Console Server interacts with the RADIUS host or hosts:

1. From the Main menu, select '**radius configuration**':

2. Within the radius configuration menu, select from one of add/delete authentication/accounting host.

   A list of hosts from the unit's host table is now displayed (see):

3. Highlight your selection and press <return>.

   You will be asked to enter a 'secret' (a password):
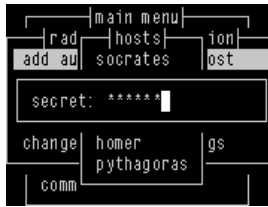
4. Key a maximum of sixteen alphanumeric characters.
To change the secret you must delete the host and then add it again; when you add a host you are prompted for a secret.The first host entered becomes the primary authentication/accounting host, the next host entered becomes the secondary host. You can enter a maximum of two hosts in each of the fields.

You must enter the same secret in the RADIUS host (see your RADIUS documentation); the secret is not transmitted over the network. Note that to set RADIUS authentication on/off, go to back to the Main Menu and select 'server configuration'. See Setting up an IP address on page 33.

5. Select '**change radius settings**', you are presented with the following (shown in the next picture):
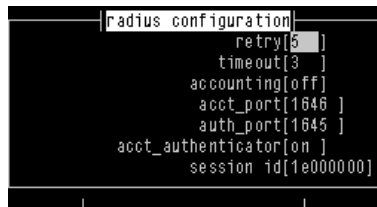
The RADIUS parameters are described in RADIUS parameters description on page 54.

6. When you have completed the form, press <return>. You will be presented with the following display:

```
┤radius configuration├
         retry[5  ]
       timeout[3  ]
    ┤options├        f]
accept and exit form  46 ]
                     45 ]
acct_authenticator[on ]
    session id[1e000000]
```

7.   Accept the form; you will be returned to the menu.

Tip   *You may want to save your configuration changes permanently; see* Saving
           configuration changes on page 62

RADIUS parameters description

The RADIUS parameters are as follows:

retry

(for authentication) the number of times the unit will re-send a request to a RADIUS authentication host, before re-presenting another login to the user.

(for accounting) the number of times the unit will re-send a request to a RADIUS accounting host, before understanding that the accounting request has failed.

The default retry value is 5; the unit will try the primary host up to 5. You can enter values between 0 (don't retry) and 255. If you have different authentication and accounting hosts unit will retry first the authentication host(s) and then the accounting host(s).

timeout - the time in seconds between unit sending a request to a RADIUS accounting or authentication host and receiving a reply. If no reply is received before the expiry of the timeout period, the unit will retry the same host up to and including the number of retry attempts specified under 'retry'.

The default timeout period is 3 seconds (you can enter values between 1 and 255).

accounting - turns accounting on or off within the unit; the default is off.

RADIUS
accounting

RADIUS host specified	accounting flag	state of RADIUS host	result
no	off	-	no accounting
yes	on	up	accounting in both Console Server and RADIUS host
yes	on	down	accounting in Console Server only

Notes on Table above:

'accounting' within the Console Server is an increment of the session id (see below).

'accounting' in the RADIUS accounting host means that you should be able to see accounting information by interrogating the host (see your RADIUS documentation).

acct_port - the UDP port number for RADIUS accounting. The default value is 1646 which should match most RADIUS implementations. Change this value if your RADIUS host is using a different UDP port number.

auth_port - the UDP port number for RADIUS authentication. The default value is 1645 which should match most RADIUS implementations. Change this value if your RADIUS host is using a different UDP port number.

acct_authenticator - a flag to instruct the unit to check the authenticator field in the accounting reply transmission from a RADIUS host to the unit. The authenticator field contains the secret, encrypted. The options are 'on' (the unit will check this field) or 'off' (the unit will not check this field); the default is 'on'. Make sure the setting in your RADIUS host is the same as the unit.

session id - displays in real-time the hexadecimal value of the current session (incrementing with each session). The current session is the most recent connection into the unit when the line service is set to 'cslogin' (the default line service).

You can reset the session id to zero; enter 0s from your keyboard.

An explanation of the eight digit value displayed in the session id field is as follows:

> the first two digits show the number of reboots which have taken place. The maximum number which will be shown is ff (255); on the next reboot, this value will reset itself to 01 (1).

> the last six digits show the number of user sessions which have started since the last reboot (on reboot these six digits are reset to zero). The first session will be 000001, the second session will be 000002, etc. The maximum number of sessions is approximately 16 million, i.e. ffffff, at which point the counter would reset itself to all zeros, i.e. 000000.

> An example of all eight digits in a session id is:

> `0a000006`

> which means there have been 10 reboots (0a) of this unit (since the counter was reset or wrapped around) and 6 (000006) sessions started since that reboot.
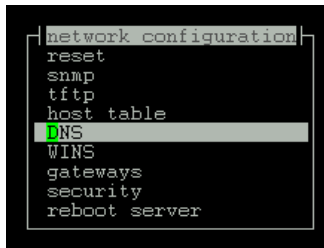
Sessions are measured through the RJ45 ports on the front panel; connections through any of the ports on the rear panel are not shown.

DNS configuration

You can enter the addresses of two DNS hosts in the Console Server (the '*unit*'); one will be 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 Appendix D RADIUS & Networking.

To configure DNS host proceed as follows;

1.   From the Main menu select '**network configuration**':

```
┌─┤network configuration├─┐
│ reset                   │
│ snmp                    │
│ tftp                    │
│ host table              │
│ DNS                     │
│ WINS                    │
│ gateways                │
│ security                │
│ reboot server           │
└─────────────────────────┘
```
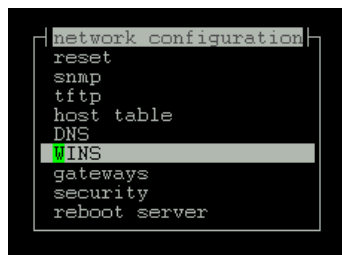
Cli syntax: 2.   From the network configuration menu, select DNS.

add DNS   The Add/Delete DNS menu is now displayed.

3.   Within the Add/Delete DNS menu select the Add DNS option.

You are now prompted to enter an internet address;

4.   Enter this address in dot decimal notation. If you wish, it can be the same address as a machine already entered in the unit's host table.

The first host entered becomes the primary DNS host, the next host entered becomes the secondary host. You can enter a maximum of two DNS hosts.

delete DNS   5.   If required, change the DNS entry by deleting it, then entering the replacement value.

WINS configuration

WINS (Windows Internet Name Service) is a database of hostnames and corresponding internet addresses. It is a Microsoft specific name resolution service. The basic function of WINS is the similar to DNS, i.e. it maps computer names to TCP/IP addresses for client computers on a network. For more information on WINS see Appendix D RADIUS & Networking.

You can enter the addresses two WINS hosts in the unit; one will be the primary host, the other a secondary host. 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 WINS parameters in his/her computer.

1. From the Main menu select '**network configuration**':

Cli syntax: 2. From the network configuration menu, select WINS.
add WINS
         You are now prompted to enter an internet address;

3. Enter this address in dot decimal notation. If you wish, it can be the same address as a machine already entered in the unit's host table.

         The first host entered becomes the primary WINS host, the next host entered becomes the secondary host. You can enter a maximum of two WINS hosts.

delete WINS 4. If required, change the WINS entry by deleting it, then entering the replacement value.

Configuring network gateways

Gateways are hosts that connect Local Area Networks (LANs) together. If you want to access a host which isn't on your local network you will be connected via a gateway. Gateways route data via other gateways until the destination local network is reached. There are three types:

- **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.

The unit allows you enter a maximum of twenty gateways.

Particularly useful when checking routes to/from gateways is the *show routes* command;.

Active and passive gateways

The unit supports both active and passive gateways. The default is active. Definitions of these types are as follows:

Active gateway: a gateway which is temporarily listed in the unit's routing table (while RIP packets are received). If the unit detects that the gateway is no longer operating (no RIP packets received) it will be deleted from the routing table.

Passive gateway: a gateway which is permanently listed in the unit's routing table. It is thus always available.

See the following for how to configure gateways:

- Adding a gateway on page 59

- Deleting a Gateway on page 60.

Adding a gateway

To add a gateway proceed as follows:

1. From the Network Configuration menu, select 'Gateway'.

2. From the Gateway menu, select 'Add Gateway'.

3. From the host table now displayed, select a host.
    Note that you can define a host only once as a gateway.
    When you have added a gateway, you must define its type.

4. From the Gateway menu, select 'Change Gateway'.

    The Gateways form is now displayed (for example):

    This form lists all gateways defined for your network. In this example, only one
    has been defined.

5. Complete the Type field; the values are 'host', 'network' or 'default'.

    If you set the field to 'host' or 'network', you must include the internet address of
    the target host or network. If you change a gateway from 'host' or 'network' to
    'default', the internet address will be ignored.

6. Complete the 'Status' field; the values are 'active' or 'passive'.

Note   *the gateways configured in this table will be ignored if you have used DHCP or
           BOOTP to download a single passive gateway into the unit; see* Appendix F
           BOOTP.

Deleting a Gateway

delete gateway

If a host on your network is retired from gateway duty, you can use this option to delete it from the list of gateways. Note that the host will NOT be deleted from the host table.

To delete a gateway proceed as follows:

1. From the Network Configuration menu, select 'Gateway'.

2. From the Gateway menu, select 'Delete Gateway' to list your gateways:

```
┌network configuration├
 reset
 snmp
 tf┌─gateway├
 ho┌delete gateway├
 DN│ socrates
 WI│ plato
 ga│
 security
 reboot server
```

3. Delete the gateway you require from the list.

Verifying your network installation

To check that you have installed the Console Server (the '*unit*') successfully proceed as follows;

1. At the command prompt, try to ping a remote host by typing the following command:

   ping *hostname*

   Choose a host that you have defined in the host table. If no packet loss is reported, your unit is ready to use.If the command returns an error, refer to the ping cli command. See Appendix B The CLI commands;

Saving configuration changes

Saving to non-volatile memory

To save your configuration settings to non volatile memory proceed as follows;

1. After making changes to the configuration exit the text menu screen (form) you are using.

   The 'options' form now appears:
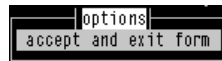
2. Within the options form select 'accept and exit form' to retain your changes in RAM (volatile memory).

3. To save your changes permanently exit the text menu system completely then return to the Main Menu and select 'command line mode';

   The exit full screen mode form is now displayed:

4. Within the 'exit full screen mode' form select '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.

5. To return the menus, at the command prompt, 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 Appendix B The CLI commands.

Setting date and time

The Console Server (the '*unit*') has a real-time clock which you can set and view. It is battery-backed and therefore will operate when power is off and over reboots. The clock is year 2000 compliant.

To set the date and time on your unit proceed as follows;

1. From the Main Menu select `Hardware`.

    The hardware form is now displayed. Only the `date` and `time` fields are user editable.

```
                        hardware
            mac address 0080ba0000c2
               board id CS4300076R1.6
             processor 80386
                  uarts 2 * Perle ASIC
             flash rom 1 x 1MB
                   ram 2 x 2MB
            battery ram 32kB
           serial ports 16


                  date[23/2/2001 ]
                  time[14:51:05   ]
```

2. Identify your unit using the hardware information displayed.
    (To view hardware details in command line mode (cli) use the command `show hardware`).

3. Within the 'hardware' form. move the cursor to the start of the field using the 'delete' key; then enter information in the format (for the date):

    `DD/MM/YYYY e.g. 30/03/2001`

    and in the format (for the time):

    `HH:MM:SS e.g. 20:32:00`

    Note that you do not have to enter the number of seconds.

4. Alternatively, in command line mode (cli) enter the commands 'set date' and 'set time';

To view the date and time select 'hardware' from the Main Menu and check the 'hardware' form; In command line mode, enter the commands Show date, Show time, or Show hardware.

Performing a soft reboot

To perform a soft re-boot (cli syntax: reboot);

1. From the Network Configuration menu, select 'Reboot'.

    You will be asked whether you wish to save your configuration changes to non-volatile memory:

    ```
    ┌network configuration┐
     reset
     snmp
     tftp

    save config to flash ROM (y/n)

     gateways
     security
     reboot server
    ```

2. At the prompt, type y and press the Enter key.

The unit will close all connections and then reboot.

Restoring factory default settings

Resetting to factory defaults using software

This feature enables you to reset the unit to its default settings. This will clear all configuration data entered by the admin user, and all user accounts, except the default admin user, will be deleted.

To reset to factory default settings from within the software (cli syntax: reset factory):

1. From the Network Configuration menu, select 'Reset'.

    You will be asked to confirm the reset:

```
┌network configuration┐
│ reset                │
│ snmp                 │
│ tftp                 │
└                     ┘
 confirm reboot unit (y/n)

   gateways
   security
   reboot server
```

2. At the prompt, type 'y' to reset the unit, or 'n' to cancel the command.

Resetting to factory defaults using reset switch

To reset to factory defaults using the reset switch, proceed as follows;

Power
Connector

Admin
Port

10/100
Port

MAC address label

Ethernet Address

110 - 240V
0.5 - 1 A
50 - 60 Hz
AC (~)
25W

ADMIN

FACTORY

RESET

10 BASE T

AUI

ON/OFF
switch

Factory
Reset
Recessed
Switch

AUI
Port
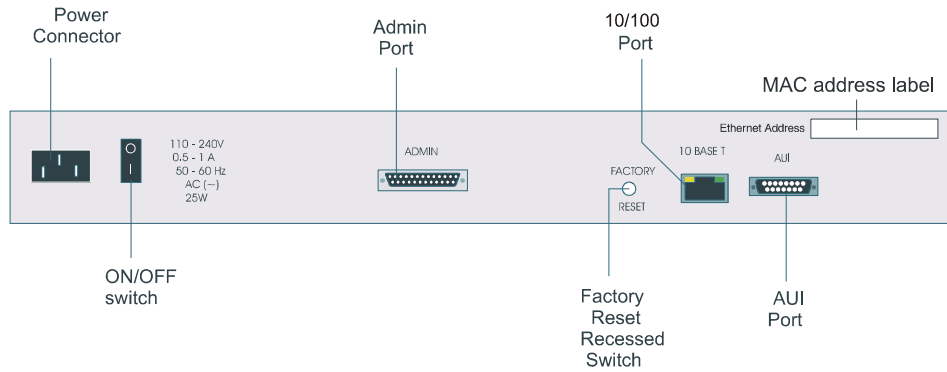
1. Use the tip of a pen or pencil to press the reset switch located on the rear of the
    unit.

The Console Server will then reboot and reset itself to factory default settings.

Chapter 3 System administration

You need to read this chapter if you want to do system administration with the Console Server.

This chapter provides task oriented information on system administration with the Console Server.

This chapter includes the following sections;

- Security on page 70

- Setting up the line on your Console Server on page 70

- Viewing and editing your line settings on page 71

- Lost password on page 73

- Configuring a dial in line on page 74

- Configuring users on page 94

- Configuring Break Pass Through on page 110

- Resetting the line to default on page 111

- Saving your settings on page 112

Security

The Console Server has a number of security features built in that can be enabled or disabled depending on the security level required.

These features include:

- Telnet access - Login and password required.
  See set line on page 166 in Appendix B The CLI commands.

- SSH access - Makes ports only accesible via SSH connections.
  See Accessing devices via SSH on page 118 in Chapter 4 Using your Console Server.

- Radius authentication - Allows user names and passwords to be authenticated by an external Radius server.
  See About user accounts and RADIUS on page 96 in Chapter 3 System administration.

- Disable Daemons - Allows unused Daemons to be disabled to prevent unauthorised access by hackers.
  See set server on page 173 in Appendix B The CLI commands.

- Trusted host filtering - Prevents the unit from being seen on the network by non-authorised systems
  See set server on page 173 in Appendix B The CLI commands.

Setting up the line on your Console Server

The default use of the Console Server is as a Console server. Therefore all lines are set with a service of "Reverse Telnet". This allows a user on the LAN to be able to telnet into the ports and access the attached devices.

Each port also requires a TCP socket number in order to work. By default, the unit is set to use numbers 10001 to 10024. You can change these to any other socket number as long as there is no conflict on the network.

For an explanation of other line services see Appendix E Summary of Line Service Types.

Viewing and editing your line settings

Lines set to reverse Telnet by default

cli syntax:
set line

A reverse telnet connection enables a TCP/IP host on the local network to establish a login connection via a Console Server (the '*unit*') port on a non-TCP/IP machine external to the network, such as routers, servers and so on.

A Typical
Reverse
Telnet
Configuratio
n
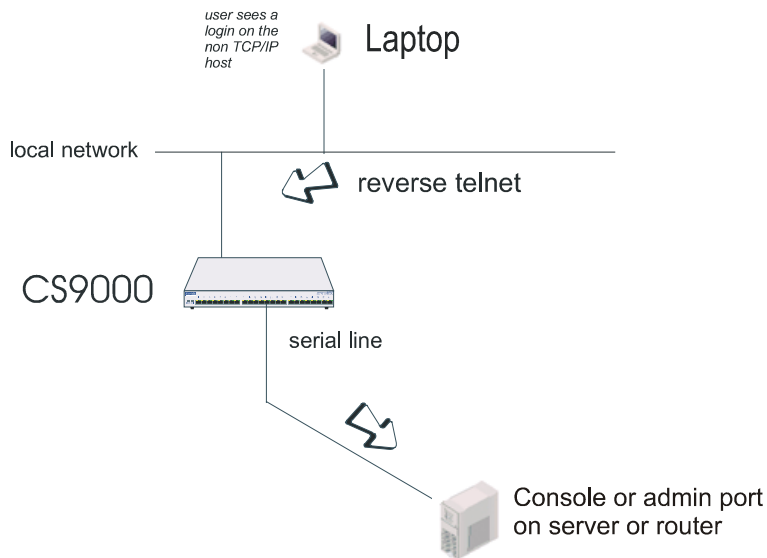
To set up a reverse telnet connection, follow these steps:

1. Select Line Settings from the Line Configuration menu then select the line that you want to configure.

2. Set 'service' to rev tel (default setting).
    Note when field is highlighted, pressing L will list all available options.

3. Assign a TCP port number to the unit port using the 'CS 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 (By default, lines are set to TCP port 10001 to 10024 for each port. For example, Line 1 10001, Line 16 10016).

4. Do *not* configure the idle and session timers; these timers have no effect on reverse telnet connections.

5. The 'Hostname' and 'Host Port' fields may contain default or last-used values, but these will be ignored.

6.   The line should now be configured similar to that shown in the next picture:

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

8.   If you want to configure all lines with the same parameters, refer to .

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 Console Server (the '*unit*') to its factory default settings.

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

Configuring a dial in line

Introduction to SLIP and PPP connections

This section deals with setting up SLIP and PPP connections on a line. There is also a summary of the configurable features of modems.

Deciding whether to 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 Configuring PPP on page 82, 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 Configuring PPP on page 82 for more details.

For more information on the SLIP and PPP protocols see Configuring a dial in line on page 74.

Setting up the line

1. From the Line Configuration menu, select 'Line Settings'.

2. Within the Line settings menu, select a particular line; e.g. line 3.

   The line form will be displayed (default values shown in the next example):

```
                            ┌─line─┐
                            │line 2│
   service[rev tel]         └line name[                    ]

      speed[9600  ]            terminal[dumb  ]
      flow[none]
      bits[8]                      user[              ]
   parity[none]               hostname[a           ]
      stop[1]               host port[23    ]
                              CS port[10003]


      dial[none ]           modem name none
phone number[                              ]

   idle timer[          ]  session timer[          ]
```

3. Within the line form, set the **Service** field using one of the options given in the next table;

Service option	Description
PPP	When you want a remote access service connection using PPP, or when you want to use the unit as a router with PPP. In both cases the user (whether real or dummy) will be authenticated within PPP (provided you use Security - PAP or CHAP).
cslogin	When you want a remote access service connection 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 Configuring a user account on page 100). Choosing the 'cslogin' option, the unit will present the login prompt: the user will be required to enter a name and password and hence will be authenticated.
SLIP	When you want to use the unit as a router with SLIP. There will be no authentication of each unit by the other unit.

Option	Description
Line name	Line name can be configured to uniquely identify the line.
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 to either 'soft' (software) or 'hard' (hardware). 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 82)
Host port field.	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.
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 *router use only*	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 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.

Service option	Description
Session Timer *router use only*	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).

<table>
<tr><td></td><td>4.</td><td>Ignore the other fields in this form. Press <return> to exit; if you do not wish to save your changes press the <escape> key.</td></tr>
<tr><td rowspan="2">cli syntax:
add modem</td><td>5.</td><td>Now go to the Line Configuration Menu:</td></tr>
<tr><td>6.</td><td>Within the Line Configuration Menu, select 'Add Modem'.</td></tr>
<tr><td></td><td>7.</td><td>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.</td></tr>
<tr><td></td><td>8.</td><td>Within the Line Configuration Menu, select 'Change Modem'. Select your modem/ISDN TA name. Enter the initialisation string; see your modem/ISDN TA documentation.</td></tr>
<tr><td></td><td>9.</td><td>Press <return> to exit; if you do not wish to save your changes press the <escape> key.</td></tr>
<tr><td>set line</td><td>10.</td><td>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.</td></tr>
<tr><td></td><td>11.</td><td>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);

You can reset this line to default (an option as you exit this form); refer to Resetting the line to default on page 111</td></tr>
<tr><td></td><td>12.</td><td>You may want to save your configuration permanently; if so, refer to Saving settings to non-volatile memory on page 112.</td></tr>
</table>

Configuring SLIP

cli syntax:
set slip line,
show slip
line

To configure the SLIP parameters proceed as follows;

1. From the Line Configuration menu, select 'SLIP' and then select a line.

   The SLIP form is now displayed (default values shown):

2. Within the SLIP form, set the parameters listed in the next table:

Option	Description
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.

Option	Description
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 Configuring a user account on page 100, sub-section 'framed ip'. If your user is authenticated by RADIUS *and* the RADIUS parameter 'Framed-Address' is set in the RADIUS file 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 the unit will use the value in the RADIUS file in preference to the 'Subnet Mask' value configured here.
Maximum transmission unit	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 Configuring a user account on page 100, 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 Configuring a user account on page 100, sub-section 'framed mtu'. If your user is authenticated by RADIUS *and* the RADIUS parameter 'Framed-MTU' is set in the RADIUS file 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.

Option	Description
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 Configuring a dial in line on page 74 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 Configuring a user account on page 100, sub-section 'framed compression'.
	If your user is authenticated by RADIUS *and* the RADIUS parameter 'Framed-Compression' is set in the RADIUS file 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'.

Configuring PPP

This section describes how to configure a dial in line using PPP and includes the following:

An example of a remote access connection using PPP, including the setup of a remote user is described in Configuring a dial in line on page 74.

PPP configuration procedure

cli syntax:
set PPP line,
show PPP
line

To configure a line using PPP proceed as follows;

1. Within the Line Configuration menu, select 'PPP'.

2. Now select a line.

   The PPP form for the selected line is now displayed as shown in the next picture (default values shown in this example):

3. Within the PPP form set all the fields to the values you require. See PPP form field descriptions on page 83 for details of how to set each field within the PPP form.

PPP form field descriptions

This section describes the fields and settings used in the PPP form referred to in PPP configuration procedure on page 82. The following fields are described in this section.

- Local ip address on page 84

- Remote ip address on page 84

- Subnet Mask on page 84

- ACCM on page 85

- Max. receive unit on page 85

- Security on page 85

- User on page 87

- Password on page 87

- Remote User on page 87

- Remote Password on page 88

- Address/Control comp on page 88

- Protocol compression on page 89

- VJ Comp on page 89

- Magic No. negotiation on page 89

- IP address negotiation on page 89

- Configure req. timeout on page 90

- Terminate req. timeout on page 90

- Configure req. retries on page 90

- Terminate req. retries on page 90

- Configure NAK retries on page 90

- Authentication timeout on page 90

- Roaming callback on page 90

- Challenge_ interval on page 92

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 'Setting up an IP address on page 33'. 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 Configuring a user account on page 100, sub-section 'framed ip'.

If your user is authenticated by RADIUS *and* the RADIUS parameter 'Framed-Address' is set in the RADIUS file 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 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 75) 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 Configuring a user account on page 100, 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 Configuring a user account on page 100, sub-section 'framed mtu'.

If your user is authenticated by RADIUS *and* the RADIUS parameter 'Framed-MTU' is set in the RADIUS file 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:

- authenticate a port or user on the unit, from a remote location, or

- 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.

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 'cslogin', 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. CS_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 I 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 I 6 ruser kevin)

When connecting together two networks, enter a dummy user name; e.g. CS_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 comp   This 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 compression	This 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 Configuring a dial in line on page 74 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 Configuring a user account on page 100, sub-section 'framed compression'.

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

Magic No. negotiation	This 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 (Configuring a user account on page 100), 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)
Authenticatio n 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 Roaming callback on page 90. Roaming callback can only work with a user whose (fixed) callback parameter is set to 'on'. See Configuring a user account on page 100. Roaming callback therefore overrides (fixed) callback.To use roaming callback, the remote end must be a Microsoft Windows which support Microsoft's Callback Control Protocol (CBCP) The user is allowed 30 seconds to input a telephone number after which the unit ends the call.

```
                          ┌─────────────────┐
                          │    PPP line     │
                          └────────┬────────┘
                                   │
                          ┌─────────────────┐
                          │    ROAMING      │
                          │    CALLBACK     │
                          └────────┬────────┘
```

OFF   **ON**

-

for the particular user you must set (fixed) callback to 'on'. See Configuring a user account on page 100. Unless fixed callback is set to on for user, he/she cannot receive roaming callback.

the user must initially dial into the unit on a line where roaming callback is set to 'on'. You must therefore provide the user with the telephone number for this type of line(s).

the unit can still provide fixed callback - provided you have set the (fixed) callback parameter to 'on' for that particular user; see Configuring a user account on page 100.

after successful authentication the unit will prompt the user for a telephone number to call him/her back. After receipt of the number, the unit will drop the line, call the user back on that telephone number. The user will be authenticated again (a precaution).

*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 unit.

Configuring a modem

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

Note   *all references to modems apply equally to ISDN Terminal Adaptors*

cli syntax: •   you can set the 'dial' parameter to 'in', 'out' or 'none' (default 'none') in the line
set 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. cslogin, 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.

add modem   •   when the 'dial' parameter to 'in' and the line service is set to 'cs_login', 'slip' or
set modem   '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.

See add modem on page 146 in Appendix B The CLI commands.

Configuring users

You need to configure user accounts on the Console Server (the 'unit') for those users who are tasked with administering the attached devices 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 Configuring a dial in line on page 74.

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

```
                              +user mark+
              username mark
     screen switch[1 ]                         level[normal    ]
          service[csprompt ]                 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 Configuring a user account on page 100.

When telneting or using SSH to connect to a port, the user will need to supply a user name and password.

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 About user levels on page 108. A maximum of 32 user accounts can be created.

This section includes the following:

• About user accounts and RADIUS on page 96

• Adding a user account on page 99

• Configuring a user account on page 100

About user accounts and RADIUS

Overview

You can have a maximum of 32 user accounts on the Console Server. You will also be able to configure user accounts on the RADIUS 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.

Caution   *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.*

When RADIUS authenticates users

If the unit cannot authenticate user, it will send an authentication request to the RADIUS host

....or.......

The unit will not try to authenticate user, it will send an authentication request to the RADIUS host

CS9000

Authentication in the unit set to either "both" or "radius"

User dials into the unit and inputs user name and password

user situated either locally or remotely
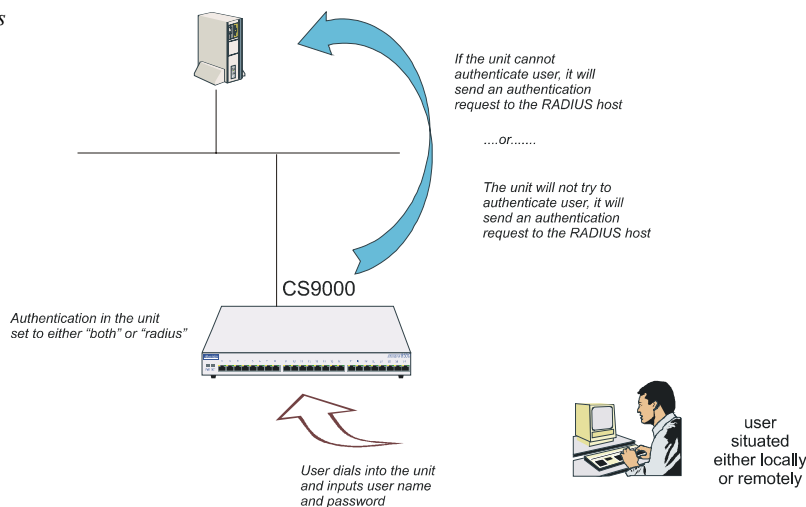
Caution   *If you set the port to authenticate by RADIUS only, users will not be able to dial in and connect if the network connection is down (no access to RADIUS server).*

RADIUS host authenticates
the user.
In this example the username
and password are correct

....so.......

The RADIUS host sends
instructions for the service
which the unit should provide
to the user

CS9000

user
situated
either locally
or remotely

The unit starts a user service
(e.g. telnet, SLIP) with configuration parameters
passed down by the RADIUS host.
These parameters apply to the user and to the line.
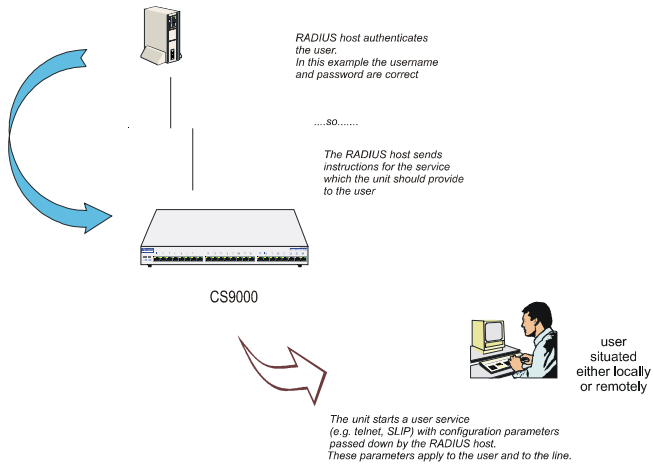
Example RADIUS user file: telnet service

```
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 Example RADIUS user file: telnet service on page 98 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 Configuring a dial in line on page 74 for a more detailed discussion on line parameters.

Adding a user account

To add a user account, proceed as follows;

1. Within the Users menu, select 'Add User' (cli syntax: add user).

2. Enter a username, maximum sixteen characters (do not use spaces). If your user is equipment allocate an appropriate name, e.g. barcode2.

3. 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 Changing a user's password on page 109. Normal users can change their own passwords; see Changing a user's password on page 109.

Configuring a user account

The section includes the following:

-

-

-

-

Configuration procedure

To configure a user account, proceed as follows;

Tip   *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* Configuring a dial in line on page 74.

1.   Select 'Change User' from the Users menu (cli syntax: set user).

2.   Choose your user from the list of names now displayed.

     A user form will now be displayed as shown in the next example (uses default values):

```
                         +user mark+
         username mark
   screen switch[1 ]                         level[normal   ]
        service[csprompt ]                 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 ]
```

3.   Within the user form, set the fields you require.See User form field descriptions on page 101 for a description of how to set each field in more detail.

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

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.*

User form field descriptions

This section describes the fields within the user form detailed in Configuration procedure on page 100.The following fields are included:

- Service on page 102

- TCP Port No on page 103

- phone number on page 103

- idle timer on page 103

- session timer on page 103

- Level on page 103

- IP Host on page 103

- callback on page 104

- Callback for a user on page 105

- framed ip on page 107

- framed netmask on page 107

- framed mtu on page 107

- framed compression on page 108.

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

csprompt: 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.

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.

Rlogin: an Rlogin service provided by the unit. Use this service when you are 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.

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.

SLIP: The SLIP service will be started using the SLIP parameters set for that line; see Configuring SLIP on page 78. 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 'cslogin'; see* Setting up the line on page 75.

PPP: The PPP service will be started using the PPP parameters set for that line; see Configuring PPP on page 82. 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 'cslogin'; see* Setting up the line on page 75.

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* Configuring a user account on page 100.

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.

Level   This field cycles through 'admin', 'normal' and 'restricted'. These are privilege levels and are described in Configuring a dial in line on page 74. The 'admin' user (i.e. you as system administrator) always has 'admin' level account (maximum privileges).

IP Host   *(ignore this field unless you have selected a user **service** of 'telnet' or 'rlogin' or 'tcp clear').*

> 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 Console Server, (or in the cli see command 'set server'). The IP address entered here does not affect the host table or any line configuration.

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.

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.

callback (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).

Note: 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 82, sub-section 'Security'), because these protocols provide authentication.

For a diagrammatic view of callback, see Callback for a user on page 105. 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 82.

*Callback for
a user*

Configuration area	User
parameter	**CALLBACK (fixed)**
Value	OFF → ← ON
other actions necessary	-
	the line must have authentication: for SLIP, set line service to CS_login (set user service to slip) for PPP, set line service to PPP, and turn on either PAP or CHAP (set user service to PPP)
	enter a telephone number for the unit to dial the user
result	The unit will not provide any type of callback to the user, neither fixed nor roaming. *Note: Roaming callback is described in* Configuring PPP on page 82
	The unit will call the user back, after successful authentication, using the telephone number entered for that particular user. ***except.....*** when, for that PPP line, roaming callback is set to 'on'. In this situation, the unit will override the fixed callback and it will provide roaming callback to the user. See Configuring PPP on page 82. In both situations the unit will require the user to log in again (a security precaution).

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 Configuring SLIP on page 78 or Configuring PPP on page 82.

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 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 Configuring SLIP on page 78 or Configuring PPP on page 82.

framed (use only when the user service field is set to 'slip' or 'ppp') this parameter
compression 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 Configuring SLIP on page 78 or Configuring PPP on page 82.

If you set up any restricted users, you must predefine their sessions; they can only open sessions predefined for them by the admin user.

About user levels

There are four user levels which can be used to determine the level of access the user has to Console Server 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.

Note: When users are authenticated by a Radius host, each user will be entitled to Normal user level access.

CLI prompts

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

Changing a user's password

To change a user's password, proceed as follows;

1. Within the Users menu, select 'Set Password' (cli syntax set user).

2. 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 <del> key to backspace if necessary.

3. Enter the password and press <return>.

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

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

Deleting a user account

To delete a user account, proceed as follows;

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

1. Within the Users menu, select 'Delete User' (cli syntax delete user).

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

    You will be asked to confirm the deletion;

3. Type 'y' and press <return>.

The user will be deleted.

Configuring Break Pass Through

The Console Server will not send break signals on power cycles. It is also configured not to allow break signals to be sent through to attached devices by default. However, some administrators may wish to be able to send the break signal i.e. to take a Sun Solaris system to the Open Boot prompt.

To enable this feature, please use the following CLI command to enable/disable proprietary inband SSH break signal processing as well as existing Reverse Telnet break signal.

set server break <on/off>

save

The OEM mode flag 0x0010 will be set/reset based upon this command. Alternatively, you can enable/disable this feature but using "set server OEM_mode".

A break signal is generated on a specific serial port only when the server's break option is enabled and the user has typed the exact break string over a reverse SSH connection.

The OEM mode flag 0x0010 will be set/reset based upon this command. Alternatively, you can enable/disable this feature but using "set server OEM_mode".

For SSH, the default break signal is '~break', where ~ is tilde. To change the SSH break signal, use the following command:

set server sshbreakstring <8-characters>

Note   *A terminal emulator must be used that is capable of sending the break signal.*

Resetting the line to default

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).

To reset the line to the default settings proceed as follows;

1. Within the Line Configuration Menu, select Line settings (cli syntax reset line).

    The Line Settings form is now displayed

2. Within the Line Settings form, with the cursor at any position inside the form, press <return>.

3. The Options form is now displayed:
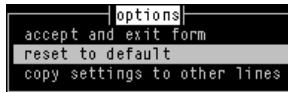
4. Within the Options form, select 'reset to default'.

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 'rev tel', the TCP Port '23', the Idle Timer '300' seconds and the hostname the first host entered in the host table.

Saving your settings

Saving settings to non-volatile memory

1. After making changes to the configuration, exit the text menu screen (form) you are using.

   The 'options' form now appears:

   ```
   ┌──options──┐
   │accept and exit form│
   ```

2. Within the options form select 'accept and exit form' to retain your changes in RAM (volatile memory).

3. To save your changes permanently exit the text menu system completely then return to the Main Menu and select 'command line mode';

   The exit full screen mode form is now displayed:

   ```
   ┌─main menu├─┐
   │ sessions   │
   │┤exit full screen mode├│
   │exit and save changes │
   │exit without saving changes│
   │return to main menu   │
   │                      │
   │ hardware             │
   │ command line mode    │
   ```

4. Within the 'exit full screen mode' form select '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.

5. To return the menus, at the command prompt, type: screen

Saving settings 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** Appendix B The CLI commands

Chapter 4 Using your Console Server

You need to read this chapter if you want to...

You need to read this chapter if you want information on how to use the Console Server as a console server.

This chapter provides task orientated information on using the Console Server as a console server.

This chapter includes the following sections

- Introduction on page 116

- Accessing devices via Telnet from the LAN on page 117

- Accessing devices via SSH on page 118

- Accessing devices via modems using PPP on page 122

- Accessing devices via modems using a dumb device on page 123

For details of installation procedures, see Chapter 2 Installation.

For information about performing system administration tasks with your Console Server, see Chapter 3 System administration.

For information on using your Console Server as a console server, see Chapter 4 Using your Console Server.

Introduction

Once the unit has been configured and users added using the procedures given in Chapter 2 Installation and Chapter 3 System administration, you can begin to use it as a console server.

There are three methods of accessing the devices attached to the serial ports:

- Accessing devices via telnet from the LAN. See page 117

- Accessing devices via SSH from the LAN. See page 118

- Accessing devices via modems on a dial in link using PPP. See page 122

- Accessing devices via modems on a dial in link with no network. See page 123

Accessing devices via Telnet from the LAN

In order to perform this function you must have a system capable of running a telnet session.

Terminal emulators Microsoft Windows does have an implementation of telnet but it is limited. You may wish to use a terminal emulator package such as:

> Term - Century Software - www.censoft.com (eval available)
> NetTerm - shareware

Information required

To connect to a specific device you must know the following information:

• ip address of Console Server device is connected to

• Port on Console Server device is connected to

• TCP socket number of port (by default port 1 will be 10001, port 2 10002 etc.)

Access procedure

To access a device using Telnet proceed as follows;

1. Set your terminal emulator to connect to the ip address of the Console Server and set socket number for correct port.

2. If running from command line, run following command:
   telnet 'ipaddress' 'socket num'
   Example - telnet 192.65.121.4 10004

   A Console Server login prompt will then be displayed.
   Note: To disable this feature use the cli command, *set line security <on/off>*

3. At this prompt, enter your user name for the Console Server and press enter.

4. At the password prompt, enter your password for the Console Server and press enter.

You will now be connected to the port and thus the connected device.

Accessing devices via SSH

In order to perform this function you must have a system capable of running an SSH session. The Console Server supports both SSH version 1 and SSH version 2. You may wish to use a SSH client software such as :
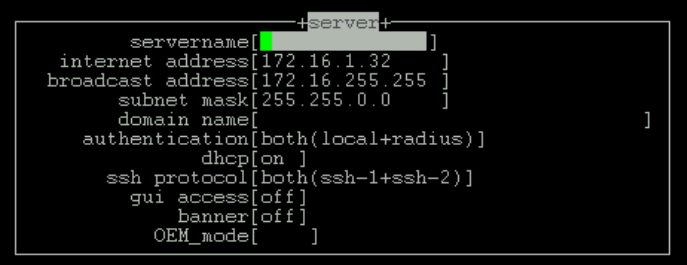
PuTTY - PuTTY is a free implementation of Telnet and SSH for Win32 platforms available from the web.

SSH Setup Procedure

To connect to a specific device using SSH you must configure the Console Server to support the SSH protocol. By default, the SSH protocol is disabled.

To configure the Console Server for SSH perform the following steps:

1. Through console/admin port or by telnet access across the LAN, access the server configuration through CLI commands or through the menu configuration screens.

```
                           +server+
            servername[               ]
     internet address[172.16.1.32     ]
    broadcast address[172.16.255.255  ]
         subnet mask[255.255.0.0      ]
         domain name[                             ]
      authentication[both(local+radius)]
               dhcp[on ]
      ssh protocol[both(ssh-1+ssh-2)]
         gui access[off]
            banner[off]
           OEM_mode[     ]
```

2. Select the appropriate SSH protocol setting.

    SSH1 – SSH version 1 only
    SSH2 – SSH version 2 only
    Both – Both SSH version 1 and SSH version 2 supported
    Disabled – SSH protocol is disabled.

```
                           +server+
             servername[              ]
    internet address[172.16.1.30      ]
   broadcast address[172.16.255.255   ]
        subnet mask[255.255.0.0       ]
        domain name[                             ]
     authentication[both(local+radius)]
               dhcp[on ]
       ssh protocol[ssh-1              ]
         gui access[off]
             banner[off]
           OEM_mode[    ]
```

3. You will be prompted to generated the SSH keys associated with the version of SSH selected. This initial generation of key takes a few minutes and you will be asked to confirm if you want to proceed with the key generation. The SSH key generation is only performed once unless the Console Server is reset back to factory default.

```
                        +server+
            servername[             ]
   internet address[172.16.1.30      ]
  broadcast address[172.16.255.255   ]

  About to generate SSH-1 keys.                  ]
  This will take 5 to 10 minutes - proceed? y/n █

          gui access[off]
              banner[off]
            OEM_mode[    ]
```

4. During key generation, an indicator at the bottom of the screen shows the keys being generated. During the key generation process, any users connected to the box may experience performance delays due to the intense CPU time to generate secure keys for the SSH protocol support.

```
                          +server+
         servername[                   ]
    internet address[172.16.1.30    ]
  broadcast address[172.16.255.255 ]

    About to generate SSH-1 keys.                    ]
    This will take 5 to 10 minutes - proceed? y/n
    . . . + + + + + + .  █

            gui access[off]
                banner[off]
              OEM_mode[     ]
```

5. Once the keys have been generated, you will be prompted to save your settings.

6. Each line which you require secure access to will have to be configured for
    reverse ssh. Go to the appropriate line configuration setting to set the line service
    to **rev ssh**
    NOTE: the line will only support the SSH protocol which was selected in the
    server configuration.

```
                          +line 1+
        service[rev ssh]           line name[                    ]

         speed[9600  ]             terminal[dumb  ]
          flow[none]
          bits[8]                     user[                ]
        parity[none]             hostname[tftp          ]
          stop[1]                host port[23   ]
                                    CS port[10001]

          dial[none ]          modem name none
  phone number[                                 ]

    idle timer[          ]  session timer[          ]
```

7. Save your line configuration settings and SSH protocol is now supported.

Required Information

To connect to a specific device you must know the following information:

•   Ip address of Console Server device is connected to

•   Port on Console Server device is connected to

•   TCP socket number of port (by default port 1 will be 10001, port 2 10002, etc)

- SSH protocol enabled and associated key generated on the Console Server

- Disable decompression on SSH client software – feature is not supported on Console Server

Access procedure

To access a device over a secure SSH session, proceed as follows:

1. Set up your SSH client software to connect to the ip address of the Console Server and set socket number for the correct port.

2. Setup your SSH client software to match the SSH protocol version that is configured on the Console Server unit.

3. A Console Server login prompt will appear and you can enter your user name. **NOTE:** In order to provide a secure SSH connection across the LAN the Console Server login prompt can be delayed by a few seconds as the secure line is being negotiated.

4. A password prompt will appear and you can enter your password.

You will now be connected to the port over a secure SSH LAN connection.

Accessing devices via modems using PPP

For this method you will need to setup one of the serial ports for PPP (see Configuring a dial in line on page 74 in Chapter 3 System administration).

With a line configured for PPP you will be able to dial in for a PC using Microsoft's dial up networking.

A remote user will dial up by using dial up networking and once authenticated by the Console Server will be connected to the network. At this point a telnet session can be initiated as in the Accessing devices via Telnet from the LAN on page 117.
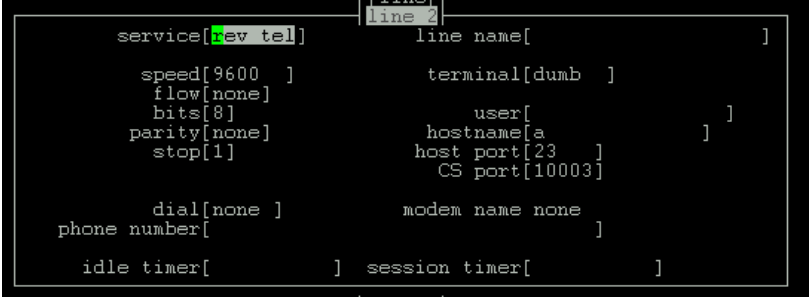
Note   *Even in the event of a main network failure a user will still be able to connect to the*
              Console Server and access a port.

Accessing devices via modems using a dumb device

For this method you will be using either a PC with a terminal emulator or a dumb terminal.

To setup a serial port for this method proceed as follows:

1. Login in to Console Server as admin.

2. At Console Server prompt type **screen** and press **enter**.
The Main menu now appears.

3. From the Main menu, select **Line settings**.

4. Select the line number you wish to configure.

```
                          ┌─line 2─┐
        service[rev tel]        line name[                    ]

        speed[9600  ]            terminal[dumb  ]
        flow[none]
        bits[8]                      user[                 ]
      parity[none]               hostname[a             ]
        stop[1]                 host port[23   ]
                                  CS port[10003]

        dial[none ]            modem name none
phone number[                                 ]

     idle timer[          ]  session timer[         ]
```

5. Set the service to **cslogin.**

6. Check speed, flow, bits, parity and stop are the same as your modem settings.

7. Press **enter** and select **Save settings**.

8. Exit menus and save settings to flash memory.

9. Connect modem to the serial port on your Console Server.

10. Dial into your Console Server unit via modems.
You are now presented with a login prompt

11. At the login prompt enter your Console Server user name and press enter,
A password prompt is now displayed

12. At the prompt enter the password and press enter.
A Console Server prompt is now displayed.

13. At this prompt telnet to the appropriate port
    For example Telnet 'ipaddress' 'socket #'

Appendix A Cabling information

You need to read this appendix if you want cabling information for the Console Server.

This appendix provides connector pinout and cabling information for the Console Server console server.

This appendix includes the following sections;

RJ45 RS232 serial ports

The RS232 RJ45 serial ports are 8-pin shielded and surge-suppressed to 15KV. Note that DCD is an input.

The pinouts are shown in *shielded RJ45 pinouts RJ45 pinouts (serial ports) on page 126*.

shielded RJ45 pinouts RJ45 pinouts (serial ports)

Pin	Circuit	Direction	Function
1	DCD	Input	Data Carrier Detect
2	DSR	Output	Data Set Ready
3	DTR	Input	Data Terminal Ready
4	S/GND	—	Signal Ground
5	TXD	Output	Transmit Data
6	RXD	Input	Receive Data
7	CTS	Output	Clear To Send
8	RTS	Input	Request To Send
Shield	P/GND	—	Protective (Chassis) Ground

Notes:

1. P/GND means Protective (Chassis) Ground

2. S/GND means Signal Ground

Pin locations RJ45 connectors

The pins in all the RJ45 connectors (front and rear panels) are located at the bottom, with pin 1 on the right;

*Pin
numbering in
the RJ45
connectors*

Left | | | | | | | | Right
              8 7 6 5 4 3 2 1
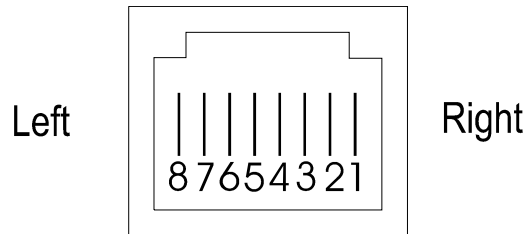
AUI port

The port labelled AUI, on the rear panel, is a 15-way female D-type. Pin-outs are:

Note   *To use the AUI port on Console Server units equipped with Revision 2 boards you need to select the AUI interface during initial configuration using CLI commands. See* Selecting AUI or 10/100 Base T interface on page 32.

Pin	Signal	Pin	Signal
1	Ground/chassis link	9	Collision-
2	Collision+	10	Data Out-
3	Data Out+	11	Ground
4	Ground	12	Data In-
5	Data In+	13	+12 volt
6	Ground	14	Ground
7	do not connect	15	do not connect
8	Ground		

RJ45 10/100BaseT port

The RJ45 port on the *rear* panel, labelled '10/100BaseT' is 8-pin shielded RJ45. It is wired as shown in on page 129the next table. The positions of the pins inside the connector are shown in . The pinouts are shown below .

Pin	Signal	Function
1	TXD+	Transmit Data+
2	TXD-	Transmit Data-
3	RXD+	Receive Data+
4	-	do not connect
5	-	do not connect
6	RXD-	Receive Data-
7	-	do not connect
8	-	do not connect

Admin Port

The port labelled 'Admin' is on the rear of the unit. When fitted with a 25-pin female D-type connector the wiring is as follows:

Pin	Signal	Function
2	RXD	Receive
3	TXD	Transmit
7	S/GND	Signal Ground
all others	-	(do not connect)

If you wish to connect a terminal into the Admin Port, see the connection example in Terminals on page 138.

Direct (1:1) Connections

This section describes direct (1:1) connections (definition below) and shows you connection examples. **Definition of a Direct (1:1) connection:**

> a single length of cable joins the Black Box device and your equipment; there is *no* structured cabling system or any other connection in-between.

Notes:

1. Some user equipment need additional signals on the connector. These may not be supported by the Black Box device or your cable. The normal way to overcome this is to loopback - on your equipment - one of the output lines to the required input. Refer to the documentation supplied with your equipment, or the supplier of the equipment, for information on which loop-backs, if any, are required.

2. Other than a specific requirement at your equipment (as in note 1), do not connect unused pins on either connector.

3. Protective Ground (P/GND) terminates on the connector and so does not have a pin number.

Example direct connections

In this section we show example connections between Black Box ports and the following devices:

- Sun Microsystem servers on page 132
- CISCO RJ45 console ports with software flow control on page 134
- Black Box 833AS on page 134
- Black Box Series router console port on page 134.

Sun Microsystem servers

For connecting a port on the front of the Console Server to the console port on a Sun server with software flow control;

```
Console Server                          Sun server
Port                                    DB25

        4       GND             7       GND
        5       TX              3       RX
        6       RX              2       TX
```

For connecting a port on the front of the Console Server to the DB25 console port on a Sun server with hardware flow control;

```
Console Server                          Sun server
Port                                    DB25

        1       DCD             20      DTR
        2       DSR             6&8     DSR&DCD
        3       DTR             20      DTR
        4       GND             7       GND
        5       TXD             3       RXD
        6       RXD             2       TXD
        7       CTS             5       CTS
        8       RTS             4       RTS
```

For connecting a port on the front of the Console Server to the DB9 console port on a Sun server;

```
Console Server                          Sun server
Port                                    DB9

        1       DCD             4       DTR
        2       DSR             1&6     DCD&DSR
        3       DTR             4       DTR
        4       S/GND           5       S/GND
        5       TXD             2       RXD
        6       RXD             3       TXD
        7       CTS             8       CTS
        8       RTS             7       RTS
```

For connecting a port on the front of the Console Server to Sun Netra t1 and other Sun systems with RJ45 console ports.

```
Console Server                        Sun server
Port                                  RJ45

        1     DCD            2    DTR
        2     DSR            7    DSR
        3     DTR            2    DTR
        4     S/GND          4    GND
        5     TXD            6    RXD
        6     RXD            3    TXD
        7     CTS            8    CTS
        8     RTS            1    RTS
```

CISCO RJ45 console ports with software flow control

```
Console Server                          CISC0


        TX      5    —————————>  6   RX
        RX      6    <—————————  3   TX
        GND     4    <—————————  4   GND
```

Black Box 833AS

```
Console Server                          833AS
                                        DB9

        TX      5    —————————>  2   RX
        RX      6    <—————————  3   TX
        GND     4    —————————   5   GND
```

Black Box Series router console port

```
Console Server                          Router
                                        DB25

        TX      5    —————————>  2   RX
        RX      6    <—————————  3   TX
        GND     4    —————————   7   GND
```

IBM RS6000

```
Console Server                          RS6000
                                        DB25
        DSR    2   <————————  1  DCD
        S/GND  4                5  S/GND
        TX     5   ————————>  2  RX
        RX     6   <————————  3  TX
```

PC serial port

PC, example connections,

with a Black Box RS232 RJ45 connector and a direct (1:1) connection to the PC (connection not through a structured cabling system), and using hardware flow control:

```
Black Box RS232                         PC
RJ45                                    DB9

        DSR    2   <————————  4   DTR
        DTR    3   ————————>  6   DSR
        S/GND  4              5   S/GND
        TXD    5   ————————>  2   RXD
        RXD    6   <————————  3   TXD
        CTS    7   <————————  7   RTS
        RTS    8   ————————>  8   CTS
```

1. If your PC is fitted with a DB25 connector, use the same DB25 pinouts as for modems, shown in *Section Modems*

2. We assume you are connecting your PC directly to the Black Box device (no structured cabling system).

3. In addition to the signals shown in the examples above, you may connect Protective Ground (P/GND) if you have shielded twisted-pair (STP) cable. Connect P/GND at *either* your equipment *or* the Black Box device (but not both). P/GND will reduce interference in noisy environments.

4. The application of the connection example is a PC running terminal emulation software set to 'hardware flow control'.

Connection from the 25-pin Admin Port to a PC

```
Black Box 25-pin Admin Port             PC
DB25                                    DB9

        TXD       3   ————————>  2     RXD
```

```
RXD        2      <───────   3      TXD
GND        7      ────────   5      GND
```

Terminals

Terminals (slow speed or using software flow control)

For a standard terminal operating at slow speeds, or using software flow control, a simple 3-pin connection can be used:

```
Black Box RS232                    Terminal
RJ45                               DB25

        RXD    6   <————————  2   TXD
        TXD    5   ———————-->  3   RXD
        S/GND  4   ————————-  7   S/GND
```

Notes:

1. In addition to the signals shown in the examples above, you may connect
    Protective Ground (P/GND) if you have shielded twisted-pair (STP) cable.
    Connect P/GND at *either* your equipment *or* the Black Box device (but not both).
    P/GND will reduce interference in noisy environments.

Connection from the 25-pin Admin Port to a Terminal

```
Black Box 25-pin Admin Port                    Terminal
DB25                                           DB25


        TXD     3     ————————>   3     RXD
        RXD     2     <————————   2     TXD
        GND     7     ————————    7     GND
```

For a terminal operating at speeds faster than 9600 baud, or for a terminal which cannot use xon/xoff flow control, the following connections are required:

```
Black Box device                               Terminal
RS232 RJ45                                      DB25


        RXD     6     <————————   2     TXD
        TXD     5     ————————->  3     RXD
        RTS     8     <————————   4 or  RTS or
                                  20    DTR
        *CTS    7     ————————->  5     *CTS
        S/GND   4     ————————-   7     S/GND
```

Notes:

1. In addition to the signals shown in the examples above, you may connect Protective Ground (P/GND) if you have shielded twisted-pair (STP) cable. Connect P/GND at *either* your equipment *or* the Black Box device (but not both). P/GND will reduce interference in noisy environments.

2. * asterisk denotes that you connect CTS to CTS only if input flow control (from the Terminal to the Black Box device) is required.

Modems

Direct connections

Modems; example connections,

```
Black Box device                    Modem
RS232 RJ45                          DB25

        RXD    6    <————————   3   RXD
        TXD    5    ——————--—>  2   TXD
        RTS    8    <————————   5   CTS
        CTS    7    ——————--—>  4   RTS
        DSR    2    ——————--—>  20  DTR
        S/GND  4    ————————-   7   S/GND
        DCD    1    <————————   8   DCD
        DTR    3    <————————   6   DSR
```

Notes:

1. At the modem, signal RXD is received data from the PSTN; signal TXD is transmitted data to the PSTN.

2. In addition to the signals shown in the examples above, you may connect Protective Ground (P/GND) if you have shielded twisted-pair (STP) cable. Connect P/GND at *either* your equipment *or* the Black Box device (but not both). P/GND will reduce interference in noisy environments.

Appendix B The CLI commands

You need to read this appendix if you want to... You need to read this appendix if you want information on the Console Server Command Line Interface (CLI).

This appendix provides descriptions of each Command Line Interface (CLI) command.

This appendix includes the following sections;

CLI commands

add community

user level:
admin

This command enables you to define up to four SNMP communities.

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 | defines the access permission for the community.
readwrite

See also

add trap, *delete community*, *set contact*, *set location*, *show snmp*

add DNS

user level:
admin

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 DNS configuration on page 56.

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:

name   is the name of your modem, e.g. usrobotics28.8, or a name you wish to use, e.g. modem4. Do not enter spaces in the name; use the underscore _ character; e.g. us_robotics_28.8

init_string   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:
admin

Use this command to add RADIUS authentication and accounting hosts to the unit.

Syntax

```
add radius host type   host name secret
```

Where:

host type   is either `authentication_host` or `accounting_host`

hostname   is the name of the RADIUS host

secret   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* add host on page 144. *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 comunities 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

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:
admin
This command enables you to delete SNMP communities defined using the `add community` command.

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:
admin   This command enables you to delete the DNS (Domain Name Service) host or hosts in your network.

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   Network Configuration - DNS - delete DNS
equivalent
See also   *add DNS*, *delete WINS*, *show server*

delete gateway

user level:
admin   This command enables you to delete a gateway. The host will not be deleted from the host table.

Syntax   `delete gateway hostname`

Menu   Network Configuration - Gateways
equivalent
See also   *add gateway*, *set gateway*, *show gateways*

delete host

user level:
admin   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.

Syntax   `delete host hostname`

Menu equivalent	Network Configuration - Host Table
See also	*add host*, *set host*

delete modem

user level: admin	Use this command to delete modem details from the unit.
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: admin	Use this command to delete RADIUS authentication and accounting hosts from the unit.
Syntax	`delete radius host type    host name`
	Where:
	host type is either `authentication_host` or `accounting_host`
	hostname is the name of the RADIUS host
Menu equivalent	radius configuration - radius settings
See also:	*add radius*, *show radius*

delete trap

user level:
admin
This command enables you to delete SNMP trap communities defined using the add
trap command.

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:
admin
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.

Syntax delete user *username*

Menu Users - *delete user*
equivalent

See also *add user*, *set user*, *show user*

delete WINS

user level:
admin
This command enables you to delete the WINS (Windows Internet Naming Service)
host or hosts in your network.

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 Network Configuration - WINS - delete WINS
equivalent

See also *add WINS*, *delete DNS*, *show server*

heap

user level: This command tells you how much free memory currently exists and the largest
admin   available fragment.

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: This command can be used to kill the processes on a *serial* line.
admin

Syntax   kill line *n*

Where *n* is the line that you want to kill.

Menu   Line Configuration - Kill Line
equivalent

See also   *reset line*, *restart*

logout

user levels: This command logs you off the unit. You won't be allowed to log out if you still have
all users   sessions running.

Syntax   logout

Menu   Sessions - Logout
equivalent

See also   *kill line*

netload

user level: This command allows you to download a file over a network from a host using TFTP.
admin   The file can be one of several types; e.g. a configuration file of another unit. The list of file types is shown below.

Syntax   `netload [nowrite] filetype hostname filename`

where you replace the word 'filetype' with one of the following words:

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/xxxx/config/... The path/filename must start with the 'forward slash' / character; do *not* 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 *without* 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:

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	

software   when you reboot the unit. See

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

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/xxxx/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:

hostname/ inetaddress	is the hostname or internet address of the machine that you want to ping.
packet_size	is the size of packet sent (default = 100 bytes).

packets_sent   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, Appendix F BOOTP.

Rebooting does not reset the unit to factory default settings.

Syntax   `reboot`

Menu   Network Configuration - Reboot
equivalent

See also   *show server*

reset factory

user level:
admin

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.

Syntax   `reset factory`

Menu   Network Configuration - Reset
equivalent

See also   *reboot*

reset line

user level:
admin

This command will reset the specified serial line(s) to the default line configuration.

Syntax   `reset line ./n/*`

Where:

.   specifies the current line.

n   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 user

user level: admin	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.
Syntax	`reset user ./*/username`

Where:

.	specifies the current user.
username	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*

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   *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 [termtype termtype]
[user username]
```

Where:

hostname/ inetaddress	is the hostname or internet address of the machine you want to log into.
termtype	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 termtype in accordance with its UNIX TERM variable.
username	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   *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

user level: This command will change you from Command Line mode to Full Screen mode (on
admin 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-
admin time clock. For more information on the real-time clock see Console Server, Setting
date and time on page 64.
Syntax   `set date dd/mm/yyyy`

for example; set date 05/12/2000
Menu Main Menu - hardware
equivalent
See also   *set time*

set ethernet interface RJ45

user level:
admin
This command enables you to select the RJ45 10/100Base-T interface.

Syntax

```
set ethernet interface RJ45
```

See also

set ethernet interface AUI, *show hardware*

set ethernet interface AUI

user level:
admin
This command enables you to select the AUI interface.

Syntax

```
set ethernet interface AUI
```

See also

set ethernet interface RJ45, *show hardware*

set gateway

user level:
admin
This command enables you to redefine a gateway.

Syntax
```
set gateway hostname type [inetaddress] [status]
```

Where:

hostname	is the name of the gateway.
type	is one of 'default', 'host' or 'network'.

inetaddress   is the internet address of the target host or network.

status   is one of: 'active' or 'passive'.

Menu equivalent	Network Configuration - Gateway - Change Gateway
See also	*add gateway*, *delete gateway*, *show gateways*

set host

user level: admin   Use this command if you need to change the internet address of one of the hosts in your host table.

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.

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]
[termtype term-type]
[dial dial-status]
[user user-name]
[nouser]
[service line_service]....followed by (optionally)
 [raw/telnet/ssh][raw/telnet]
[hostname][cs_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]
[line_name line_name]
```

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 'cslogin' 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 termtype value using the command telnet.
dial-status	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.
user-name	(for cslogin 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.
nouser	(for cslogin line service) nullifies the user argument; it enables any user to log in on this line.

line-service	select from one of: cslogin, direct, silent, reverse, bidir, slip or ppp.
	for remote access connections, see Setting up the line on your Console Server on page 70,
	when you select 'direct', 'silent' or 'reverse', you must specify whether the line service is 'raw','telnet'or 'ssh'; e.g. silent telnet.
	when you select 'direct', 'silent' or 'bidir', you must enter the target host name; e.g. sophocles.
	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.
	when you select 'reverse raw' 'reverse ssh'or 'bidir', you must specify the TCP port assigned to the unit's port (that is the Console Server TCP port number). TCP/IP hosts will use this TCP port to establish a connection with the unit.
phone-number	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.
modem-name	is the name of the attached modem; e.g. usrobotics28.8, or a name you wish to use, e.g. modem 1. Do not enter spaces in the name; use the underscore _ character; e.g. us_robotics_28.8. You can enter a total of nineteen alphanumeric characters (including spaces).
i-timer value	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).
	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.
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**. This parameter is only available from the CLI.
line_name	Name to help identify the line. Do not enter spaces.

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 location

user level: admin	This command enables you to configure the SNMP sysLocation object.
Syntax	`set location location`
See also	*set contact*, *show snmp*

set ppp line

user level:
admin

Use this command to configure PPP on a line.

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
auth_tmout	authentication timeout

The meanings and values of these parameters are explained in Introduction to SLIP and PPP connections on page 74.

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:
admin

Use this command to set RADIUS settings of the unit:

Syntax

```
set radius <parameter>
```

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]
[dhcp dhcp-status]
[ssh-protocol ssh-protocol-status]
[gui_access gui-status]
[banner banner-status]
[OEM-mode mode-flags]
[services XXXX]
[break on-off]
[sshbreakstring string]


Where:
```

server-name	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 `reboot`.
inet-address	set or change the internet address of the unit. After this action, you must reboot the unit afterwards; use the command 'reboot'.
subnet	set or change the subnet mask of your network. For information on the subnet mask parameter, see General installation procedure on page 24.
broadcast	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 `reboot`.

domain	set or change your domain name. After this action, you must reboot the unit; use the command `reboot`.
user-iphost	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.
auth-method	set the authentication method for users, when they login to the unit; the method is 'local', 'both' or 'radius'.
retry-value	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.
timeout-value	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.
security-status	By enabling security, the CS9000 will restrict incoming connections to the source IP addresses that are configured host table. Regardless of the type of access (SNMP, reverse telnet, SSH, etc), all frames from any IP host NOT configured in the host table will be filtered/dropped if security is enabled. By not responding to unauthorised IP hosts (even pings), it prevents common IP/port mapping utilities from discovering the server's IP address and listening port information.
dhcp-status	By enabling dhcp, the Console Server allows a dhcp server to provide the configuration for the Console Server. The values are 'on' or 'off'; the default is 'off' (dhcp disabled).
ssh-protocol-status	By enabling the ssh protocol, you allow secure ssh connections to be established across the LAN to a port device. The values that ssh-protocol-status can be set to are "disabled", "ssh-1", "ssh-2" and "both (ssh-1+ssh-2)".
	By default, the ssh protocol is set to "disabled". By setting the ssh protocol to "ssh-1", ssh client connecting using SSH version 1 protocol will be allowed access. Encryption keys will only be generated for SSH version 1 which you will be prompted to generated. Similarly, encryption keys will only be generated for SSH version 2, when set to "ssh-2" and only ssh clients that connect using SSH version 2 protocol will be allowed access. Both sets of keys will be generated when setting ssh-protocol-status to "both (ssh-1+ssh-2)" and will support both SSH version 1 and 2 protocols.
	NOTE: generation of keys can takes several minutes depending upon the SSH version chosen. Key generation is only required once unless the Console Server is reset back to a factory default state.

gui-status   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.

banner-status   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   The OEM_mode field is a 4 digit hexadecimal number. The number is defined as a bit field, each bit being a different option that is either enabled or disabled.

The following options are currently used :-

Bit   Value   Option

0   1   Login prompt uses OEM1 string

When set, and a custom language file is in use, the login prompt will use the string defined in the language file as the login prompt instead of the 'login: ' default prompt.
Note that this option applies to ealier versions of the software only.

1   2   Bypass Password

When set, authorised users who do not have a password set, with the exception of the admin account, WILL NOT be prompted for a password at login.

2   4   Disable Routed

When set, the routed process will not be started at boot time. Instead, a static route will be created using the first entry found in the gateways table that is set to type default.

3   8   Telnetp Single Connection

Sets all reverse connections (raw and telnet) to a one connection at a time mode. Server side applications will get a (socket) connection refused until :

- All data from precious connections on that serial port have drained;

- There are no other connections;

- A (upto) 1 second interconnection poll timer has expired.

OEMmode 8 also enables a per-connection keepalive TCP keepalive feature - after approx 3 minutes of network connection idle time, the connection will send a gratuitous ACK to the network peer – thus either ensuring the connection stays active OR causing a dropped connection condition to be recognised by the reverse raw service.

Without OEM mode 8 set the software continues to work as before.

Applications using OEM mode 8 need to be aware that there may be some considerable delay between a network disconnection and the port being available for the next connection attempt - this is to allow any data sent on prior connections to be transmitted out of the serial port. Application network retry logic needs to accommodate this feature.

Bit	Value	Option
4	10	**Send Break Option**

When set a port will allow the sending of a break signal through to attached device. This can be used in the Sun Server environment when the administrator needs to take the Sun Server to the OBP mode (Open Boot Prompt)

The number entered into the OEM_mode field should be the sum of the required options values.

ie. to just disable the routed process, enter 4, or to use the customised login prompt, and not prompt for password if a password has not been set, enter 3 (1+2)

services

This command allows the ability to enable/disable specific processes in the Console Server.The services field is a 4 digit hexidecimal number. The number is defined as a bit field, each bit being a different process that is either enabled or disabled. By default, all processes are enabled with the flag set FFFF). This service flag will be saved when configuration is saved to FLASH.

The following options can be used:

Bit	Value	Option
0	0001	DHCP Process

The DHCP process will be enabled when service flag is set to 0001. Although DHCP is also controlled by the command 'set server DHCP <status>', this flag will be updated accordingly and vice versa.

Bit	Value	Option
1	0002	ROUTE Process

The ROUTE process will be enabled on well-know port 520 when service flag is set to 0002. ROUTE process can also be enabled/disabled by OEM_mode bit.

Bit	Value	Option
2	0004	Telnet Process

The Telnet process will be enabled on well-known port 23 when the services flag is set to 0004.

Bit	Value	Option
3	0008	SSH Process

The SSH process will be enabled on well-known port 22 when the services flag is set to 0008.

Bit	Value	Option
4	0010	HTML Process

The HTML process will be enabled on well-known port 80 when the services flag is set to 0010. Note that disabling the server's services flag for HTML process is different than GUI_ACCESS configuration in such that there will be no response from the server when the HTML process is disabled.

5	0020	SNMP Process

The SNMP process will be enabled on well-known port 161 when the services flag is set to 0020.

6	0040	SPCD Process

The proprietary SPCD (Trueport) process will be enabled on port 668 when the services flag is set to 0040.

break

The break option can be set to either on or off. This option will enable/disable proprietary inband SSH break signal processing as well as the existing Reverse Telnet break signal. The OEM_mode flag 0010 will be set/reset based upon this command. This configuration parameter will be saved when the configuration is saved to FLASH.

sshbreakstring

The sshbreakstring can be set up to 8 characters which defines the break string used for inband SSH break signal processing. The default is set to '~break', where ~ is tilde. A break signal in generated on a specific serial port only when the server's break option is enabled and the user currently connected using reverse SSH has typed the break string exactly.

Any combination of the arguments can be used. Examples:

```
set server name stimpy
set server name stimpy 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:
admin

Use this command to configure SLIP on a line.

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 Introduction to SLIP and PPP connections on page 74.

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:
admin
Use this command to set telnet parameters on a line. It is available for line service types of:

> *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]
[termtype terminal-type]
[echo  value]
[mapnl value]
[mode  value]
[intr  value]
[quit  value]
[eof   value]
[erase value]
[break value]
```

Where:

line_number	is the serial line number connected; for example 3
terminal type	is your terminal type; for example wyse60. Note this value will be ignored if you have set a termtype value using the command `telnet`.
echo	on or off
mapnl	on or off
mode	on or off
intr	<hexadecimal>
quit	<hexadecimal>
eof	<hexadecimal>
erase	<hexadecimal>
break	<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:
admin   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 Console Server, Setting date and time on page 64.

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:
admin,
normal   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.

Syntax   `set user username/.`

```
[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:

password	if you include this argument you will prompted to enter a new password.
user-level	is 'admin', 'normal', 'restricted' or 'menuing'.
switch-character	is the hex value of the 'hot-key' used for switching sessions. The default is 1 (^a).
user-service	select one of: csprompt, telnet, rlogin, tcp_clear, slip or ppp. For more information on these user services see Appendix E Summary of Line Service Types.
iphost-address	(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 set server on page 173.
	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
t-port number	(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.
callback-flag	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).
phone-number	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-timer value	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.

s-timer 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 2^{32} seconds.
	The session timer (here) will override the session timer which you can configure for a line.
f-ip address	use only when the user service field is set to 'slip' or 'ppp';
f-netmask	ignore this parameter; it is reserved for future use.
f-mtu value	use only when the user service field is set to 'slip' or 'ppp';
f-compression value	use only when the user service field is set to 'slip' or 'ppp';
session	use this argument to predefine sessions for the user. You can predefine one specified session (*n*), or all sessions (*). It takes the arguments defined below:
Session arguments	```... session n/* type telnet/rlogin host hostname [termtype termtype] [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	You can set all users to the same parameters by using the * asterisk character, e.g.
	```set user * level normal```
	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   Main Menu - hardware
equivalent

See also   *set date*, *set time*, *show time*, *show hardware*

show gateways

user levels:
admin,
normal

Use this command to list the gateways you have defined. The list will be displayed in the following format:

```
CS_9000# show gateways
hostname          service   internet address  status
socrates          host      192.101.34.184    passive
homer             default                     active
CS_9000#
```

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   Network Configuration - Gateways - Change Gateway
equivalent

See also   *add gateway*, *delete gateway*, *set gateway*

show hardware

user level:
admin,
normal

This command displays the hardware configuration of your unit. An example display is:

```
CS_9000# show hardware
mac address           0080ba0000d4
ethernet i/f          RJ45 10/100Base-T
board id              CS4300076R2.1
processor             80386
uarts                 2 * Serial ASIC
flash rom             1 x 1MB
ram                   2 x 2MB
battery ram           32kB
serial ports          16
date                  13/12/2001
time                  15:03:44
CS_9000#
```

Syntax   show hardware

Menu   Main Menu - Hardware
equivalent

See also   *set date*, *set time*, *show line*

show hosts

user levels:
admin,
normal

Use this command to list the contents of the host table:

```
CS_9000# show hosts
hostname          internet address
socrates          192.49.144.4
aristotle         192.50.123.76
plato             192.78.26.21
sophocles         192.111.89.2
homer             192.111.64.3
pythagoras        192.168.0.254
CS_9000#
```

Syntax   show hosts
Menu   Network Configuration - Host Table - Change Host
equivalent
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: admin, normal 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.

For a single line the display will look similar to this:

```
JS_8500# show line 2
line name              line_name_2
speed                  9600
terminal               dumb
dial                   none
flow                   none
bits                   8
parity                 N
stop                   1
phone number
modem name             none
idle timer             0
session timer          0
routing                none
service                rev raw
CS port                10002
security               on
JS_8500#
```

If you specify all lines, the display will look similar to this:

```
login: admin
Password:
login: admin
Password:
CS_9000# show line *
line  line name          speed   service
1     sshline1           9600    rev ssh  -/10001            nouser
2                        9600    rev ssh  -/10002            nouser
3                        9600    rev ssh  -/10003            nouser
4                        9600    rev tel  -/9004  security=on admin
5                        9600    rev tel  -/10005 security=on nouser
6                        9600    rev ssh  -/10006            nouser
7                        9600    rev tel  -/10007 security=on nouser
8                        9600    rev raw  -/10008 security=on admin
9                        9600    rev tel  -/10009 security=off in use
10                       9600    bidir       nouser
11                       9600    rev tel  -/10011 security=on nouser
12                       9600    rev tel  -/10012 security=on nouser
13                       9600    rev tel  -/10013 security=on nouser
14                       9600    rev tel  -/10014 security=on nouser
15                       9600    rev tel  -/10015 security=on nouser
16                       9600    rev tel  -/10016 security=on nouser
CS_9000# 
```

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.'In use' means the line is in use but line security is off so no the user can be identified

The security status for an individual line can be determined from the show line display. "Security=on" indicates that security is enabled for the particular line and "Security=off" indicates security is disabled for the line.

Syntax   `show line line_number`

Where line_number is :

.   the current line.

n   a specific line number.

*   all lines

Menu   Line Configuration - Line Settings
equivalent

See also   *set line*, *show user*

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   Line Configuration - Modems - Change Modem
equivalent
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 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.

For example:

```
CS_9000# show ppp line 1
local address            0.0.0.0
remote address           0.0.0.0
subnet mask              0.0.0.0
accm                     00000000
mru                      1500
security                 chap
user
password                 ****************
ruser
rpassword                ****************
ac comp                  on
proto_comp               on
vj_comp                  on
magic_neg                off
ipaddr_neg               off
cr_timeout               3 seconds
tr_tmout                 3 seconds
cr_retry                 10
tr_retry                 2
nak_retry                10
auth_tmout               1 minutes
roaming_callback         off
challenge_interval       0 minutes
CS_9000#
```

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 shown in the next table:

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
auth_tmout	authentication timeout

The meanings and values of these parameters are explained in Introduction to SLIP and PPP connections on page 74.

Menu equivalent Line Configuration - Line Settings

See also set ppp line

show radius

Use this command to check the RADIUS settings of the unit:

Syntax   `show radius`

The output of this command are the RADIUS settings of the unit (e.g.):

```
CS_9000# show radius
primary authentication host        homer
secondary authentication host      plato
primary accounting host            plato
secondary accounting host          homer
retry                              5
timeout                            3
auth_port                          1645
acct_port                          1646
acct_authenticator                 on
accounting                         off
session id                         d0000000
CS_9000#
```

For details of these parameters, see Console Server, RADIUS configuration on page 51.

Menu   radius configuration - radius settings
equivalent

See also   *add radius*, *set radius*, *set server*

show routes

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:

```
CS_9000# show routes

destination      gateway          flags    refs     use      interface
192.168.0.0      192.168.0.101    U        2        3        le0


CS_9000#
```

Syntax   `show routes`
Menu   there is no menu equivalent
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:
admin,
normal

This command displays the base configuration of the unit, for example:

```
login: admin
Password:
CS_9000# show server
servername
internet address        172.16.28.100
subnet mask             255.255.0.0
broadcast address       172.16.255.255
domain name

DNS
 primary                198.235.216.131
tftp retry              5
tftp timeout            3
security                off
authentication          both(local+radius)
services                fffc
                        (SPCD+SNMPD+HTMLD+SSHD+TELNETD)
dhcp                    off
ssh protocol            both(ssh-1+ssh-2)
break                   on
sshbreakstring          sinned
gui access              on
banner                  off
OEM_mode                0014
CS_9000#
```

Fields which are unconfigured will not appear in the list on your screen.

Syntax   show server
Menu   server configuration
equivalent
See also   *set server*, *show hardware*

show slip line

user levels:
admin,
normal

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.

For example:

```
CS_9000# show slip line 1
local address          0.0.0.0
remote address         0.0.0.0
subnet mask            0.0.0.0
mtu                    256
icmp_suppress          off
priority               on
vj_comp                on
transmit_parameters    on
CS_9000#
```

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 Introduction to SLIP and PPP connections on page 74.

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:

```
CS_9000# show snmp
snmp contact          John Smith
snmp location         IT Helpdesk x3423
snmp communities:     1. public        192.168.0.234   readonly
                      2. admin         192.168.0.10    readwrite
snmp traps:           1. local         192.168.0.35
CS_9000#
```

Syntax   show snmp
Menu   network configuration - snmp
equivalent
See also   *add community*, *add trap*, *set contact*, *set location*

show telnet

user levels: admin, normal

Use this command to show telnet parameters on a line. Note that telnet parameters shown here apply only to line service types of:

Direct telnet
Silent telnet

The command also shows telnet parameters entered using the command set telnet.

```
CS_9000# show telnet line 1
echo mapnl mode intr quit eof erase break  terminal
off  off   off  7f   1c   04  08    1d
CS_9000#
```

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: admin, normal

This command enables you to show the time as measured by the real-time clock in the unit; e.g.

    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, admin user can show details of any user, a normal user can only view their own
normal details:

```
JS_8500# show user mark
username                 mark
screen switch            01
level                    normal
service                  csprompt
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
JS_8500#
```

Syntax   `show user ./username`

Where:

.   specifies the current user.

username   is the name of a specific user.

Menu   Admin user: Users - Change User.
equivalent Normal user: Sessions - Set Up User
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 establishes 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 port [termtype termtype] [echo on/off] [mapnl on/off] [mode on/off] [intr <hex>] [quit <hex>] [eof <hex>] [erase <hex>] [break <hex>]`

Where:

hostname/ inetaddress	is the name or internet address of the machine you want to log into
termtype	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 termtype in accordance with its UNIX TERM variable.
	The termtype argument overrides a termtype value entered into the unit when using the `set line` or `set telnet` commands.
echo, mapnl, etc.	these are telnet options. They set values once only, for the duration of a single telnet connection. See comments under telnet on page 201 above.

Menu equivalent	Users - Set Sessions *(to set default values)*
	or
	Sessions - Start telnet *(to use or override default values)*
See also	*resume*, *rlogin*, *set telnet*, *show telnet*, *start*

version

user levels: This command tells you what version of software your unit is running.
admin,
normal

Syntax   `version`

Menu   Version of software is displayed at the top of any menu display, e.g.
equivalent

```
user [admin]    xxxxxx 2.00 i.1              telnet 1
```

The text in the middle of the line (xxxxxx) will display the name of your product.

Appendix C SNMP

You need to read this appendix if you want information on the Console Server support of SNMP.

This appendix describes the Console Server support of SNMP.

This appendix includes the following sections;

Overview

The Simple Network Management Protocol (SNMP) is a protocol for access and control of network management information on TCP/IP networks. Console Server (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 Console Server Private MIB. Summary of objects in the private MIB on page 207 gives a summary of the objects defined by this MIB. The full version of the MIB is in on page 209.

Configuring SNMP support

To configure for SNMP support proceed as follows;

1. From the Main Menu select 'network configuration' and then 'snmp'.

cli syntax: 2. Select 'snmp contact information' to configure the SNMP sysContact and
set contact   sysLocation objects; an example screen is shown below:
set location

```
              ┌network configuration┐
              │reset                │
              │snmp                 │
                      ┌─snmp─┐
                      │ snmp │
    ┌─────────────────┴──────┴──────────────────┐
    │contact          location                  │
    │[john smith   ][IT Helpdesk              ] │
    └────────────────────────────────────────────┘
              │security             │
              │reboot server        │
```
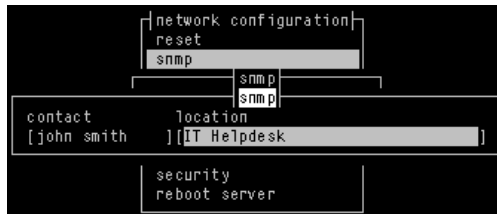
add trap   3. Select 'edit traps' to create up to four trap communities; an example screen is
delete trap   shown below:

```
              ┌network configuration┐
              │reset                │
                    │traps│
    ┌───────────────┴─────┴──────────────────┐
    │trap           internet address         │
    │[pink        ][192.168.0.1      ]        │
    │[turquoise   ][192.168.0.42     ]        │
    │[            ][                 ]        │
    │[            ][                 ]        │
    └─────────────────────────────────────────┘
              │ reboot server       │
```
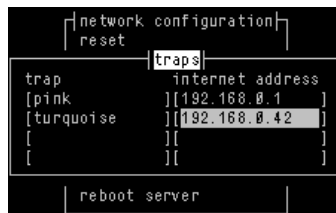
SNMP Trap messages generated by the unit will only be broadcast to hosts defined
by SNMP Trap communities.(note that the unit generates no enterprise specific
traps).

add   4. Select 'edit communities' to create up to four communities; an example screen is
community   shown below:
delete
community

```
          ┌─network configuration─┐
          │ reset                 │
          │ ┌─communities─┐
community │ │internet address   permissions
[public        ][192.168.0.65   ] [none    ]
[              ][               ] [none    ]
[              ][               ] [none    ]
[              ][               ] [none    ]

              │ reboot server    │
```

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

Summary of objects in the private MIB

OBJECT NAME	ADDRESS	TYPE	PERMISSIONS
ServerInfo	1.3.6.1.4.1.667.3.1	Aggregate	not-accessible
freeSpace	1.3.6.1.4.1.667.3.1.1	Guage	read-only
swVersion	1.3.6.1.4.1.667.3.1.2	DisplayString	read-only
serverName	1.3.6.1.4.1.667.3.1.3	DisplayString	read-only
domaiName	1.3.6.1.4.1.667.3.1.4	DisplayString	read-only
portsInfo	1.3.6.1.4.1.667.3.2	Aggregate	not-accessible
portsNumber	1.3.6.1.4.1.667.3.2.1	INTEGER	read-only
portsInfoTable	1.3.6.1.4.1.667.3.2.2	Aggregate	not-accessible
portsInfoEntry	1.3.6.1.4.1.667.3.2.2.1	Aggregate	not-accessible
portId	1.3.6.1.4.1.667.3.2.2.1.1	INTEGER	read-only
terminalType	1.3.6.1.4.1.667.3.2.2.1.2	INTEGER	read-write
baudRate	1.3.6.1.4.1.667.3.2.2.1.3	INTEGER	read-write
dataBits	1.3.6.1.4.1.667.3.2.2.1.4	INTEGER	read-write
parity	1.3.6.1.4.1.667.3.2.2.1.5	INTEGER	read-write
stopBits	1.3.6.1.4.1.667.3.2.2.1.6	INTEGER	read-write
pages	1.3.6.1.4.1.667.3.2.2.1.7	INTEGER	read-write
defaultUser	1.3.6.1.4.1.667.3.2.2.1.8	INTEGER	read-write
validUser	1.3.6.1.4.1.667.3.2.2.1.9	INTEGER	read-write
dial	1.3.6.1.4.1.667.3.2.2.1.10	INTEGER	read-write
flowControl	1.3.6.1.4.1.667.3.2.2.1.11	INTEGER	read-write
service	1.3.6.1.4.1.667.3.2.2.1.12	INTEGER	read-write
hostPort	1.3.6.1.4.1.667.3.2.2.1.13	INTEGER	read-write
localPort	1.3.6.1.4.1.667.3.2.2.1.14	INTEGER	read-write
host	1.3.6.1.4.1.667.3.2.2.1.15	INTEGER	read-write
pinDCD	1.3.6.1.4.1.667.3.2.2.1.16	INTEGER	read-only
pinDTR	1.3.6.1.4.1.667.3.2.2.1.17	INTEGER	read-only
pinRTS	1.3.6.1.4.1.667.3.2.2.1.18	INTEGER	read-only
charSends	1.3.6.1.4.1.667.3.2.2.1.19	Counter	read-write
charReceiveds	1.3.6.1.4.1.667.3.2.2.1.20	Counter	read-write
phoneNumber	1.3.6.1.4.1.667.3.2.2.1.21	DisplayString	read-only
modemName	1.3.6.1.4.1.667.3.2.2.1.22	DisplayString	read-only
idleTimer	1.3.6.1.4.1.667.3.2.2.1.23	INTEGER	read-only
SessionTimer	1.3.6.1.4.1.667.3.2.2.1.24	INTEGER	read-only

OBJECT NAME	ADDRESS	TYPE	PERMISSIONS
lineName	1.3.6.1.4.1.667.3.2.2.1.25	DisplayString	read-only

Private MIB definitions

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
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

OBJECT TYPE	SYNTAX	ACCESS	STATUS	DEFINITION

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

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

OBJECT TYPE	SYNTAX	ACCESS	STATUS	DEFINITION
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 {
	cslogin(1)
	directraw (2)
	silentraw (3)
	directtelnet (4)
	silenttelnet (5)
	reversetelnet (6)
	reverseraw (7)
	bidir (8)
	directlogin (9)
	silentlogin (10)
	slip (11)
	ppp (12)
	reverseshh(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

OBJECT TYPE	SYNTAX	ACCESS	STATUS	DEFINITION
pinDCD	INTEGER { off (1) on (2)}	Read-only	Mandatory	The current status of the port's DCD pin.
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
charReceiveds	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:

Editing the RFC1213 MIB

Editing the MIB

Edit MIB Variables...

Node Name: 192.101.34.217   Repeat Count: 1

MIB Path: alix(667).js8500(2).portsInfo(2).portsInfoTable(2).portsInfoEntry(1).portId(1)

Variable Name:

portId.6

Variable Value: MIB: JS8500-MIB

6

[..]
portId
terminalType
baudRate
dataBits
parity
stopBits
pages
defaultUser
validUser

⊙ Number   ○ IP Addr   ○ ObjID
○ HexArr   ○ String

An index that uniquely identifies the port. Starts from 1 and must
be less than or equal to 24.

Buttons: Next, Get, Set, Repeat..., Stop, Top, Up, Export..., Done, Help

Routing information

192.101.34.217 IpRouteEntry

Edit | Grph | Chrt | List | Hist | Exprt | Cust | Menu | Flip | Help

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

Appendix D Upgrading your firmware

You need to read this appendix if you want to...

You need to read this appendix if you want information on upgrading the Console Server firmware.

This appendix provides task orientated information on upgrading the Console Server firmware.

This appendix includes the following sections;

Introduction

If you have been supplied with a software upgrade this appendix shows you how to install it.

To check the version of software your unit is running see the information displayed at the top of any menu display, that is:

```
user [admin]            xxxxxx 1.0              telnet 1
```

Compare this with the version number of software which you have obtained. If you have a more recent version of software, you should install it.

There are three methods for upgrading the software in the unit:

•   Using the administrative Command Line Interface (CLI) on the unit (see *Using TFTP from a host on page 217*).

•   Using a BOOTP server (see *Using BOOTP from a boothost on page 220*)

•   Using the JETset web configuration tool (see *Upgrade using JETset, the web browser interface on page 221*).

The method you choose will depend on how you operate your unit.

Before you upgrade the software on your Console Server unit we recommend you save the existing configuration information to a network file server.

In all cases the software upgrade process requires that the software has been installed to a readable directory on a network fileserver and that the TFTP service has been enabled. The unit's FLASH firmware can be identified by the file name and type and will always be of the form: **xxxxxv*XXX*.cfg**, where

   xxxxx is the product type, here Console Server, and

   XXX is the firmware version number.

Saving your existing Configuration

Saving the existing configuration will allow the configuration information in the unit to be restored at a later date.

Note   *Upgrading the software on the unit does not alter the stored configuration information which will be preserved during the upgrade.*

The procedure requires the presence of a write enabled empty file on a suitable network fileserver. The fileserver must have the TFTP (Trivial File Transport Protocol) service enabled and running.

Example of saving a configuration file

The following is a example of how to save the configuration of a Console Server on a UNIX fileserver called **BIGSERVER**, the file will be saved to the file **/home/xxxxx/xxxxx.cfg**.

In this example the administrator issues the CLI command:

```
netsave configuration BIGSERVER  /home/xxxxx/xxxxx.cfg
```

Using TFTP from a host

1. Place the new software file on a host machine. Ensure the file has global read/execute permissions for its entire path.

cli syntax: 2. Exit the menus and go into the CLI. Type:
netload
software
```
netload software <hostname> <filename>
```

3. Press <return>. The Console Server will download the new software file using TFTP.

TFTP configuration

cli syntax:
set server tftp

You can configure TFTP in the Console Server (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.

Writing to FLASH memory

The Console Server will load the software into RAM, perform checks, and then write the software into FLASH memory. The writing to FLASH will take a few minutes and during this time the unit will not respond to user input. While the new software is being loaded into FLASH memory, the power and network LEDs on the front of the unit display a pattern.

WARNING   **do not turn the power off/on while the unit is writing to FLASH memory**

*pattern of
Console
Server LEDs
during load
of software
into FLASH*

you will see

**then....
you will see**

**then
repeat
from the
beginning...**

PWR NET

PWR NET

yellow

green

green

yellow
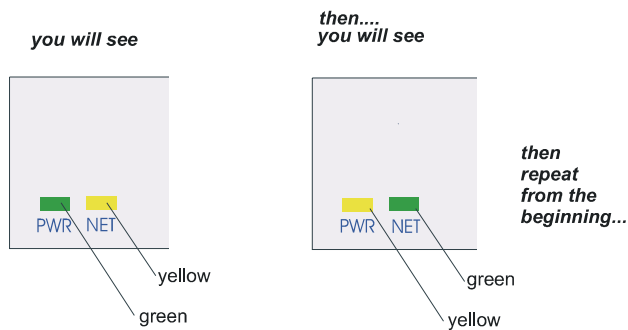
This pattern is repeated approximately once per second.

The Network LED flickers green if network traffic is identified on the network ports.

The pattern on each LED is repeated approximately once per second.

reboot   When the software has finished downloading you must reboot the unit. To do this, type the command:

```
reboot
```

Using BOOTP from a boothost

When installing with BOOTP, the SW_FILE parameter in your BOOTFILE will need to be changed to point to the new software image. We recommend that you keep the name of the image file as supplied as this will guarantee that the software is recognised as a new version by the existing software installation.

Reboot your unit. The new software will download and write to FLASH memory, see Writing to FLASH memory on page 219. You can monitor the progress of this operation with a terminal (or terminal emulation) connected to the Admin port at the rear of the unit.

WARNING **DO NOT SWITCH OFF THE UNIT whilst the unit is programming the FLASH memory.**

You can use BOOTP to compare a software version placed on the boot host and one loaded in the Console Server; if there is a newer version on the host, it will be downloaded to the unit.

For a full description of how to use BOOTP to download a new software file from a host, see Console Server, *Section Appendix F BOOTP*.

Upgrade using JETset, the web browser interface

1. Start JETset by pointing your network browser at the Internet Address of your the unit.

2. Log in as the Admin user and select file transfer from the main menu.

3. Complete the file transfer form by selecting software download from the pull-down menu, and completing the internet address of the TFTP server and the download software image filename.

4. Select save from the main menu to start the download process. Your browser may ask you to confirm this action before the download will start.

The new software will download and written to FLASH memory, see Writing to FLASH memory on page 219. You can monitor the progress of this operation with a terminal (or terminal emulation) connected to the Admin port at the rear of the unit.

WARNING   **DO NOT SWITCH OFF THE UNIT whilst the unit is programming the FLASH memory.**

Enabling BOOTP/DHCP after upgrading software

If you require automatic BOOTP/DHCP configuration, be sure to set the server DHCP parameter to ON:

```
set server dhcp on
```

Save the configuration:

```
Save
```

Disable BOOTP/DHCP

The server parameter DHCP is used to disable BOOTP/DHCP (set server dhcp on/off). Setting DHCP to OFF prevents the unit from initiating a BOOTP/DHCP request. This parameter is only accessible from the CLI.

RARP is unaffected by this parameter.

After any software upgrade you should always check that DHCP is set to ON if you require BOOTP/DHCP to configure your unit.

Appendix E Summary of Line Service Types

You need to read this appendix if you want to... You need to read this appendix if you want a summary of line service types for the Console Server.

This appendix provides a list of line service types for the Console Server.

This appendix includes the following sections;

List of line service types

When you are configuring a line on the Console Server (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
Bidir	Allows a bidirectional modem connection on a port	A UUCP connection for batch file transfer and printing.
Direct telnet *or* **rlogin**	When using the unit as a Serial Server, to bypass the unit and allow users to login straight into a specific host. *These are non-permanent connections*	Users on terminals.
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*). *These connections are established by pressing <return>.*	On dialin connections: user applications for devices such as bar code readers and smart cards.
cslogin	The default connection. The unit presents a login on that line.	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
PPP	a) Remote access connection b) Using the unit as a router (two units back-to-back)	A mobile employee Joining together two networks

Line Service Type	Description/Uses	Example
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).
Reverse Telnet (Default)	Enables a TCP/IP host to establish a login connection on an external machine attached to a port	To access machines like routers, firewalls, servers and so on.
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. *These are permanent connections, therefore consume system resources*	Users on terminals.
Reverse SSH	Enables a SSH secure connection to establish a login connection on an external machine attached to a port.	Secure remote connection to access machines like servers, routers, firewalls etc.
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*). *These connections are established automatically*; they are suitable for computer to computer communications.	Dialin connection from an external host machine.
SLIP	a) Remote access connection b) Using the unit as a router (two units back-to-back)	A mobile employee Joining together two networks

Appendix F BOOTP

You need to read this appendix if you want to...

You need to read this appendix if you require information about BOOTP for the Console Server.

This appendix provides information about BOOTP for the Console Server.

This appendix includes the following sections;

Introduction

You can use BOOTP to perform the following actions on a single or multiple Console Server (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.

How BOOTP works

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 on You can stop the BOOTP server from replying to the unit;

BOOTP request and response

The BOOTP server checks the ethernet address and looks for a matching address in its bootptab 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 bootptab 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.

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.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.*

How to setup BOOTP

Your nominated BOOTP server should be on the same network as 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.

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 bootptab file entry for a single unit on page 231 on page 231. An example for multiple units is shown at bootptab file entry for multiple units on page 238.

bootptab file entry for a single unit

```
xxxxxx_blue:\

:ht=1:\
:ha=0080ba000057:\
:ip=192.101.34.211:\
:ds=192.65.144.44:\
:sm=255.255.255.224:\
:hn:\
:bf=/tmp/xxxxxxp.bfc:\
:dn=xxxx.co.uk:\
: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 (Console Server_blue) to be allocated to this unit.
bf (bootfile name) enter the name of the file containing specific
configuration information; see An example bootfile on page 234.
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 Section Chapter 2 Installation.

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 An example bootfile on page 234.

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

An example bootfile

```
# cat xxxxxxp.bfc

SW_FILE192.65.144.95:/src/pscx/sw/xxxxxx.bin
CONFIG_FILE192.65.144.95:/src/pscx/cfg/jconfig.0183
GUI_ACCESSyes
AUTH_TYPE0
IP_HOST192.101.34.199
SECURITYno
TFTP_RETRY3
TFTP_TMOUT21
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 An example bootfile on page 234; e.g. AUTH_TYPE.

4. An explanation of these parameters is shown in Bootfile parameters on page 235.

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/xxxxx.bin
```

Table 1 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	Appendix D Upgrading your firmware
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 parameters will not overwrite network configuration parameters specified in your bootfile.
GUI_ACCESS	on, off	access to the unit from a web browser	Chapter 2 Installation
AUTH_TYPE	both, local or radius	authentication method employed by the unit for all users	Chapter 2 Installation
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'	
SECURITY	on, off	'reverse' line types, 'printer' line type and remote configuration - all restricted to devices listed in the the unit's host table	

Parameter	Value	Brief Meaning	Fuller explanation
TFTP_RETRY	numeric; e.g. 5	number of tftp attempts before aborting	TFTP configuration on page 218
TFTP_TMOUT	numeric; e.g. 3	period in seconds before retrying a download/upload	TFTP configuration on page 218
EXTRA_TERM1 (or 2, or 3)	a filename and full pathname - all prefixed by a hostname/ip address	termcap files for specific terminal types	

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.

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 Appendix H Troubleshooting 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 bootptab file entry for a single unit on page 231 on page 231, place a hash before all the lines, e.g.

:ht=1:\
:ha=0080ba000057:\

..
:gw=192.101.35.254:\

- in bootptab file entry for multiple units on page 238 you would place a hash before the line referring to each unit; e.g:

```
# xxxxx_2:ht=1:ha=0080ba000025:\
# ip=192.101.34.194:tc=common:
```

Booting multiple units

You can boot mutliple unit's simultaneously using BOOTP; we recommend you alter the format of your bootptab file entry, as shown in bootptab file entry for multiple units on page 238. 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'.

bootptab file entry for multiple units

common is the collective name for the list of information in this file →

```
common:\

        :bf=/usr/js/xxxxxxp.cus:\
        :sm=255.255.255.224:\
        :hn:\
        :dn=xxx.co.uk:\
        :ds=192.101.34.211
```

xxxxxx_1 is the name of the first Console Server →

```
xxxxxx_1:ht=1:ha=0080ba000024:\
        :ip=192.101.34.193:tc=common:
```

xxxxxx_2 is the name of the second Console Server →

```
xxxxxx_2:ht=1:ha0080ba000025:\
        :ip=192.101.24.194:tc=common:
```

ethernet addresses of Console Server

to=common, means: use all the information listed under "common:\"

Notes on the above figure:

1. The example shown is for the Console Server.

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 231

- 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.

*Our example
entry in a
BOOTPTAB
file*

```
xxxxxx_3:\

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

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

*Our example
bootfile*

```
# cat test

SW_FILE192.65.146.71:/xxxxxx.fls
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.

Appendix G JETset

You need to read this appendix if you want information on the Console Server JETset utility.

This appendix provides task orientated information on using the describesConsole Server JETset utility.

This appendix includes the following sections;

- [Introduction to JETset on page 244](#)

- [Using JETset on page 246](#)

- [JETset program summary on page 249](#)

Introduction to JETset

Once you have allocated an ip address, you can use the Graphical User Interface, named 'JETset'. This is a web-based program which you access from the web browser on your networked PC/computer. See *JETsethome page on page 244.* A summary of the program is in JETset program summary on page 249.

JETsethome page

Product logo will display the name of your product

Address   http://192.168.0.101/

Blackbox JETset 2.4.0

The web based configuration utility for **CONSOLESERVER 9000**

Enter the password for the **admin** user then click the login button
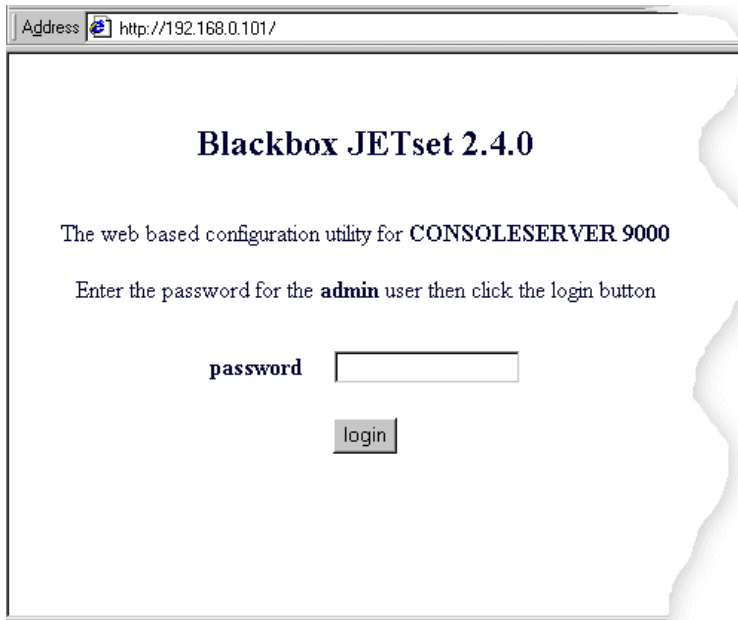
password   [   ]

[login]

1.   Make sure you set 'gui_access' to 'on', see Chapter 2 Installation

2.   Open your web browser and enter the ip address of your Console Server; e.g.

   ```
   http://192.101.34.211
   ```

   You should be presented with the login page:

The program prompts you for a password (for user of name 'admin').

Caution   **the only access permitted is username 'admin'. Console Server assumes this username and so prompts you for the password for this user.**

On successful login you will be presented with the JETset home page (*JETsethome page on page 244* on page 244). From the home page you can now configure your unit.

Using JETset

using JETset

Navigate by selecting these buttons

If you have made changes, remember to save them before moving to another option
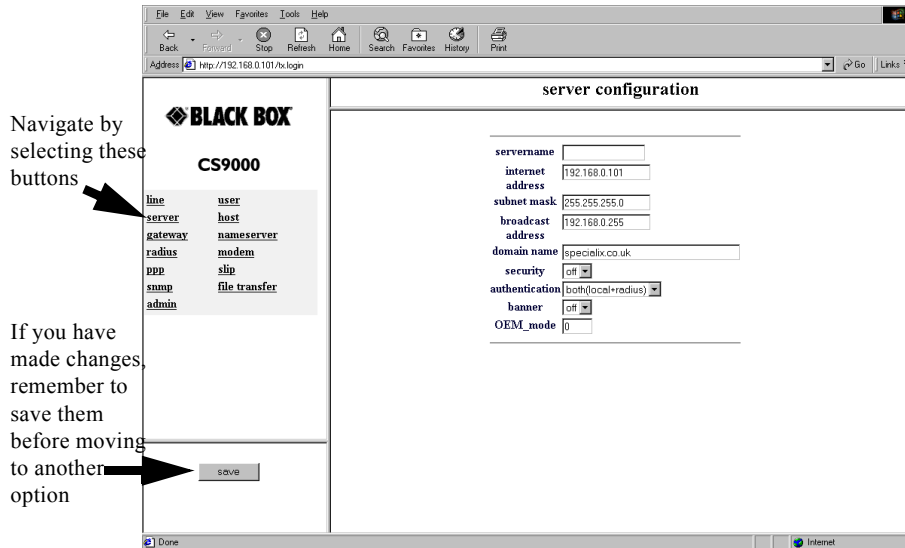
Note the following guidelines about JETset:

- JETset uses the 'Frames' feature of HTML, which allows you to see four different 'windows' simultaneously inside your main browser window. This viewing method will make configuration easier. However, in common with all programs which use Frames there are particular ways of using JETset:

    - navigate using the main JETset buttons (see *using JETset on page 246*); we do not recommend using the 'Forward' or 'Backward' buttons of your Browser

    - set your browser to always check if there is a newer version of the page than the version stored in cache. This action will ensure that JETset will display the most up-to-date information; see *Netscape Navigator - configuration on page 246* and *Internet Explorer - configuration on page 247*.

Netscape Navigator - configuration
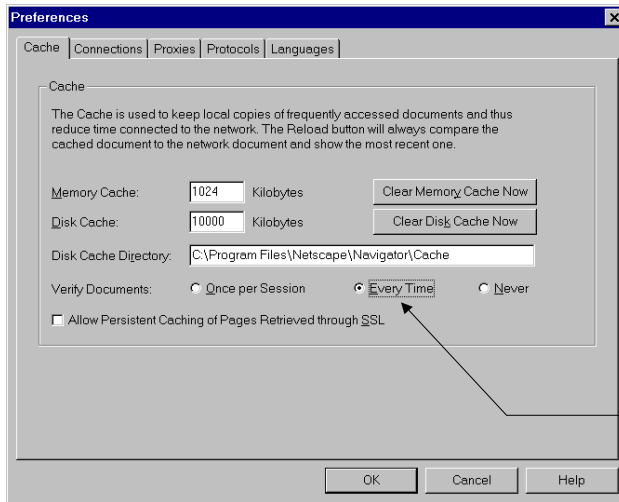
in the 'Preferences' dialog box, click on the 'every time' radio button

- press the JETset 'Save' button before moving from one area, e.g. 'line' to another area, e.g. 'user'; see *using JETset on page 246*. This action will save your changes in volatile memory (RAM); the saving process is instantaneous.

- to save your configuration changes to non-volatile memory, press the 'Admin' button and then select the 'Save to FLASH' button. The unit will spend a few seconds writing to FLASH memory, so we suggest you save to FLASH periodically (e.g. once every thirty minutes)

Internet Explorer - configuration
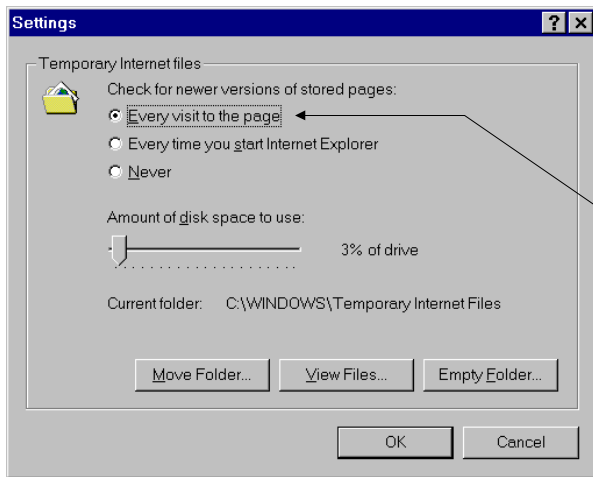
in the 'Settings'
dialog box,
click on the
'every visit to the page'
radio button

- if you visit another URL (address on the World Wide Web) and then wish to return to JETset you can either:

    use the 'JETset' bookmark/favourite entry (the JETset home page), or

    use the 'Go' feature of your browser (if 'JETset' is listed - this is the JETset home page), or

    re-type the ip address of the unit in your 'location' field; e.g.

    ```
    http://192.101.34.211
    ```

    the login page will be displayed; you will need to login again.

JETset program summary

- compatible with Microsoft Internet Explorer® or Netscape Navigator®, both at version 3 or more recent versions

- you can configure most Console Server parameters

- access is restricted to the person with username 'admin'

- although you can configure Console Server sessions, you cannot run them from JETset (sessions are character-based features suited to terminals)

- you can use the 'bookmark/add to favourites' feature of your browser only with the login and home pages

- you can use the 'Go' navigation method of your browser (history file) of your browser only with the login and home pages

Appendix H Troubleshooting

You need to read this appendix if you want information on troubleshooting the Console Server.

This appendix provides information on troubleshooting the Console Server.

This appendix includes the following sections;

Introduction

This appendix contains solutions for problems that may arise while Console Server (the '*unit*').

- if you bought your unit from a registered Black Box Supplier, you must contact their Technical Support department; they are qualified to deal with your problem.

- if you are a registered Black Box Supplier, and bought your unit from Black Box, please contact the Technical Support department of your nearest Black Box office. The addresses and telephone numbers of your nearest Black Box office are shown on the cover of this manual.

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 on the unit devices 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.

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 Appendix F BOOTP 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

JETset problems

Trying to access JETSET you see an 'alert' dialog box, e.g. :

•change the parameter 'gui_access' to 'on'.

Login 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.

- when connecting using a reverse ssh connection, a delay of about 10 seconds for SSH version 1 will be experience. A delay of 20 seconds for SSH version 2 will be experienced. These delays are due to the negotiation of a secure LAN connection. This involves the exchanging of encryption messages to establish a secure communication.

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.

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.

Problems with terminals

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.

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 Appendix F 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.

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.

Index

A

B

C

◆ BLACK BOX®
NETWORK SERVICES