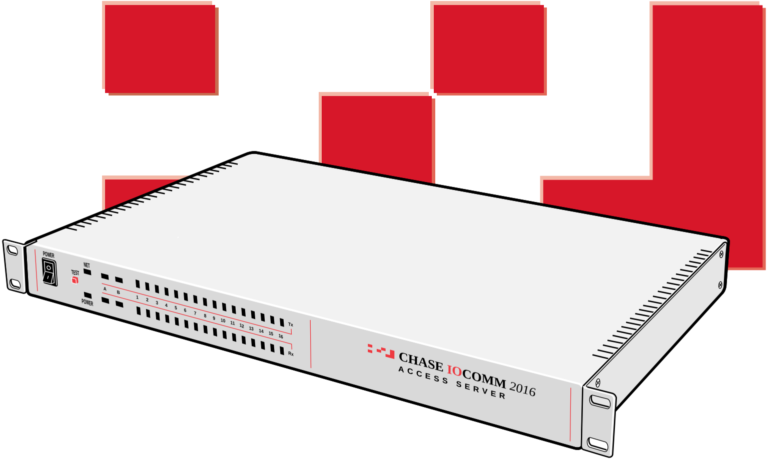
IOCOMM
Access Server



Administration Guide

CHASE
RESEARCH
CONNECTING THE WORLD

Chase Research reserves the right to change product specifications without prior notice.

Ref: IOC/045/104

Contents

Appendices

Figures

Introduction

About this Guide

This guide describes the installation and configuration of the Chase IOCOMM Access Server. It is written with the assumption that the installer will be a systems administrator or someone with a similar level of knowledge.

Experienced users may save set-up time by following the instructions in the *Quick Start Guide* and can consult the sections in this guide for details of more advanced operations.

The remainder of this guide is sectioned as follows:

IOCOMM Set-up
Covers the approach to IOCOMM configuration, connection and power up.

Configuration
Describes the set up and configuration tasks that can be performed.

Bootstrap
Provides information on Start-up process and the Diagnostic menu.

Indicators
Describes the Status indicators and how to interpret the Start-up sequence LEDs.

Troubleshooting
Suggestions for resolving problems encountered while installing or using IOCOMM.

Event Logging (syslog)
Describes the IOCOMM problem and event logging system (syslog).

Exception Display
Provides interpretation information for critical IOCOMM errors.

iocommd
Describes the set up and use of the iocommd peripheral daemon.

Command Line Interface
Defines the command line interface available from the serial and remote login ports.

Connectors & Cabling
Provides pin-out and cabling information.

Technical Specification
Provides a detailed technical description.

Glossary of Terms

Accessories
Lists the Accessories available for the IOCOMM.

Notation Conventions Used

Text in the following font:

```
iocomm
```

indicates input to, or output from the IOCOMM.

Symbols like ↵ and ESC are used to represent keys.

Obtaining More Information

There is a series of on-line documents available to help you use the IOCOMM, and provide up to date information on Chase developments and new features. See our websites listed below.

Support and Help

If you encounter problems during set-up or subsequent use, you should contact your supplier for support. If your supplier cannot resolve the problem, you can use the support facilities provided by Chase Research.

Chase Research WWW

You can check the support sections of our web sites and FTP sites for the latest information, at any time:

www.chaser.co.uk or ftp.chaser.co.uk

www.chaser.com or ftp.chaser.com

Chase Research Technical Support Staff

Here is the standard support route for quickest answers:

1. Have your serial number and problem overview ready.

2. Check with your supplier or distributor.

3. Contact your local Chase Technical Support office, as follows:

United States, Canada & South America:
Email support@chaser.com - fax +1.615.872.0771.

Europe, Asia and Africa:
Email support@chaser.co.uk - fax +44 (0)1256 324562.

Germany, Eastern Europe and Russia:
Email support@chaser.de - fax +49 711.7287.156.

The IOCOMM

Thank you for purchasing the Chase Research IOCOMM Access Server. IOCOMM is a TCP/IP based remote access server and router that allows serial devices to be connected directly to LANs and WANs. IOCOMM is intended to support the following serial devices:

- Modems for remote access and Internet subscribers
- ISDN terminal adapters
- Terminals for multi-user systems
- All types of serial printers
- Data acquisition equipment (manufacturing, laboratory, etc.)
- Retail point-of-sale equipment (bar code readers, cash registers, etc.)
- High-speed leased line drivers (LTU, DSU/CSU, etc.)

IOCOMM can interoperate with hosts running the following operating systems:

- Microsoft Windows®
- Citrix WinFrame
- SCO Unix & SCO UnixWare
- IBM AIX
- Sunsoft Solaris
- Hewlett Packard HP/UX
- Data General DG/ux
- All other variants of Unix (BSD, Linux, etc.)

The configuration diagram shows a typical application of the IOCOMM:

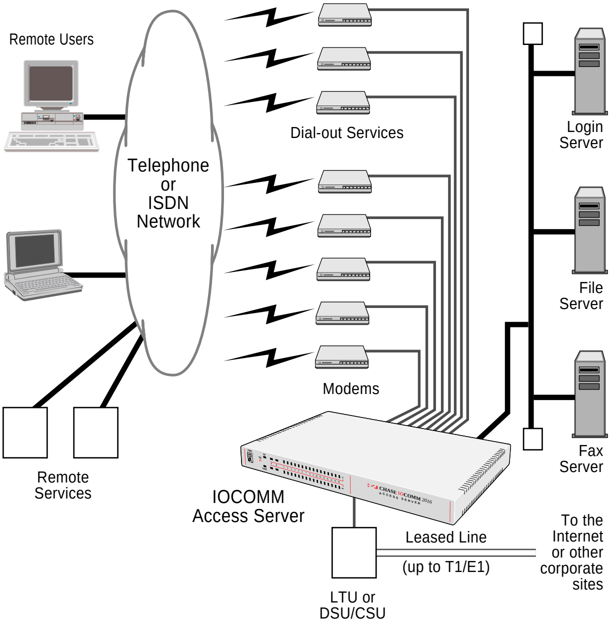


Figure 1: Typical application for the IOCOMM.

Product Description

IOCOMM is a TCP/IP access server with 8 or 16 (RS-232) asynchronous ports, and a synchronous leased line interface for connecting to the Internet or other remote sites via a fixed link. The primary aim of IOCOMM is to provide access to the LAN (or fixed link) for remote dial-in users.

Other services are also available such as LAN attachment for local devices, and dial-on-demand outgoing access for LAN based users.

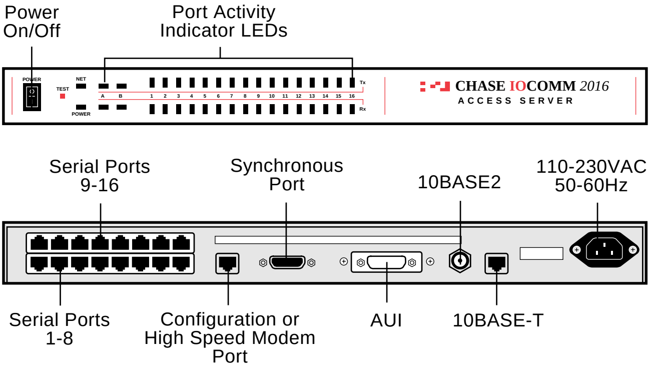


Figure 2: Panel layout of the IOCOMM Access Server.

Hardware features:

- Either 8 or 16 RJ45 serial ports supporting speeds of up to 115.2 kbps.
- A console port that can be configured as an additional remote access port (up to 460.8 kbps).
- A synchronous port for leased line (V.35, X.21 or V.24) access at up to 2.048 Mbps.

  Note: If a synchronous port is not required, this port can be used for asynchronous remote access at up to 460.8 kbps.
- FLASH memory for downloading firmware releases.
- 10BASE2, 10BASE-T and AUI Ethernet auto-sensing interfaces.
- Auto-sensing internal power supply, 110-230V AC
- LEDs for power, network activity, port activity and diagnostic testing

Software features:

- Support for TCP/IP protocols including telnet and rlogin.
- Remote access support including PPP, SLIP, CSLIP and RADIUS.
- Support for RIP, RIP2.
- Printer support via LPD and Chase utilities.
- Chase utilities provide ‘fixed tty’ support for Unix systems.
- User friendly web interface (command line also available).
- ARP or BOOTP for network based set-up.
- Dynamic statistics displays and line status reporting for fast problem diagnosis.
- Support of SNMP MIBs, allowing remote configuration via SNMP as well as statistics gathering.
- Domain Name Server (DNS) support.
- WINS support for Windows environments.
- Port configuration copy and save config function.
- Self-test on power-up.

Security features:

- RADIUS authentication.
- Administration and port password.
- Port locking.
- Authentication with PAP support.
- Per user access level assignment.
- Service logging.

Accounting features include:

- RADIUS accounting.
- Logging facility for audit.
- Logging facility for billing.

Unpacking and Installing IOCOMM

Before unpacking the unit, ensure that you have a suitable, clear working area available.

Carefully open the packaging and remove all items from the box using the list below as a checklist.

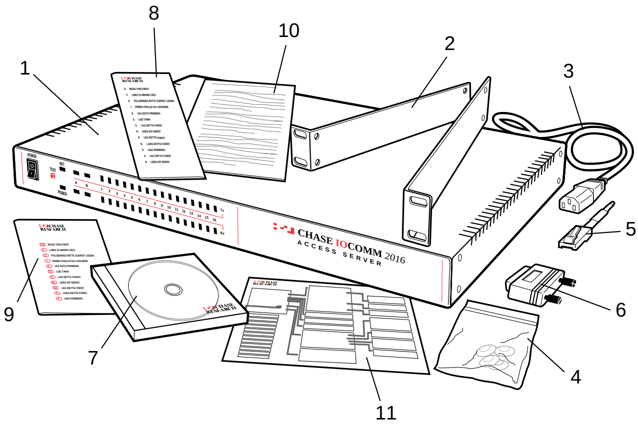


Figure 3: Package contents.

1 IOCOMM unit

2 Rack-mount brackets (fitted)

3 Power cord (for your local supply)

4 Bag containing 6 plastic feet

5 RS-232 loop-back connector (RJ45)

6 Sync port-(B) loop-back connector (DB26)

7 CD-ROM containing Administration Guides

8 Quick Start Guide

9 Electrical safety booklet

10 Release notes (if applicable)

11 IOCOMM Set-up Menu Structure Card

Note: If any items are missing or damaged please contact your supplier.

Rack-Mounting

IOCOMM is shipped with two rack-mounting brackets fitted; the unit will slot directly into a 19" rack without modification.

Reverse Rack-Mounting

IOCOMM can be reverse mounted, to position the LAN connectors and serial port RJ45 connectors at the front of the rack.

To reverse the rack-mount brackets:

1 Place the IOCOMM unit on a stable surface with the brackets at the front,

2 Using a screwdriver, carefully remove the three screws from one bracket only,

3 Remove the bracket and re-fit with the mounting flange at the back of the unit. Refit the 3 screws.

4 Repeat procedure for the other bracket.

5 Check that all six screws are tight and the casing is secure.

Desktop Use

To remove the rack-mount brackets, proceed as follows:

1 Place the IOCOMM unit on a stable surface with the brackets at the front,

2 Using a screwdriver, carefully remove the three screws from one bracket only,

3 Remove the bracket and re-fit the screws immediately to secure the unit's casing.

4 Repeat procedure for the other bracket.

5 Check that all six screws are tight and the casing is secure.

You are advised to keep the brackets in a safe place in case you wish to use the IOCOMM in a rack system at a later date.

Six self-adhesive plastic feet are supplied for the underside of the unit (not to be fitted for rack-mounting). Locate the feet positions marked on the underside of the unit, peel off the adhesive backing from each of the feet and press firmly into place at the marked positions.

Configuration Interfaces

IOCOMM comes with a powerful web browser configuration interface. A Command Line Interface (CLI) is also provided, although this is less comprehensive.

The only action which cannot be executed using the web browser interface is the initial setting of the IOCOMM's IP address, which is covered at the beginning of the next section.

The Command Line Interface (CLI) may be used as a complementary tool for configuration, troubleshooting and maintenance.

Note: Turn off your web browser's cache.

Setting up IOCOMM

Before set-up, carefully consider the location of your unit.

You can connect the IOCOMM to a LAN via one of the three Ethernet connectors:

- 10BASE-T (twisted pair) RJ45 connector,
- 10BASE2 (thin) BNC connector,
- AUI DB15 connector.

The Ethernet connectors will automatically detect the connected media. If no LAN connection is made, the IOCOMM defaults to 10BASE-T.

Note: You can only connect one type of LAN media at any one time. You can however change the LAN media type at any later stage, but you will need to perform a hardware reboot (switch off / switch on) for the unit to recognise the new media type.

10BASE-T:

Attach the cable (with RJ45 connector) from a hub to the port on the rear of the IOCOMM marked 10BASE-T.

10BASE2:

Attach the LAN cable (with BNC T connector) to the port on the rear of the IOCOMM marked 10BASE2. If this unit is the last device on the network, a terminator will be required.

Note: Always ensure that the Ethernet cable segment is at least 0.5 metre in length. The maximum length for a single segment of thin Ethernet cable is 185 metres.

AUI port:

Attach the AUI connector to the IOCOMM port on the rear of the unit marked AUI. The AUI connector allows an external transceiver to be connected, enabling a number of different media types to be used, including 10BASE5 and fibre optic.

The IOCOMM Access Server is now connected to the LAN.

The IOCOMM power supply accepts input voltage in the range 110 to 230 VAC, allowing it to be used world-wide. The power supply is auto-sensing for local conditions and requires no additional user set-up.

Check that the power switch on the front of the IOCOMM is off. Connect the mains lead and then power-on the unit. The green POWER indicator LED on the front left of the unit should be lit.

Configuration

This chapter describes set-up and configuration tasks. Some tasks are mandatory, others are optional.

The tasks in this section are:

Getting Started

Web Access

First Time Configuration Tour

Configuring DNS on IOCOMM

Changing Serial Port Configuration

Resetting a Serial Port

Using a Modem for Dial-in Operation

Outgoing Services

Disabling Incoming Calls by Port

Adding a Terminal

Configuring the Synchronous Port (B)

Printing

Configuring RADIUS

Local Authentication

Dynamic Routing (RIP)

Enabling TCP Security

Global Messages

Configuring Status Logging

Telnet Service (telnetd)

Monitoring Status

Making Changes to IOCOMM

The complete configuration menu structure is shown in the Menu Map below. A full size version is supplied with your IOCOMM.

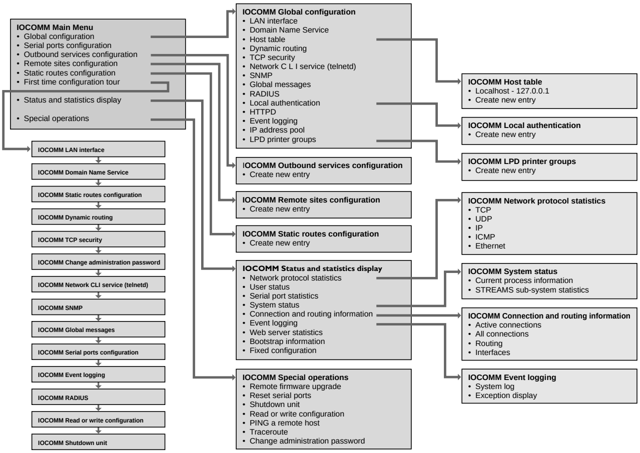

IOCOMM Main Menu
• Global configuration
• Serial ports configuration
• Outbound services configuration
• Remote sites configuration
• Static routes configuration
• First time configuration tour
• Status and statistics display
• Special operations
IOCOMM LAN interface
IOCOMM Domain Name Service
IOCOMM Static routes configuration
IOCOMM Dynamic routing
IOCOMM TCP security
IOCOMM Change administration password
IOCOMM Network CLI service (telnetd)
IOCOMM SNMP
IOCOMM Global messages
IOCOMM Serial ports configuration
IOCOMM Event logging
IOCOMM RADIUS
IOCOMM Read or write configuration
IOCOMM Shutdown unit
IOCOMM Global configuration
• LAN interface
• Domain Name Service
• Host table
• Dynamic routing
• TCP security
• Network C L I service (telnetd)
• SNMP
• Global messages
• RADIUS
• Local authentication
• HTTPD
• Event logging
• IP address pool
• LPD printer groups
IOCOMM Outbound services configuration
• Create new entry
IOCOMM Remote sites configuration
• Create new entry
IOCOMM Static routes configuration
• Create new entry
IOCOMM Status and statistics display
• Network protocol statistics
• User status
• Serial port statistics
• System status
• Connection and routing information
• Event logging
• Web server statistics
• Bootstrap information
• Fixed configuration
IOCOMM Special operations
• Remote firmware upgrade
• Reset serial ports
• Shutdown unit
• Read or write configuration
• PING a remote host
• Traceroute
• Change administration password
IOCOMM Host table
• Localhost - 127.0.0.1
• Create new entry
IOCOMM Local authentication
• Create new entry
IOCOMM LPD printer groups
• Create new entry
IOCOMM Network protocol statistics
• TCP
• UDP
• IP
• ICMP
• Ethernet
IOCOMM System status
• Current process information
• STREAMS sub-system statistics
IOCOMM Connection and routing information
• Active connections
• All connections
• Routing
• Interfaces
IOCOMM Event logging
• System log
• Exception display

Figure 4: Configuration Menu Structure

If you are installing multiple units, you can copy the configuration details between units. The read / write configuration options are covered in *Making Changes to IOCOMM* and in *First Time Configuration Tour*.

The First Time Configuration Tour presents you with a logical sequence of pages extracted from other menus. Avoid using the Cancel button as this will take you off the *First Time Configuration Tour* .

To set up the minimum configuration you can use the *Quick Start Guide* supplied with your IOCOMM or the *First Time Configuration Tour*. It is recommended that Expert mode is not used in the *First Time Configuration Tour*.

Getting Started

The following sections show, step-by-step, how to set up and configure IOCOMM.

Communicating with IOCOMM

IOCOMM needs an Internet Protocol (IP) address. This can be assigned:

- using ARP on a network host,
- via a terminal or PC on port A, or
- using BOOTP on a network host (Unix / Windows® NT).

Using ARP on a local network host is the preferred method.

Determining the Ethernet Address

You will need to enter the Ethernet address of the IOCOMM if you use the ARP jamming or BOOTP procedures.

To determine the Ethernet address, either:

- refer to the product label on the underside of the unit, or
- use a terminal or PC attached to Port A of the IOCOMM, hold in the **TEST** switch, and then turn on the unit - keep the button pressed until the IOCOMM bootstrap menu appears.

Select `1. Hardware Diagnostics` and then option `d` to display the **Diagnostic monitor** and then enter the command `d boot`. The Ethernet address will then be displayed. Press ESC and then `q` to quit the bootstrap.

Setting IP Address via Local Host (ARP jamming)

This is a simple and the recommended method to set the IOCOMM IP address. IOCOMM supports ARP which is the Address Resolution Protocol. ARP allows you to temporarily connect to the IOCOMM to assign an IP address. You will need to perform this operation before you can access the web browser configuration menus.

You must first establish connection to the IOCOMM:

1. From a Unix host, type:

   ```
   arp -s a.b.c.d aa:bb:cc:dd:ee:ff
   ```

   where `a.b.c.d` is the IP address you want for the IOCOMM, and `aa:bb:cc:dd:ee:ff` is the Ethernet address of the IOCOMM (shown on the bottom of the unit).

   On a Windows® system, the ARP command is a slight variation (using dashes instead of colons):

   ```
   arp -s a.b.c.d aa-bb-cc-dd-ee-ff
   ```

   Note: If there are any errors, re-check both the IP address and Ethernet address.

2. Now go to *Setting IP Address Permanently*.

Setting IP Address via Terminal or PC

You can also connect to the IOCOMM using a terminal (or a PC running terminal emulation). The procedure is as follows:

1. Ensure that power to the IOCOMM is switched off.

2. Connect a terminal or PC to port A on the IOCOMM rear panel.

   The IOCOMM serial ports are DTE type RS-232. When connecting a terminal/PC directly, the RS-232 signals need to be crossed over (2 and 3 crossed, 7 straight through). Refer to *Connectors & Cabling* for pinout information.

3. Set the terminal to the following default settings:

   9600 bps, eight data bits, one stop bit, software flow control, no parity

Note: If there are any errors, check the cable you are using (this is the most common problem).

4. Power-on the IOCOMM.

5. You are prompted to enter a **login**. Enter `admin` and press ↵.

6. When prompted to enter a **Password**. Enter the default IOCOMM password `iocomm` and press ↵.

   You should see the prompt `[admin:1]>>`.

   Note: You will need to run the `admin` command before getting permission to run `ifconfig`.

7. To set the **IP address**, enter the following command:

   `ifconfig quicc0 a.b.c.d` and press ↵.

   (where `a.b.c.d` is the IP address you have assigned to the IOCOMM).

   Note: The IP address has now been temporarily set and turning off the power before the IP address has been permanently set via the web browser (see *Setting IP Address Permanently*) will re-set the unit to factory default status with no IP address.

   Note: At this stage, you should set the **netmask** if you use subnets. If the IOCOMM is installed without access to a BOOTP server, the netmask will be a default based on the IP address. This netmask may be suitable for most installations, but if the IOCOMM is installed on a subnet, it will not be possible to communicate with the IOCOMM via the network. If you need to change the netmask enter the following command:

`ifconfig quicc0 netmask a.b.c.d` and press ↵.

(where `a.b.c.d` is the netmask value you require for the IOCOMM.)

8. Go to *Setting IP Address Permanently*.

Setting IP Address via Local Host (BOOTP)

1. Edit the BOOTP file (bootptab under Unix) on a local network host to create a new entry for each IOCOMM you wish to install. This will enable you to connect to the IOCOMM, but you must still permanently set the IP address on the IOCOMM by using the web browser pages.

2. Go to the next section, to permanently set the IP address on the IOCOMM.

Setting IP Address Permanently

To set the **IP address** permanently on the IOCOMM:

1. Activate a web browser on a host on the LAN.

2. In the URL field, type in the IP address you have assigned to the IOCOMM- in the form: `http://[IP address]` and press ↵. You will obtain the **IOCOMM Administration** page.

3. Type in the default password `iocomm` and select **Confirm**. It is recommended that you change this password after installation to maintain security of your network (see *Making Changes to IOCOMM - Changing Passwords*).

The **IOCOMM Main menu** appears.

4. Select **Global configuration**, then **LAN interface**.

5. Enter the IOCOMM's IP Address in the **IP address** field.

6. Select **Submit**.

7. Select **Return to the main menu**.

The IOCOMM Access Server's IP address is now permanently stored.

Configuration and Storage Mechanisms

IOCOMM has three configuration mechanisms; the **Web Browser**, **Command Line Interface** (CLI) and **SNMP**.

During normal start-up, configuration is read from Non-Volatile RAM.

The Web based configuration system makes immediate updates that are also stored in case of power off.

The SNMP and CLI interfaces monitor and modify the live configuration, but changes made are not stored or shown on the Web interface.

Factory reset causes the start-up configuration to be read from a fixed template and various bootstrap detected defaults rather than the permanent store.

TFTP based configuration transfers always run to and from the non-volatile configuration storage and are not acted upon until the system is rebooted.

Note: If you performed a soft factory reset (optioin 3.s in the Booystrap menu), you must submit a confgiguration Web page in order to make a factory reset permanent.

Web Access

Supported Web Browsers

The configuration interface supports the following browsers:

- Netscape (version 3.01 onward)
- Internet Explorer (version 3.02 onward)

Configuring via a Web Browser

Each web page features action buttons which execute entries or provide navigation. Not all action buttons appear on all of the pages; they are only present when they can perform a particular task related to the current page.

The action buttons featured are:

Skip, Cancel, Submit and Expert

Web browser versions / Windowing systems

The exact appearance of the configuration pages will vary slightly between workstations. All web browsers are user configurable and allow changes to font type and size, display parameters, etc. Changes to these settings will cause IOCOMM web pages to display differently.

For example, if you set the typeface on your browser to a very small size, the bold IOCOMM key field names may not appear on-screen as bold type.

IOCOMM Administration password

A password is required to open or change any of the browser pages in order that security can be maintained and access is restricted to authorised configuration personnel only.

IOCOMM is shipped with the factory default password set to `iocomm`. The password should be changed as soon as possible. See also Time-out Function, below.

Note: The Administration password must be a minimum of 4 characters. If a password is too long, it will be truncated to 40 characters.

Other IOCOMM Passwords

All other passwords which can be entered on the IOCOMM web pages, have no minimum number of characters (can be null if required) but will be truncated to 40 characters.

Time-out Function

As a security measure, the IOCOMM Web browser pages feature a time-out function. If a browser page has been open for approximately 15 minutes without an action button being used, the current session / user is terminated.

The IOCOMM administration password must be re-entered before work can continue.

Using Bookmarks

The IOCOMM URL may be added to your bookmark list to save typing in the address every time you access the IOCOMM web browser pages.

Second User

If a second user / administrator has been issued with the browser password and tries to log on to the system whilst it is already in use, a warning message will be displayed to this effect. If the second user continues, enters the password and confirms it, the current user will be locked out until the administration password is re-entered.

Text Fields

IOCOMM web pages use text input fields to enable the unit to be set up and configured. Text input fields (other than those detailed separately in this section) are restricted to a maximum of 100 characters.

Key Fields

Certain IOCOMM web pages contain a text entry field which is known as a key field. This means that the text entered in the field must be unique to that particular entry. The key fields are identified on the web pages by the name of the field being shown in bold text. A key field will usually be the first text field on the relevant page.

On the following page is a list of Key fields used on the IOCOMM web pages:

Page	Sub-page	Field name
SNMP		IP Address
Domain Name Service	Host table	Host name
Local authentication		User I.D.
LPD Printer groups		Printer Group Name
Outbound services configuration		Service Name
Remote sites configuration		Remote Host name

Figure 5: Table of Key Fields.

Text entered in key fields is case sensitive. If you create an entry in a key field with the text `England`, you would also be able to create an additional and separate entry with the text `england`.

Text entered in key fields may be up to 62 characters long and is limited to a specified range of allowable characters. These are:

`a` - `z`, `A` - `Z`, `0` - `9`, underscore (_), dash (`-`) and full stop (`.`)

Task Oriented Instructions

Most of the sections in this guide provide detailed information on performing specific tasks (each section provides a step-by-step guide to set-up and configuration operations).

Changing the Web Server TCP Port Number

The most commonly used TCP port number for web page services (httpd) is 80. This number is the default for the IOCOMM and should be able to be used with no problems. If you wish to change the port number, this can be done through the **IOCOMM HTTPD** page.

To change the port number:

1. On the **IOCOMM Main menu**, select **Global configuration**.
2. Select **HTTPD**.

   The page will display the current web port number in the selection box:

   ```
   IOCOMM Web server port [80 ]
   ```

3. Using the cursor, select the current number and enter your new number.

   Note: If you change the web server port number, you will need to add the new port number to the IOCOMM URL each time you access the unit. For example, if you change the web server port number to 8000:

   ```
   IOCOMM Web server port [8000 ]
   ```

   You must enter a new URL in the form: `http://[IOCOMM address]:8000`.

4. Select **Submit**.
5. Select **Return to the main menu**.

Changing the IP Address

The IOCOMM needs an IP address to communicate with and obtain services from other machines on local or remote networks. The IP address should have already been set, but if you wish to change it:

Note: This address must be set to a value that is consistent with the network the IOCOMM is on.

You should also ensure that any relevant entries on DNS servers are updated.

1. On the **IOCOMM Main menu**, select **Global configuration**.
2. Select **LAN interface**.
3. Enter the new **IP address** that is assigned to the IOCOMM.
4. Select **Submit**.
5. Select **Return to the main menu**.

Changing the Netmask

If you do not enter a netmask, the IOCOMM will itself calculate and provide a default netmask. If you wish to change the netmask for any reason proceed as follows:

1 On the **IOCOMM Main menu**, select **Global configuration**.

2 Select **LAN interface**.

3 Enter the new **IP netmask**.

4 Select **Submit**.

5 Select **Return to the main menu**.

Setting the IOCOMM Hostname

The DNS host name for the IOCOMM can be entered through the web browser pages. Note that this procedure only allows you to enter the name for administration purposes; it does not set up the DNS profiles for the network. This must be done as a separate operation on the network's DNS server. Enter the DNS host name as follows:

1. On the **IOCOMM Main menu**, select **Global configuration**.
2. Select **LAN interface**.

3. Check that the **IP address** field is already completed.

   a If not already completed, enter the assigned IP address and select **Submit**.

   b If it is already completed, select **Cancel**

   Both option a and option b return you to the **Global configuration** page.

4. Select **Domain Name Service**.

5. Enter the assigned name in the **IOCOMM host name** field.

   Note: The name entered here should be the name which has been set up on the DNS server(s) for this device.

6. Select **Submit**.

7. Select **Return to the main menu**.

Setting an IP Address Pool

If you wish to offer floating IP addresses to the PPP dial-in calls, set up an IP address pool:

1. On the **IOCOMM Main menu**, select **Global configuration**.

2. Select **IP address pool**.

3. In the **IP address range**, enter the range by filling in the following fields:

```
Start IP address  [                 ]
End IP address   [                 ]
```

4. Select **Submit**.

5. Select **Return to the main menu**.

First Time Configuration Tour

This section guides you step-by-step through the configuration pages allowing you to check the default values and change them if required.

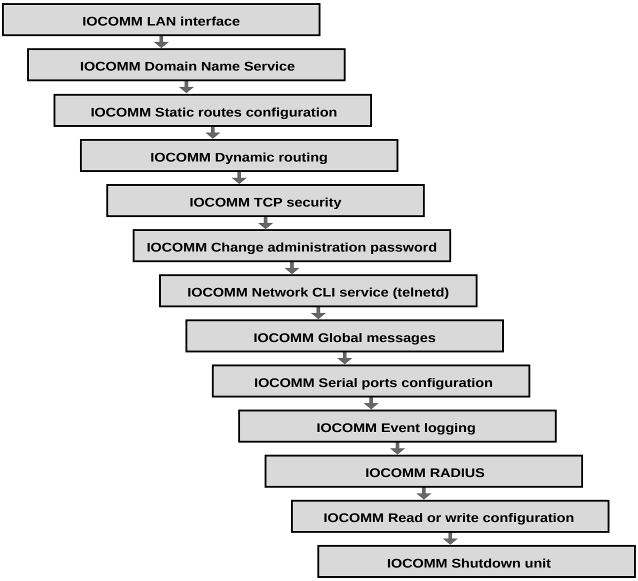

IOCOMM LAN interface
IOCOMM Domain Name Service
IOCOMM Static routes configuration
IOCOMM Dynamic routing
IOCOMM TCP security
IOCOMM Change administration password
IOCOMM Network CLI service (telnetd)
IOCOMM Global messages
IOCOMM Serial ports configuration
IOCOMM Event logging
IOCOMM RADIUS
IOCOMM Read or write configuration
IOCOMM Shutdown unit

Figure 6: The First Time Configuration Process Tour Map.

Note: Using the Cancel button will take you out of the First Time Configuration Tour.

1. Activate a Web browser on a local host on the LAN.

2. In the URL field, type in the IP address of the IOCOMM and press ↵. You will obtain the **IOCOMM Administration** page.

3. Type in the administration password and select **Confirm**.

4. On the **IOCOMM Main menu** page, select **First time configuration tour**.

The **IOCOMM LAN interface** page

1. In the **IP address** box, enter the IP address assigned to this IOCOMM.

   Note: The IP address may have been previously entered.

2. In the **IP Netmask** box, enter the appropriate netmask value.

   Note: The Ethernet address for the IOCOMM is factory set and cannot be modified.

3. When you have completed the **LAN interface** page, select **Submit** to confirm entries or, if you have made no changes, select **Skip** to continue to the next page.

The **IOCOMM Domain Name Service** page

Entering data in the fields is optional; you may find it useful.

Note: To avoid confusion, the name entered here should be the name which has been set up on the DNS server(s) for this device. Although you can enter a different name, it serves no purpose.

1. Complete the following fields as required:

   ```
   First server
   Second server
   Third server
   Default domain
   IOCOMM host name
   NetBIOS name servers
   ```

2. If you enter data select **Submit**, if not select **Skip** to continue to the next page.

The **IOCOMM Static routes configuration** page

You need to add a new entry for each permanent route you wish to create. RIP listening is a more dynamic alternative to these fixed links and can be found on the next page in the **First Time Configuration Tour**.

To create a static route:

1. Select **Create new entry**. The following fields will need to be completed.

   `Destination IP`

2. Enter the IP address of the remote host to which you wish to create a static route.

   Note: You can also specify a host name in this box, but there must be a corresponding DNS entry.

   `Destination mask`

3. Enter the appropriate mask value.

   `Gateway IP`

4. Enter the IP address for the gateway (router) device.

   Note: You can also specify a host name in this box, but there must be a corresponding DNS entry.

5. Select **Submit**. You will obtain the **Static routes configuration** main page and your new entry will be listed.

6. If required, create further static routes by selecting **Create new entry**.

7. If you wish to store a default route enter the IP address in the **Default route** field and select **Submit**.

Note: You can also specify a host name in this box, but there must be a corresponding DNS entry.

8. If you do not wish to store a default route, select **Skip** to continue to the next page.

The **IOCOMM Dynamic routing** page

1. Select to enable one of the three RIP options:

   ● **Enable RIP listening only**

   ○ **Enable RIP listening and advertising**

   ○ **Disable RIP**

2. Select the appropriate version of **RIP**

   ○ **RIP Version 1 only**

   ● **RIP Version 2**

3. Enter the **RIP Version 2 authentication password** (if applicable)

4. If you enter data select **Submit**, if not select **Skip** to continue to the next page.

The **IOCOMM TCP security** page

This page enables you to enter TCP security information for up to three permitted IP addresses.

1. In the First permitted **IP addresses fields**, enter the **Mask value** and **Mask result**.

2. Repeat this step for the second and third permitted IP address (as appropriate).

3. f you enter data select **Submit**, if not select **Skip** to continue to the next page.

The **IOCOMM Change Administration password** page

Note: You do not have to change the administration password from the default at this time, but if not already changed it is advisable to do so. If you do decide to change it, make sure to keep a note of the new password - it is very difficult to recover admin control without the correct password.

1 If you enter a new **password**, complete the **password** boxes and select **Submit**.

2 If you do not wish to enter a new password at this time, select **Skip** to continue to the next page.

The **IOCOMM Network CLI service (telnetd)** page

1. Select **Enable telnetd**.

   This option allows or disallows an external user to make a telnet connection to the access server.

2. From the list below, select the **authentication type** you wish to impose when the user tries to establish a dial-up connection to the IOCOMM.

   □ **Allow automatic PPP detection**

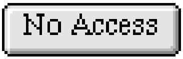
   □ **PPP uses PAP authentication**

   □ **PPP uses CHAP authentication**

3. If required, select **Display login banner** to enable display of the login banner (entered on the **Global messages** page) when a user makes a telnet connection to the IOCOMM.

4. If required, select **Display message of the day** to enable display of the message of the day (entered on the **Global messages** page) when a user makes a telnet connection to the IOCOMM.

5. Click the appropriate button to select the type of authentication mode for telnet connections to the CLI:



Disallows any access.

Asks for the password.

Allows them straight in.

6. Select **Submit** if you have entered data or **Skip** if no changes have been made.

The **IOCOMM SNMP** page

□ Enable SNMP access

1. If you wish to implement SNMP, check the box.

   You have the option of entering general system information in the following fields; for example:

```
Support contact       [John_Brown}
System description    [Access_Server_03]
System location       [Accounts_Department]
```

   This information may be useful for general network administration. The information you enter in these fields will appear on the **IOCOMM Administration** page each time the Web browser for the IOCOMM is opened.

   The **Support contact** line can also be used to create an e-mail shortcut, enabling e-mail messages to be sent directly to the relevant support person (internally or externally).

To use this facility, complete the field using the form as follows:

```
Support contact        [mailto:john_brown@anyco.com]
```

The e-mail shortcut can then be used by clicking on the mail address line shown on the **IOCOMM Administration** page.

□ Enable SNMP traps

2. If you require SNMP traps, check the box.
3. Enter the **IP Address** and **Community name** for up to three trap settings as required.
4. Select **Submit** if you have entered data or **Skip** to continue to the next page.

The **IOCOMM Global messages** page

The **Global messages** page allows you to enter any information that you feel would be relevant or useful to log-in users.

For example, the **Login banner** might say **Welcome to the XYZ network**. The **Message of the day** might say **Network unavailable after 4pm today**.

1. Complete the text fields for **Login banner** and **Message of the day** as required.

   Note: Product I.D. and **Serial number** are factory pre-set and cannot be changed.

2. If you enter data select **Submit**, if not select **Skip** to continue to the next page.

The **IOCOMM Serial ports configuration** page

This page allows you to specify a port you wish to configure.

The options are:

1. Select **Physical parameters**

```
Description    [Asynchronous serial device ]
```

Note: The **Description** field is for information only and is set to **Asynchronous serial device** as default. It can be changed as required, but has no operational function.

The next options allow you to specify:

```
Terminal type         [wyse50 ]
Attached device       [Asynchronous terminal ]
Current mode is:      Asynchronous
Select new mode       [Synchronous]
Baud rate             [9600 ]
```

Note: The **Terminal type** field is for information only and is set to **wyse50** as default.

2. For **Attached device** and **Baud rate**, select the down arrow for option list and select the required settings.

3. At this point, you can write this configuration to one or more additional ports for which you require the same settings. If required, check the additional port boxes.

4. Select **Check here to reset port and make changes immediate** if you wish the new settings to be effective immediately.

5 Select **Access options**.

6. If you require the port(s) to be **Available for outgoing services** (e.g. dial out), check the box.

   Incoming authentication

7. If you require **PPP services**, select the appropriate box(es) from the following options:

   ☒ **Allow automatic PPP detection**

   □ **PPP uses PAP authentication**

   □ **PPP uses CHAP authentication**

8. If you wish the **Login banner** and/or the **Message of the day** to appear on this port, select the appropriate boxes:

   ☒ **Display login banner**

   □ **Display message of the day**

Granted capabilities

9. The items under **Granted capabilities** specify the local and remote access capability of the port(s). Select the boxes as required .

   ☒ **Login (to remote host)**
   This option allows the dial-in user to connect onward to other hosts via the IOCOMM using telnet or rlogin.

   ☒ **Framed access (PPP or SLIP connection):**
   This option allows the user to run PPP or SLIP protocols over the link.

   ☒ **NAS (Command Line Interface):**
   This option enables access to the CLI with user level (non-admin) commands.

   ☒ **Admin:**
   This option enables access to CLI with a full set of access server administration commands.

10. Select **Check here to reset port and make changes immediate** if you wish the new settings to be effective immediately.

11. Select **Modem options**.

    The Modem options (initialisation commands) available on this page are listed below. The entries shown to the right of each field are the default settings.

    ```
    1st init string      [AT ]
    Response             [OK ]
    2nd init string      [ATV1 ]
    Response             [OK ]
    3rd init string      [ATS0=1 ]
    Response             [OK ]
    Dial string          [ATD ]
    Response             [CONNECT ]
    Modem disconnect     [%D+++%DATH%D ]
    Response             [OK ]
    ```

    IOCOMM is shipped with default standard AT command settings. These default settings should work with many ‘standard’ modem types.

12. Edit the commands as required and then select any additional ports to which you wish to write the new configuration.

    Note: Initialisation strings should not contain any commands that may cause the modem to pause operation. For example, the **save configuration** command on some modems.

    Changes will not take place until port is next reset.

13. Select **Check here to reset port and make changes immediate** if you wish the new settings to be effective immediately.

14. Select **Submit** to continue to the next page.

The **IOCOMM Event logging** page

IOCOMM can log events to the console port (A), an internal storage buffer or a remote host.

1. These options allow you to select where the event logging is stored or displayed and the level of event log you wish to capture. Select from the pull down menus as required.

   ```
   Minimum level to log to console      [No logging ]
   ```
   (displays on console on port A)

   ```
   Minimum level to log to buffer       [debug ]
   ```
   (stores log in internal buffer)

   ```
   Minimum level to log to remote host  [No logging ]
   ```
   (logs events in syslog on remote host)

   If you select `No logging`, no event logs will be stored to this destination. If you select any other level, all levels including the one you have selected and above, will be logged. For example, if you select `notice`, all events from `emergency` down to `notice` will be logged. Repeat this selection for the three destinations.

   Note: The IOCOMM internal log holds the last 100 event logs.

   The event logs saved to buffer or console will provide **time** and **date** stamping only if a remote host has also been specified (even if `No logging` has been set for the remote host).

   The event logs written to the IOCOMM buffer can be viewed by using either the command **syslog display [number]** in CLI mode or by using the IOCOMM web browser pages (from the **Main menu**, select **Status and statistics display**, then **Event logging**, then **System log**).

Note: If the IOCOMM is switched off or re-booted, all event logs held in the internal buffer will be lost.

2. To write logs to a remote host, enter either the host name or IP address for the host in the **Remote syslog host** box. Event logs can be viewed on the selected remote host using the standard syslog command.

```
Remote syslog host                  [ ]
Remote host facility to map to      [NONE ]
```

Note: For this option to function correctly with a host name, DNS must be correctly configured. If DNS is not correctly configured, only the IP address entry can be resolved.

3. You can set up a special facility on the remote host to capture event logs to specific locations. For example, you could select local 3 as the facility for capturing event logs from the IOCOMM in a particular location, or you could set up a log facility for each individual IOCOMM.

4. When you have completed all required sections, select **Submit** to save entries or **Skip** to continue.

The **IOCOMM RADIUS** page

IOCOMM supports RADIUS authentication and accounting.

1. Check the following boxes as required.

□ **Enable RADIUS authentication**

□ **Enable RADIUS accounting**

□ **Enable special login prefix recognition**

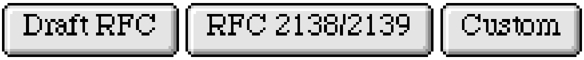
Note: Without the **Enable RADIUS authentication** box selected, only the **Enable special login prefix recognition** setting will be effective.

2. Enter the details for the **First server** on the network, completing the **Server's host name** and **Shared secret** boxes.

   First server

   ```
   Host name      [ ]
   Shared secret  [ ]
   ```

3. You can also set the **Network connection ports**. To do this, select the appropriate button. The options are:

4. Repeat the steps above, for the **Second** and **Third** servers (if required).

5. Select **Submit**, or **Skip** to continue to the next page.

The **IOCOMM Read or write configuration** page

This page allows you to copy the complete configuration information from the current IOCOMM to a file on a remote host.

1. First create a file on the remote host; the file should have zero contents. An example is given below:

   ```
   /etc/tftpboot/access_server1.db
   ```

2. In the **Name or IP address of host** field, enter the remote host IP address or host name if you specified a DNS server on the D**omain Name Service** page.

3. In the **Configuration file name** field, enter the full path and file name of the file you created on the remote host.

4. Select **Write configuration to host**. The configuration will then be copied to the file on the remote host and a page similar to the following example should appear:

   ```
   Writing file /usr/tftpboot/hamlet.db

   To remote host magma

   This is the end of the first time tour.

   To make all changes effective now, please
   click on the Shutdown button.
   ```

   When the above page appears, the operation is complete. If you select **Skip** instead of **Write configuration to host**, you will be taken straight to the **IOCOMM Shutdown unit** page without copying the configuration.

   Note: The file can be copied back to one or more IOCOMMs to duplicate configuration information. See the section Saving/Copying Configuration File.

5. Select **Shutdown** to obtain the I**OCOMM Shutdown unit** page.

The **IOCOMM Shutdown unit** page.

1. Select **Confirm shutdown**.

   The IOCOMM will re-boot and all changes submitted during the **First time configuration tour** will be implemented.

   During the re-boot, the following will appear on screen:

   ```
   Reset
   ```

```
The IOCOMM will now reset.

All connections will be dropped.

Please wait for 2 minutes and then
reconnect to the IOCOMM.
```

Note: When the IOCOMM is being re-booted, the Web browser connection is terminated.

2. Wait two minutes, re-enter your hostname or IP address and you will be presented with the **IOCOMM Administration** page.

Configuring DNS on IOCOMM

A Domain Name Server (DNS) makes addresses easier to manage by allowing the use of machine names in place of IP addresses. The actual IP addresses are obtained from the DNS server.

You will need to know which host is being used as the DNS (may be more than one). To allow IOCOMM to use DNS:

1. On the **IOCOMM Main menu**, select **Global configuration**.

2. Select **Domain Name Service**.

3. On the **Domain Name Service** page enter the following fields:

   `First server`
   (This is the primary server for DNS.)

   `Second server`
   (This is a standby server and will be used if the first server fails.)

   `Third server`
   (This is a second standby server.)

```
Default domain name
```

(Your domain name (e.g. mycompany.com).)

```
IOCOMM host name
```

(This is the IOCOMM host name.)

4. Select **Submit**. You will be returned to the **Global configuration** menu.
5. Select **Return to the Main menu**.

Changing Serial Line Configuration

Serial port settings need to match the device you are attaching to a port.

Note: No changes to settings will take effect until you activate the **reset port(s)** option at the bottom of the page.

Changing Physical Parameters

1. On the **IOCOMM Main menu**, select **Serial ports configuration**.
2. Select the **port number** for which you wish to set the physical parameters. You can configure one or more ports with the same settings by selecting additional ports on the **Physical parameters** page.
3. Select the **Physical parameters** option.

   Note: The Description field is for information only and is set to **Asynchronous serial device** by default.

   The fields allow you to specify:

   ```
   Terminal type    [wyse 50 ]
   Attached device  [Asynchronous terminal ]
   Baud rate        [9600 ]
   ```

   Note: The **Terminal type** field is for information only and is set to **wyse50** as default.

4. For the **Attached device** and **Baud rate** options, select the down arrow for option list and then select required setting.

5. At this point, you can write this configuration to additional ports for which you require the same settings by selecting the port boxes.

   There is also an **Expert** mode for **Physical parameters** offering additional configuration options.

6. Select the **Expert** button. You will be presented with the following additional fields:

```
Character framing     [8 data, no parity, 1 stop ]
Inactivity timeout    [No timeout ]
```

   Character framing defines the format of the asynchronous characters on this link.

   Inactivity timeout allows dialled connections to be automatically shut down after a period of no data traffic.

7. For **Character framing**, select the down arrow and choose from the list.

8. For **Inactivity timeout**, select the down arrow and choose the appropriate timeout setting.

   Special wiring options cause the access server to ignore the RS-232 signals DCD or DSR.

   Special operations option allows the access server to be used with modems that do not raise RTS until a call is connected.

   Special wiring

   □ **DCD ignored/not wired**

□ **DSR ignored/not wired**

Special operations required for attached modems

□ **RTS not raised until DCD present**

Flow control parameters

○ **Hardware flow control**

● **Software (XON/XOFF) flow control**

○ **None**

If required, data flow control can be performed using RS-232 signals or special XON/XOFF characters.

9. Select **Check here to reset port and make changes immediate** if you wish the new settings to be effective immediately.
10. Select **Submit**. Your changes will be saved and you will obtain the main **Serial ports configuration** page.
11. Change **Access Options** or **Modem options**, at this point if you wish. Otherwise, select **Return to the Main menu**.

Changing Access Options

1. On the **IOCOMM Main menu**, select **Serial ports configuration**.
2. Select the port number for which you wish to set the **Access options**. You can configure just one port, or by selecting additional ports on the **Access options** page, any number of ports with the same settings.
3. Select the **Access options** button.
4. If you require the port(s) to be **Available for Outgoing services** in addition to incoming, check the box.

5. If you require PPP to operate over this link, set your requirements here:

   ☒ **Allow automatic PPP detection**

   ☐ **PPP uses PAP authentication**

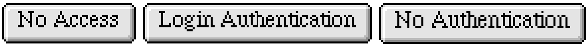
   ☐ **PPP uses CHAP authentication**

6. If you wish the Login banner and/or Message of the day to appear at start-up, check the boxes:

   ☒ **Display login banner**

   ☐ **Display message of the day**

7. For authentication, select from the following options:



8. Select the **Expert** button for additional configuration options.

Granted capabilities

9. Items specify the local and remote access capability of the port(s). Check boxes to select.

   ☒ **Login (to remote host)**
   Allows the user to make ongoing connections to other hosts from the access server using telnet or rlogin.

   ☒ **Framed access (PPP or SLIP connections)**
   Allows the user to run PPP or SLIP connections on this port.

   ☒ **NAS (Command Line Interface)**
   Enables access to the CLI for non-admin (user level) commands.

☒ **Admin**

Enables access to the CLI with a full set of administration commands.

```
Default command [shell ]
```

The **Default command** field defines what happens when the login sequence completes successfully and `shell` will be most commonly used.

The `shell` (default) command presents the user with a Command Line Interface from which they can run any command for which they have the necessary granted access.

Example: To make an automatic connection to a specific host, the following could be used:

```
rlogin -1 newuser signup.my.domain
```

10. To change the command, delete the old entry and type in the new command.

11. You can now write this configuration to additional ports for which you require the same settings. Check the additional port boxes.

12. Select the **Check here to reset port and make changes immediate** box if you wish the new settings to be effective immediately.

13. Select **Submit**. Your changes will be saved and you will return to the main **Serial ports configuration** page.

14. To change the **Physical parameters** or **Modem options**, you can select them from here and follow the appropriate instructions. Otherwise, select **Return to the Main menu**.

Changing Modem Options

1. On the **IOCOMM Main menu**, select **Serial ports configuration**.

2. Select the **port number** for which you wish to set **Modem options**. You can configure just this port, or by selecting additional ports on the **Modem options** page, any number of ports with the same settings.

3. Select **Modem options**.

   Modem options (initialisation commands) available on this page are listed below. Entries shown to the right of each field are the IOCOMM factory default settings.

   ```
   1st init string       [AT ]
   Response              [OK ]
   2nd init string       [ATV1 ]
   Response              [OK ]
   3rd init string       [ATS0=1 ]
   Response              [OK ]
   Dial string           [ATD ]
   Response              [CONNECT ]
   Command mode          [%D+++%DATH%D ]
   Response              [OK ]
   ```

   The default settings will work with many modem types.

4. If you need to edit commands, delete the existing text, insert the new text and then select any additional ports to which you wish to write the new configuration.

   Note: Initialisation strings should not contain any commands that may cause the modem to pause operation. For example, the save configuration command on some modems.

5. Select **Check here to reset port and make changes immediate**.

6. Select **Submit**. You will return to the main **Serial ports configuration** page.

7. Select **Return to the main menu**.

Resetting a Serial Port

The IOCOMM web browser provides a simple method of resetting a serial port. This can be useful in situations where an attached device has hung and you wish to re set the particular port without having to re-boot the complete unit. To reset a serial port on the IOCOMM proceed as follows:

1. On the **IOCOMM Main menu**, select **Special operations** then **Reset serial ports**.

2. Check the **port box(es)** for the **port(s)** you wish to reset.

3. Select **Reset port**. The port(s) selected will be reset and you will be returned to the **Special operations** page.

4. Select **Return to the main menu**.

Using a Modem for Dial-in Operation

Dialling in with PPP/SLIP

Dial-in users run serial line protocols such as PPP or SLIP over links. To configure IOCOMM to accept these connections:

1. On the **IOCOMM Main menu**, select the **Serial ports configuration** option.

2. Select the **port number** the modem is attached to.

3. Select **Physical parameters**.

4. In the **Attached device** field, select the down arrow and then select the **Asynchronous modem** option.

5. In the **Baud rate** field, select the down arrow and then select the appropriate setting for the attached modem.

6. Select **Expert**.

7. Set the **Character framing** option to match those of your modem by selecting the down arrow and then selecting the appropriate setting. An **Inactivity timeout** can also be set in the same way.

8. If required, select the appropriate box(es) for **Special operations required for attached modems** and then select one setting under **Flow control parameters**.

9. Select **Modem options**.

   The modem options (initialisation commands) available on this page are listed below: The entries shown to the right of each field are the default settings.

   ```
   1st init string      [AT ]
   Response             [OK ]
   2nd init string      [ATV1 ]
   Response             [OK ]
   3rd init string      [ATS0=1 ]
   Response             [OK ]
   Dial string          [ATD ]
   Response             [CONNECT ]
   Command mode         [%D+++%DATH%D ]
   Response             [OK ]
   ```

   IOCOMM is shipped with default standard AT command settings. These default settings will work with many modem types.

   If you need to edit commands, replace the text and then select any additional ports to which you wish to write the new configuration.

Note: Initialisation strings should not contain any commands that may cause the modem to pause operation. For example, the **save configuration** command on some modems.

10. Select **Check here to reset port and make changes immediate**.

11. Select **Submit**.

12. Select **Return to the main menu**.

Issue a CHAP challenge

When you have set up the IOCOMM port for dial-in facility using a PPP type link, you can have PAP or CHAP type authentication to verify the caller. PAP authentication is based on a procedure using an un-encrypted password, whereas the CHAP procedure uses an encrypted password.

By default PAP or CHAP authentication is not activated. To activate these authentication procedures:

1. On the **IOCOMM Main menu**, select **Serial ports configuration**.

2. Select the port on which you want to impose the authentication restriction.

3. Select **Access options**.

4. In **Access options** select one of the following:

   ☒ **Allow automatic PPP detection**

   □ **PPP uses PAP authentication**

   □ **PPP uses CHAP authentication**

   Note: You can select both PAP and CHAP authentications if you wish. The IOCOMM first checks if the user has CHAP facility, if not it goes on to use PAP.

5. Select **Check here to reset port and make changes immediate**.

6. Select **Submit**.

7. Select **Return to the main menu**.

Outgoing Services

Remote hosts are machines not connected to your local network. These can be reached via a fixed link (attached to the synchronous port (B) or another router on your local network), or via a temporary dial-up connection. This section covers temporary dial-up connections and fixed links.

Dial-up Connections

To make dial-up connections you need to connect a modem to a serial port on the IOCOMM:

1. On the **IOCOMM Main menu** page, select **Serial ports configuration**.

2. Select the **port number** to which you have attached the modem.

3. Select **Modem options**.

   The **Modem options** (initialisation commands) available on this page are listed below. Entries shown to the right of each field are the IOCOMM factory default settings.

```
1st init string       [AT ]
Response              [OK ]
2nd init string       [ATV1 ]
Response              [OK ]
3rd init string       [ATS0=1 ]
Response              [OK ]
Dial string           [ATD ]
Response              [CONNECT ]
Command mode          [%D+++%DATH%D ]
Response              [OK ]
```

Check that the settings are suitable for your modem.

Note: Initialisation strings should not contain any commands that may cause the modem to pause operation. For example, the **save configuration** command on some modems.

4. Select **Physical parameters**

```
Description           [Asynchronous serial device ]
```

Note: The **Description** field is for information only.

The next options allow you to specify:

```
Terminal type          [wyse 50 ]
Attached device        [Asynchronous terminal ]
Baud rate              [9600 ]
```

Note: The Terminal type field is for information only.

5. For the **Baud rate** and **Attached device** options, select the down arrow for an option list and then select the required setting.

6. Check the **port boxes** to write this configuration to additional ports for which you require the same settings.

There is also an **Expert** mode for **Physical parameters** which offers additional configuration options.

7. Select the **Expert** button while still in the **Physical parameters** page.

You will be presented with the additional options:

```
Character framing      [8 data, no parity, 1 stop ]
Inactivity timeout     [No timeout ]
```

Character framing defines the format of the asynchronous characters on this link.

Inactivity timeout allows dialled connections to be automatically shut down after a period of no data traffic.

8. For **Character framing**, select the down arrow and choose from the list.

9. For Inactivity timeout, select the down arrow to view and select the appropriate timeout setting.

   Special wiring options cause the access server to ignore the RS-232 signals DCD or DSR.

   Special operations option allows the access server to be used with modems that do not raise RTS until a call is connected.

   Special wiring

   □ **DCD ignored/not wired**

   □ **DSR ignored/not wired**

   Special operations required for attached modems

   □ **RTS not raised until DCD present**

   Flow control parameters

   ○ **Hardware flow control**

   ● **Software (XON/XOFF) flow control**

   ○ **None**

   If required, data flow control can be performed using RS-232 signals or special XON/XOFF characters.

10. Select **Check here to reset port and make changes immediate**.

11. Select **Submit**.

12. Select **Return to the Main menu**.

13. Select **Remote sites configuration** and then **Create new entry.**

    Note: Details for the following fields should be obtained from the Remote Host administrator.

14. Enter the **Remote host name**.

15. Enter the **Telephone number** of the remote modem.

16. Enter the **username**.

17. Enter the **password**.

18. Enter the **IP Address** of the Remote Host.

19. Enter the **IP Netmask** of the Remote Host.

20. Select again the **port number** to which you have attached the Modem.

21. Select **Submit**.

22. Select **Return to the Main menu**.

Routing via Fixed Links

You need to create a new entry for each permanent route you wish to create. *RIP listening* is a more dynamic alternative to these fixed links.

1. On the **IOCOMM Main menu** page select **Static routes configuration**.

2. If you have static routes already set up and wish to change one, select the entry for the route you wish to change and edit the entry as appropriate. Select **Submit** to save the entry.

3. If you do not have any static routes configured or wish to add a new route, select **Create new entry**. The following fields will need to be completed:

   `Destination IP`

   Enter the **IP address** of the remote host to which you wish to create a static route.

   Note: You can also specify a host name in this box, but there must be a corresponding DNS entry.

   `Destination mask`

   Enter the appropriate mask value.

   `Gateway IP`

   Enter the **IP address** for the gateway (router) device.

   Note: You can also specify a host name in this box, but there must be a corresponding DNS entry.

4. Select **Submit**. You will obtain the **Static routes configuration** main page and your new entry will be listed.

5. If required, create further static routes by selecting **Create new entry** or quit the page by selecting **Return to the Main menu**.

Disabling Incoming Calls by Port

Some or all of the IOCOMM serial ports can be prevented from accepting incoming calls, thereby dedicating them to outgoing calls.

1. On the **IOCOMM Main menu page**, select **Serial ports configuration**.

2. Select the **port number** to which you wish to deny access to incoming calls.

3. Select **Access options**.

4. Select **No Access**. The new setting will be displayed.

5. Select **Submit**.

6. Select **Return to the Main menu**.

Adding a Terminal

The access server can be used to connect asynchronous terminals (including screens, bar code readers, POS terminals, etc.) to the network.

1. On the **IOCOMM Main menu**, select **Serial ports configuration**.

2. Select the **serial port number** to which you have attached the terminal.

3. Select **Access options**.

4. Check that the **Available for outgoing services** field is selected and that authentication mode is set to **login authentication** or **No authentication**.

5. Select **Physical parameters**.

6. Enter the appropriate terminal type in the **Terminal type** field.

7. In the **Baud rate** field, select the down arrow and choose the appropriate setting for the attached terminal.

8. In the **Attached device** field, select the down arrow and then select **Asynchronous terminal**.

9. Select **Expert**.

10. Set **Character framing** to match that of your terminal by selecting the down arrow and then choosing the appropriate setting.
11. An **Inactivity timeout** may also be set in the same way.
12. If required, select the appropriate box(es) for **Special wiring**.
13. Select additional **port numbers** if you wish to connect similar terminals to these ports
14. Select **Check here to reset port and make changes immediate**.
15. Select **Submit**.
16. Select **Return to the Main menu**.

The port is now set up for the terminal; try to log in.

Configuring the Synchronous Port (B)

Port B can be set up to operate as either a synchronous port for fixed links, or an asynchronous port for dialled links. X.21, V.35 or V.24 (RS-232) links are supported. The access server automatically selects the physical interface according to the adapter cable that is connected.

Synchronous operation

Synchronous operation uses PPP over a fixed link between two networks. Before selecting synchronous operation on the Serial ports configuration page, you first need to complete fields on the Remote Sites configuration page.

1. From the **IOCOMM Main menu**, select **Remote sites configuration** and then select **Create new entry**.
2. Select the button towards the bottom of the page, to set **Current port mode** to **Synchronous**. This will cause the message **Limiting configuration to port B** to be displayed and the removal of the port table.

3. In the **Remote host name** text field, enter the name of a host on the network that will be reached via the fixed link. Make a note of this name; it also needs to be entered on the **Serial ports configuration** page.

   A description for the connection can be entered in the **Description** field if required (this entry is text only and has no operational effect). The **Telephone number** and **Inactivity timeout** fields are ignored when synchronous operation is selected.

   ```
   Remote host name      [ ] (this is a key field)
   Description           [ ]
   Telephone number      [ ]
   Inactivity timeout    [ ]
   ```

Note: The **Current connection type** selection field is ignored when synchronous operation is selected.

Current connection type is:

● PPP

○ PPP (with Van Jacobson compression)

○ SLIP

○ CSLIP (SLIP with TCP header compression)

```
Peer ID (username)          [ ]
Secret (password)           [ ]
Local IP address            [ ]
Remote host’s IP address    [ ]
Remote host’s IP netmask    [ ]
```

4. In the **Local IP address** field, enter the **IP address** of this IOCOMM. If you leave the field blank, the entry will default to the IP address detected at start-up. You can enter a different IP address to that of the unit (for example, where the remote end needs to talk to a specific or pre-defined IP address).

5. In the **Remote host's IP address** field, enter the appropriate **IP address.**

6. In the **Remote host's IP netmask** field, enter the appropriate netmask value. If no value is entered in the netmask field, the IOCOMM will default to a netmask appropriate to the remote host (i.e. a class A, B or C mask).

   In synchronous operation, the **Current authentication** selection is ignored and **PPP** is used as default.

7. When you have checked your entries on this page, select **Submit** to confirm. The **Remote sites configuration Entry** page will then be displayed and the name of the **Remote site** you have just configured should be listed.

8. Select **Return to the main menu**.

9. Select **Serial ports configuration**.

10. Click on **Port B** to enable the selection.

    Note: Synchronous operation is available on Port B only.

11. Select **Physical parameters**,

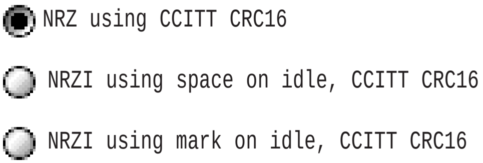
12. Select **new mode:**, select **Synchronous**.

    The **Description** field defaults to **Synchronous WAN interface** for synchronous operation. This is for information only.

13. In the **Remote site** field, enter the name as configured on the **Remote sites configuration** page.

14. Select **Expert** to display the **Physical parameters** expert options.

15. Select the appropriate **Encoding method** from the list shown (default is the first entry, which is the most common encoding method used for synchronous PPP):



● NRZ using CCITT CRC16

○ NRZI using space on idle, CCITT CRC16

○ NRZI using mark on idle, CCITT CRC16

Check with your leased line provider on
DSU/CSU setup

Special wiring options are not required for synchronous operation.

16. Select **Check here to reset port and make changes immediate** if you wish the new settings to be effective immediately.

17. Select **Submit** to confirm.

18. Select **Return to the main menu**.

Printing

Adding a printer (LPD printing)

The access server supports LPD printing from network hosts to a printer connected to a serial port.

1. Use a cable as specified in **Connectors and Cabling**.

2. On the **IOCOMM Main menu** page, select **Serial ports configuration**.

3. Select the **port number** to which you have attached the printer.

4. Select **Access options**.

   Note: The **Description** field is for information only.

5. Check that **Available for outgoing services** is selected.

6. Select **No Access**.

7. Select Physical parameters.

   Note: The **Terminal type** field is for information only and is not relevant for printing.

8. In the **Attached device** field, select the down arrow and then choose Printer.

   Note: You can copy this printer configuration to other ports by selecting the port number in the port list at the bottom of the page.

9. In the **Baud rate** field, select the down arrow and then select the appropriate baud rate from the list provided.

10. Select the **Expert** button.

11. Set Character framing to match the settings for your printer by selecting the down arrow and then selecting the appropriate setting. The **Inactivity timeout** should be set to **No timeout**.

12. Select **Check here to reset port and make changes immediate**.

13. Select **Submit**; you will be returned to the **Serial ports configuration** main page.

14. Select **Return to the Main menu**.

15. Select **Global configuration** and then **LPD printer groups**.

16. Ensure that the **Enable LPD** box is checked.

17. If you wish to use a generic print name such as port1, check the **Enable generic printer names** box.

If you use a generic print name you do not have to create an entry for a new LPD printer group. However, you can select **Enable generic printer names** and create an LPD printer group entry.

18. If you wish to create a new LPD printer group entry, select **Create new entry**. If not, go to item 23.
19. Select the box(es) for **Enable LF to CR-LF mapping** and **Enable trailing Form Feed** to activate if you require these options. For an alternative method of enabling these functions see **Configuring LPD**.
20. Enter the printer group name in the **Printer group name** field (e.g. `hp_print`).
21. Enter the **printer group description** in the **Description field** (e.g. `sales laserjet pr`).
22. Select the **port number** to which the printer is attached (as entered in item 3).
23. Select **Submit**.
24. Select **Return to the Main menu**.
25. The port is now set up. Send a print job to the IOCOMM to test printing.

If you experience problems, re-check the settings you have made and also refer to **Troubleshooting**.

Configuring LPD

There are two methods of printing from the IOCOMM; LPD and iocommd. LPD is the recommended method, however, this will depend on your application and operating system.

LPD is the Line Printer Daemon protocol supported by most operating systems including Windows® and Unix. Check our FTP site for an LPR spooler for Windows® 95.

The client is the machine that contains the file to be printed and may be running one of a range of operating systems and applications. The client must support LPD. Unix systems normally include a version of LPD and there are a number of TCP/IP applications for DOS/Windows® that also support LPD.

When printing via LPD the client refers to the printer by IP address (or the name associated with this address from the Host table) and printer name or queue name. This may take one of three forms:

- The printer name as set in the **Printer group name** field of the **LPD printer group** menu.

  More than one serial port may have the same name allowing the IOCOMM to create a hunt group of printers. The first available port to match that queue name will receive the print job.

- The name of the IOCOMM and no queue name or port number.

  This will cause the print job to be printed on the first available LPD port on the IOCOMM of this name. The **Printer group name** field in the **LPD printer group** menu does not need to be set.

- The name of the IOCOMM followed by a port number.

For example if the queue name is `server_name9` (or `server_name09`) then serial port 9 will receive the print job. The **Printer group name** field in the **LPD printer group** menu does not need to be set.

Note: There is a maximum limit of 15 LPD connections per access server, which may be distributed to all of the available LPD ports as required. If the maximum is exceeded then the request is rejected and the connection is closed.

At present it is possible to print from Windows® 3.11 or DOS, although this will normally be accomplished via a separate application program like PC/TCP or Netmanage Chameleon. Windows® NT has a built-in LPD utility, and there are shareware packages on the Internet for Windows® 95 (check our FTP site).

LPD may be used to connect a printer that will be shared between both Windows® and Unix machines.

The actual printer will be referenced by the name of the IOCOMM serial port or, by the IOCOMM and port number.

Hunt groups are supported by the access server. To use this facility, you must specify the same print/queue name in the Unix string (e.g. laser1) as set in the **Printer group name** field in the **LPD printer groups** option (under **Global configuration** on the **IOCOMM Main menu)**.

The Unix host should have a printer database, for BSD type systems this will be the file /etc/printcap and there should be an entry within this file for the server's LPD port that looks something like the following example (shown with no trailers being used):

```
lp|Laser Printer:\
:lp=:rm=accs_serv:rp=laser1:sh:sf:mx#0:\
:sd=/var/spool/output/laser1:lf=/var/log/lpd-laser1-errs:
```

Printing could then be accomplished using the following command:

```
lpr -Plp <file>
```

A limitation of printing with LPD on the IOCOMM is that no formatting of text can be carried out by the IOCOMM firmware. This is due to the lack of a spooler utility in the IOCOMM and the data being forwarded directly to the serial port.

To overcome this, the local host must perform all of the necessary processing.

Note: The **IOCOMM LPD printer group** page on the IOCOMM web browser, enables you to map line feed to carriage return-line feed (LF to CR-LF) and enable form feed. If these options are enabled in the web browser, these attributes will apply to all print jobs. There are two ways to disable these attributes; one is to un-select the setting in the web browser page, the other is to use the raw trailer in the print command, as detailed below. If only some of your print jobs require these functions to be enabled, you have the option of leaving the browser set-up disabled and adding a trailer switch in the print command to set these options on a job-by-job basis.

For example, to force form feed on a particular print job, you could change the first print command example shown, to include the form feed trailer as shown below:

```
lp1|Laser Printer:\
:lp=:rm=accs_serv:rp=laser1_ff:sh:sf:mx#0:\
:sd=/var/spool/output/laser1_ff:lf=/var/log/lpd-laser1-errs:
```

As an alternative, the following + trailer can be used to set form feed:

```
lp2|Laser Printer:\
:lp=:rm=accs_serv:rp=laser1+:sh:sf:mx#0:\
:sd=/var/spool/output/laser1+:lf=/var/log/lpd-laser1-errs:
```

In the same way, you can set LF to CR-LF, as shown in the example below:

```
lp3|Laser Printer:\
:lp=:rm=accs_serv:rp=laser1_onlcr:sh:sf:mx#0:\
:sd=/var/spool/output/laser1_onlcr:lf=/var/log/lpd-laser1-errs:
```

Finally, you can set both form feed and LF to CR-LF as shown in the following example:

```
lp4|Laser Printer:\
:lp=:rm=accs_serv:rp=laser1_ffonlcr:sh:sf:mx#0:\
:sd=/var/spool/output/laser1_ffonlcr:lf=/var/log/lpd-laser1-errs:
```

Notes: The trailer switch can be specified in either lower case or caps, but generally, you should not mix the two. You can use **ff** and **onlcr** trailers in the same statement (as shown in the above example), but you cannot use the **+** and **onlcr** in the same statement.

Regardless of what settings you have selected in the **IOCOMM LPD printer group** page, you are able to output data in **raw** form (i.e. no form feed, LF to CR-LF or other formatting) by using the text `raw` in the printer command as shown in the following example.

```
lp5|Laser Printer:\
:lp=:rm=accs_serv:rp=laser1_raw:sh:sf:mx#0:\
:sd=/var/spool/output/laser1_raw:lf=/var/log/lpd-laser1-errs:
```

If filtering or formatting is required then a local linking print queue needs to be created. This would be something like the following:

```
# Local queue to link to accs_serv lpd Printer on port 16
link? 9 laser1| IOCOMM lpd Printer 16:\
:lp=/dev/null:sf:sd=/usr/spool/lpd/laser1:\
:lf=/usr/spool/lpd/lpd_printer/log:of=/etc/IOCOMM/ link-laser1:
```

The shell script output file `link-laser1` has the contents:

```
#!/bin/sh
lpr -Plp3
```

This would be sufficient to print a header page and perform form feeds.

If a specialised filter program is required for something like a plotter, the script may be similar to:

```
#!/bin/sh
/usr/local/filter "$@" | lpr -Plp3
```

Configuring iocommd

The Chase supplied iocommd provides a pseudo TTY interface to Unix print spoolers. This software and the binaries associated with it are available on the CD provided with the IOCOMM or from any Chase web site.

If your system cannot use LPD for printing, then it is suggested you use the Chase supplied utilities. The iocommd utility supplied by Chase can be used for Unix printing only. Iocommd is a Unix tty port redirector.

Note: Some Unix systems may require Transport Layer Interface (TLI) to be fully implemented for iocommd print jobs to complete successfully.

Printing configuration can be carried out on the IOCOMM from a Web browser as follows:

1. On the **IOCOMM Main menu** page, select **Serial ports configuration**.

2. Select the **port number** to which you have attached the printer.

3. Select **Access options**.

   Note: The **Description** field is for information only.

4. Check that the **Available for outgoing services** field is selected.

5. Select Physical parameters.

   Note: The Terminal type field is for information only.

6. In the **Baud rate** field, select the down arrow and then select the appropriate baud rate from the list provided.

7. In the **Attached device** field, select the down arrow and then select the Printer option.

8. Select **Expert**.

9. Set **Character framing** to match the flow control requirements of your printer by selecting the down arrow and then selecting the appropriate setting. An **Inactivity timeout** can also be set in the same way. If required, select the appropriate box(s) for **Special wiring**.

10. Select **Check here to reset port and make changes immediate**.

    Note: At this point, it is advisable to make a note of the settings chosen. Print the browser page for future reference.

11. Select **Submit**. You will be returned to the **Serial ports configuration** main page

12. Select **Return to the Main menu**.

13. On the **IOCOMM Main menu** page, select **Outbound services configuration**.

14. Select **Create new entry**.

15. Enter the print queue file name in the **Service name** field (e.g. `HP_laserjet`). This can be any name you wish to assign, but must be one continuous string (no spaces).

16. Enter the **print queue description** in the **Description** field. This can be any description you wish to assign and can include spaces.

17. In the **TCP port** field enter an appropriate **port number**. This can be any unused number in the range 10001 to 65535.

18. Select to activate/deactivate as required in the **Configuration option** fields.

    □ **Full carrier indication required**
    This waits to see a carrier detect signal.

    □ **Output translation: map LF to CR-LF**
    This maps new line to carriage return/new line.

    □ **Output only: ignore input from port**
    This ignores all input signals from the port.

19. Select the **port number** to which the printer is attached.

    Note: This should be the same **port number** as set in the **Serial ports configuration** men item 2.

20. Select **Submit**.

21. Select **Return to the Main menu**.

On the host side:

If you are already familiar with iocommd, all you have to do for the above configuration is create the following file:

```
# iocommd -P (server name) 10006 (device name)
```

This will start the iocommd process and create a device in /dev. If you are not familiar with the iocommd program see the *iocommd* section for more details.

Configuring RADIUS

RADIUS is a client /server system allowing access servers (clients) to exchange authentication and accounting information with database servers.

IOCOMM RADIUS client

1. On the **IOCOMM Main menu**, select **Global configuration**.
2. Select **RADIUS**.
3. Select **Enable RADIUS authentication**.

   Note: Without this option selected, other settings will have no effect except **Enable special login prefix recognition**.
4. Select **Enable RADIUS accounting** if you require the accounting function.
5. Select **Enable special login prefix recognition** if required. This allows login names prefixed with P or S to request PPP or SLIP services respectively.

   Note: Any user login that starts with a capital P or capital S will not work. The IOCOMM assumes that the leading P or S is a request for either a PPP or SLIP service and that the remainder of the text is the login name, so a login such as `Peter` would request PPP but leave a login name of `eter` which would not be recognised.
6. For the **First server**, in the **Host name** field, enter the name or IP address of the host running the RADIUS server.
7. For the **First server**, in the **Shared secre**t field, enter the shared secret string. The server requires that the string be matched to that specified for the IOCOMM in the clients file on the RADIUS server for the login to succeed.

8. Select the logical network ports (UDP ports) by choosing one of the following options

This uses the port numbers specified in the RADIUS draft standard. This remains selected as the default port.

This uses port numbers specified by the RADIUS RFCs 2138 & 2139.

This allows you to set your own port numbers.

9. Select the **Expert** button, which provides further administration settings, allowing you to set the number of retries and time-out values.

10. Enter the appropriate values in the following fields:

```
Re-send to server after      [6 seconds ]
```

(This sets the time-out value)

```
Number of attempts           [3 ]
```

(This sets the number of attempts)

11. Repeat for the **Second server** and **Third server** if required.

Note: These servers are used as backup units.

12. Select **Submit**.

13. Select **Return to the Main menu**.

Note: If RADIUS authenticates a user but does not come back with a service, the connection is auto-terminated and a syslog entry is generated. If there is no authentication, the default command will be run (e.g. `shell`).

RADIUS server on Unix

Exact operation will depend on which vendor's RADIUS server is being used. The basic steps are:

1. Install the software, if necessary.
2. Add the IOCOMM to the clients file.

   This file contains one line for each access server allowed to use the RADIUS server. Each line contains **Name** and **Shared secret** which must match those configured on the relevant access server.
3. Add the dial-in users to the users file.

   The format of this file is broadly similar between vendors, but there may be some differences. Refer to the vendor's instructions.
4. Restart the server, if required.

RADIUS server on Windows® NT

The method employed for configuring RADIUS on a Windows® NT server will depend upon the particular version of RADIUS used. Consult the vendor's documentation.

Adding User to RADIUS system

Users must be added to a RADIUS server's database in order for them to be authenticated. This procedure depends upon the RADIUS server being used. Consult the documentation provided.

RADIUS Accounting

The procedure for configuring RADIUS accounting on the IOCOMM is as follows:

1. On the **IOCOMM Main menu**, select **Global configuration**.
2. Select the **RADIUS** option.
3. Check that at least one RADIUS Server is specified on this page (i.e. the **First server** section is filled in), and the **Enable RADIUS authentication** option is already selected.
4. Select **Enable RADIUS accounting**. This option allows you to use the accounting function.
5. Select **Submit**. The IOCOMM will now send accounting information to a RADIUS server.
6. Select **Return to the Main menu** .

Note: If you have not already done so, the RADIUS server will need to be instructed to maintain a log of accounting information sent to it.

Setting the IP address of the IOCOMM for PPP and SLIP

When configuring a user for Framed access (PPP or SLIP) on a RADIUS server it may be necessary to specify the IP address of the IOCOMM as one of the reply items. Because standard RADIUS doesn't provide this facility it is done by using vendor-specific attribute 224, namely Framed-NAS-Address. To add this capability it will be necessary to edit the RADIUS server's dictionary file to include a line similar to the following (see the documentation with your RADIUS server for details of the correct syntax):

```
ATTRIBUTE    Framed-NAS-Address  224    ipaddr
```

After the dictionary file has been edited it may be necessary to restart the RADIUS server for the changes to take effect.

Once this has been done the Framed-NAS-Address attribute can be used in the reply items section of a user entry in the RADIUS users file, for example:

```
fred   Password = “basingstoke”
       Service-Type = Framed-User,

       Framed-Protocol = PPP,
       Framed-IP-Address = 10.0.0.6,
       Framed-IP-Netmask = 255.0.0.0,
       Framed-NAS-Address = 10.0.0.7,
       Framed-Routing = None
```

Interpreting IOCOMM port numbers on a RADIUS server

Because the RADIUS NAS-Port attribute is an integer, and the IOCOMM uses letters as well as numbers for its ports, there is a discrepancy between the IOCOMM's port numbers and the values actually sent to the RADIUS server. This means that port values appearing on the RADIUS server, for example in the accounting information, will differ as follows:

IOCOMM port	**port value shown on RADIUS server**
LAN	0
A	1
B	2
1	3
2	4
3	5
....	....
16	18

In order to make the port values displayed by the RADIUS server match the true IOCOMM port values it is necessary to edit the dictionary file to include a section to translate the NAS-Port values.

The following is an example (see the documentation with your RADIUS server for details of the correct syntax):

```
#                 IOCOMM Port  NAS-Port Value
#                 -----------  --------------
VALUE    NAS-Port     LAN            0
VALUE    NAS-Port     A              1
VALUE    NAS-Port     B              2
VALUE    NAS-Port     1              3
VALUE    NAS-Port     2              4
VALUE    NAS-Port     3              5
VALUE    NAS-Port     4              6
VALUE    NAS-Port     5              7
VALUE    NAS-Port     6              8
VALUE    NAS-Port     7              9
VALUE    NAS-Port     8              10
VALUE    NAS-Port     9              11
VALUE    NAS-Port     10             12
VALUE    NAS-Port     11             13
VALUE    NAS-Port     12             14
VALUE    NAS-Port     13             15
VALUE    NAS-Port     14             16
VALUE    NAS-Port     15             17
VALUE    NAS-Port     16             18
```

After the dictionary file has been edited it may be necessary to restart the RADIUS server for the changes to take effect.

Local Authentication

Local authentication is intended for use when no RADIUS server is available. Using RADIUS for authentication is the preferred method.

Configuring Local Authentication

The setting up of local authentication is carried out as follows:

1. On the **IOCOMM Main menu** page, select **Global configuration**.
2. Select the **RADIUS** option.
3. Uncheck **Enable RADIUS authentication**.

   Note: To enable local authentication you must first disable **RADIUS authentication**.
4. Select **Submit**.
5. Select **Return to the Main menu**.

Setting Up a User

Proceed as follows:

1. On the **IOCOMM Main menu** page, select **Global configuration**.
2. Select **Local authentication**.
3. Select **Create new entry**.
4. Complete the following fields:

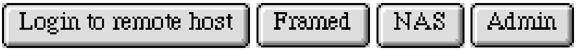
`User ID`	[ ]	The user's IOCOMM login.
`Description`	[ ]	
`User password`	[ ]	Password corresponding to login.

   Note: The Local authentication password has no minimum number of characters and will be truncated to a maximum of 40 characters.

   Note: If you wish to set the **Enable special login prefix recognition** to be active on the **IOCOMM RADIUS** page, you should avoid using either a capital P or capital S at the start of the user login (User I.D.). See **RADIUS Client on IOCOMM** for further details.

Service configuration

5. Select the required Service from the following options:

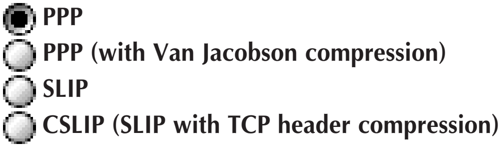


Selecting **Login to remote host** will present you with login protocol options.

6. Choose either **Telnet** or **Rlogin**. Your chosen configuration and protocol will then be displayed.

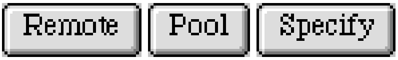
7. Selecting **Framed** will present you with a further set of options; select one option:

Framed protocol provided



● **PPP**
○ **PPP (with Van Jacobson compression)**
○ **SLIP**
○ **CSLIP (SLIP with TCP header compression)**

8. You then need to select the address resolution method from one of the following:



If you select either **Remote** or **Pool**, your current settings are displayed.

9. If you selected **Specify**, you are presented with an additional form (as shown below). Complete the form as appropriate.

Select addresses to use:

```
Local IP address      [ ]
Remote IP address     [ ]
Remote IP netmask     [ ]
```

10. Selecting **NAS** or **Admin** offers no further options.

11. Select **Submit**.

    Note: Local authentication will automatically be used.

12. Select **Return to the Main menu**.

Note: If RADIUS authentication is later enabled, the local authentication list remains but is not used.

Dynamic Routing (RIP)

RIP (Routing Information Protocol) is a protocol for exchange of routing information among gateways (routers) and hosts.

RIP is also used to advertise routes known to the IOCOMM.

Enabling RIP listening / advertising

To enable RIP:

1. On the **IOCOMM Main menu** page select **Global configuration**.

2. Select **Dynamic routing**.

3. Select one of the following options:

   ● **Enable RIP listening only**

   If you do not wish to advertise known routes, but would like to receive information from other routers.

   ○ **Enable RIP listening and advertising**

   If you wish to advertise location details of your LAN and hosts, and also would like to receive information from other routers.

   ○ **Disable RIP**

   If you do not wish to advertise or receive.

4. Select the type of RIP protocol to be used.

   ● **RIP Version 1 only**
   A simpler version needing no password for authentication.

   ○ **RIP Version 2**
   A more advanced version needing a password for authentication.

   Select whatever is compatible with your network

5. If you select RIP Version , enter the **RIP Version 2 authentication password**.

6. Select **Submit**.

7. Select **Return to the main menu**.

8. Re-boot the IOCOMM to make the change to the RIP version effective.

Enabling RIP2 authentication

RIP Version 2 is a more advanced utility needing password authentication for security. It also imposes subnet masks that enable the unit to broadcast to a specific subnet only instead of to all parts of the system.

To enable a RIP Version 2 function, proceed as follows:

1. On the **IOCOMM Main menu** page select **Global configuration** and then **Dynamic routing**.

2. Select one of the following options (as in the previous section).

   ● **Enable RIP listening only**

   ○ **Enable RIP listening and advertising**

   ○ **Disable RIP**

3. Select **RIP Version 2** as the RIP protocol to be used.
4. Enter the **RIP Version 2 authentication password**.
5. Select **Submit**.
6. Select **Return to the main menu**.

Enabling TCP Security

If you wish to deny access to the IOCOMM by certain hosts on the LAN or sub-nets of the LAN, proceed as follows:

1. On the **IOCOMM Main menu** page, select **Global configuration**.
2. Select **TCP security**.
3. In **First permitted IP addresses** enter the **Mask value** and **Mask result** for the host(s) on the LAN or the sub-nets that will be permitted access to the IOCOMM

   Example: To allow access for a single IP address, set:

   ```
   Mask value      [0xFFFFFF ]
   Mask result     [ ] Desired IP address of device
   ```

4. Repeat step 3 for the Second and Third entries (if required).
5. Select **Submit**.
6. Select **Return to the Main menu**.
7. Re-boot the IOCOMM to make the change to TCP security effective.

Note: If access is attempted to the IOCOMM via a proxy server, the connection will fail unless the proxy server is also entered. If the IP address of the proxy server is entered, any connection attempted via that proxy will be accepted. This has potential security implications.

Global Messages

There are two types of messages that can be displayed for users of the IOCOMM. One is a **Login banner**, the other is **Message of the Day**. The **Login banner** can be used to inform administrators of the location of the unit and its details. The information is also available on the Web page and via SNMP.

To set up this message facility follow the procedure below:

1. On the **IOCOMM Main menu** page, select **Global configuration**.

2. Select the **Global messages** option.

   The **Global messages** page allows you to enter any information that you feel would be relevant or useful to users of the IOCOMM in the **Login banner** and **Message of the day** fields.

   For example, the **Login banner** might say *Welcome to the XYZ network*. The **Message of the day** might say *Network unavailable after 4pm today*. Either message can be changed as and when required.

3. Complete the text fields for **Login banner** and **Message of the day** as required.

   Note: TFTP paths to message files are also acceptable.

4. You also have the option of entering general system information in the following fields; for example:

```
Support contact [John_Brown]
System description    [Access_Server_03]
System location [Accounts_Department]
```

   This information may be useful from a general network administration point of view. The information you enter in these fields will appear on the IOCOMM Administration page each time the Web browser for the IOCOMM is opened.

5. The Support contact line can also be used to create an e-mail shortcut, enabling email messages to be sent directly to the relevant support person (either internally or externally). To use this facility, complete the field using the same form as in the following example:

   ```
   Support contact  [mailto:john.brown@anycompany.co.uk]
   ```

   The e-mail shortcut can then be used by clicking on the mail address line shown on the **IOCOMM Administration** page. The e-mail address can be changed at any time.

   Note: The **Product ID** and **Serial number** are factory pre-set and cannot be changed.

6. Select **Submit**.

7. Select **Return to the Main menu**.

Configuring Status Logging

syslog (Event logging)

The quantity of operational information logged by the access server and the location used to store this information is configurable.

1. On the **IOCOMM Main menu** page, select **Global configuration** then **Event logging**.

   ```
   Minimum level to log to console     [debug ]
   ```
   Displays on console on port A.

   ```
   Minimum level to log to buffer      [debug ]
   ```
   Stores log in internal buffer.

   ```
   Minimum level to log to remote host  [No logging ]
   ```
   Logs events in syslog on remote host.

These allow you to select where the event logging is stored or displayed and the level of event log you wish to capture (this sets the quantity of information).

2. Select the level of event logging for each destination.

   To view the event log level for each destination, select the down arrow. If you select **No logging**, no event logs will be stored to this destination. If you select any other level, all levels including the one you have selected and above will be logged. For example, if you select **notice**, all events from **emergency** down to **notice** will be logged. Repeat this selection for the three destinations. If you wish, you can direct event logs to all three destinations, i.e. **console**, **buffer** and **remote host**.

   Note: The IOCOMM internal buffer holds only the last 100 event logs, so it may also be wise to write logs to the console or remote host (or both).

   The event logs saved to buffer or console will only display the correct date and time if a remote host has also been specified (even if **No logging** has been set for the remote host).

   The event logs written to the IOCOMM buffer can be viewed by using either the command `syslog display [number]` in CLI mode or by using the IOCOMM Web browser pages (from the **Main menu**, select **Status and statistics display**, then **Event logging**, then **System log**).

   Note: If the IOCOMM is switched off or re-booted, all event logs held in the internal buffer will be lost.

```
Remote syslog host                [ ]
Remote host facility to map to    [NONE ]
```

3. To write logs to a remote host, enter either the host name or IP address for the host in the **Remote syslog host** box. Event logs can be viewed on the selected remote host using the standard syslog command.

   Note: For this option to function correctly with a host name, DNS must be correctly configured. If DNS is not correctly configured, only the IP address entry can be used.

4. You are also able to set up a special facility on the remote host to capture event logs to specific locations. For example, you could select **local 3** as the facility for capturing event logs from the IOCOMM in a particular department or office. Or, you could set up a log facility for each individual IOCOMM.

5. Select **Submit**. You are returned to the **IOCOMM Global configuration** page.

6. Select **Return to the main menu**.

Configuring SNMP

1. On the **IOCOMM Main menu** page, select **Global configuration**.

2. Select **SNMP**.

3. If you wish to use an SNMP manager, select **Enable SNMP access**.

4. You have the option of entering general system information in the following fields; for example:

```
Support contact       [John_Brown]
System description    [Access_Server_03]
System location       [Accounts_Department]
```

This information may be useful from a general network administration point of view. The information you enter in these fields will appear on the **IOCOMM Administration** page each time the web browser for the IOCOMM is opened.

The **Support contact** line can also be used to create an e-mail shortcut, enabling e-mail messages to be sent directly to the relevant support person (either internally or externally). To use this facility, complete the box using the same form as the following example:

```
Support contact  [mailto:john.brown@anycompany.co.uk]
```

The email shortcut can then be used by clicking on the mail address line shown on the **IOCOMM Administration** page. The email address can be changed at any time.

5. If you require SNMP traps, select **Enable SNMP** traps.

```
IP address               [ ]
Community name           [ ]
```

6. Enter the **Community name** and **IP Address** for up to three trap settings as required.

   Note: The **Community name** (password) required for SNMP write access is the **admin** password.

   Selecting the **Expert** option allows you to specify a **Port number** for the SNMP traps (the factory default is 162).

7. Select **Submit**. Your changes will be saved and you will be returned to the **Global configuration** page.

8. Select **Return to the main menu**.

Configuring SNMP traps

1. On the **IOCOMM Main menu** page, select **Global configuration**.

2. Select **SNMP**.

3. To set SNMP traps, select **Enable SNMP traps**.

   ```
   IP address              [ ]
   Community name          [ ]
   ```

4. Enter the **Community name** and **IP Address** for up to three trap settings as required.

   Selecting the **Expert** option provides a further administration setting and enables you to specify a **Port number** for the SNMP traps (the default SNMP port number is 162).

5. Select **Submit**. You will be returned to the **Global configuration** page.

6. Select **Return to the main menu**.

Telnet Service (telnetd)

1. On the **IOCOMM Main menu** page, select **Global configuration**.

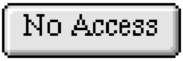
2. Select **Network CLI service (telnetd)**.

3. Select **Enable telnetd**. This option allows or disallows an external user to operate a telnet connection to the IOCOMM.

4. If required, select **Display login banner**.

5. If required, select **Display message of the day**.

6. Select the type of **authentication mode** from the following:



This disallows any access to the IOCOMM via a telnet connection.

This asks for the password when a user attempts a telnet connection to the IOCOMM.

This removes the need for authentication and no password will be asked for when a user attempts a telnet connection to the IOCOMM.

The selected authentication method will be displayed on the page to verify your choice.

7. Select the **Expert** option for further administration settings, including:

```
TCP port [23 ]
```

8. This option defaults to port 23 (normal Telnet port).

When using the default port number for telnet, the port number does not need to be specified when making the telnet connection. However, if you have changed the port number, you will need to specify it when issuing the telnet command. For example, to telnet to an IOCOMM called jaguar with a new port number of 45, the command would be:

```
telnet jaguar 45.
```

Granted capabilities

9. The items under Granted capabilities, specify the local and remote access capability to the telnetd service.

Select boxes as required.

☒ **Login (to remote host)**
This allows users to make an ongoing connection from the IOCOMM using telnet or rlogin.

☒ **Framed access (PPP or SLIP connections)**
This allows users to run PPP or SLIP protocols on the IOCOMM.

☒ **NAS (Command Line Interface)**
Network Access Server (NAS) enables access to the CLI with non-admin (user level) commands.

☒ **Admin**
This enables access to the CLI with a full set of administration commands.

```
Default command [shell ]
```

The **Default command** field defines what happens when the login sequence completes successfully and `shell` will be most commonly used.

The `shell` (default) command presents the user with a Command Line Interface from which they can run any command for which they have granted access.

Example: To make an automatic connection to a specific host, the following could be used:

```
  rlogin -1 newuser signup.my.domain
```

10. To change the default command, delete existing text and type in your new entry.

11. Select **Submit**.

12. Select **Return to the main menu**.

Monitoring Status

Using the CLI

A command line interface can be configured to be available from every serial port and to remotely connected users.

CLI Line Editing

The command line interface allows the entry of single line commands for execution by the access server.

CLI Prompt

The CLI prompts for each line of input with a prompt consisting of the assigned host name followed by the character '>' if the user is unprivileged and '#' if the user has administrative permissions and finally a single space.

Echo and Line Edit

The backspace and delete characters (^H and ^?) cause the last character in the line buffer to be removed.

The carriage return, line feed or nul character is accepted as terminating the line.

The ^U character abandons the current input buffer, echoes `CR-LF` and issues a new prompt.

^C abandons any accumulated input but may also be used to force early termination of commands.

The maximum input line length is 120 characters.

Commands and syntax details

A full list of the commands and switches is given in **Command Line Interface**.

Using finger

The `finger` utility can be used to invoke commands on the IOCOMM. The `finger` protocol service is provided on TCP network port 79.

The following CLI statistics commands may be invoked via the fingerd daemon using the username / command field to specify the command. The output from the command is returned as a result of `finger`. Optional flags may be provided to some commands by appending a '-' character and the flags to the name; these are shown as -xxx in the following list.

Name	**CLI command**
<none>	`pstatus -q`
arp	`arp -a`
except	`except`
lookmem	`lookmem`
lookstream	`lookstream`
netstat-xxx	`netstat -xxx`
pppstats	`pppstats`
ps	`ps`
pstatus-xxx	`pstatus -xxx`
syslog	`syslog disp`

For example, enter the command:

```
finger netstat-a@myiocomm
```

where, `myiocomm` is the unit's name (can also be the IP address)

Using SNMP

The IOCOMM has SNMP support which allows local or remote administration of configuration, performance monitoring, fault tracking and diagnosis, accounting and security. The client machine should be running a suitable version of SNMP and requires a valid **password** and **IP address** to make the connection into the IOCOMM.

The community name required for SNMP write access on the IOCOMM is the administration password. For read access, the community name **public** is also supported.

Important Note: Any changes to the IOCOMM using the SNMP interface only affect the live configuration and are not reflected in the permanent store or the Web interface.

Making Changes to IOCOMM

Upgrading Firmware with BOOTP

The IOCOMM firmware can be upgraded at any stage to implement latest revisions. This procedure can be carried out from the IOCOMM's bootstrap menu. The procedure is as follows:

Note: You can download new firmware from a network server to the IOCOMM using TFTP. The process uses BOOTP on the network server and requires the correct IOCOMM settings and firmware file details to be present in the BOOTP configuration file. If the new firmware file is not on the BOOTP server, you will need to specify its location and file name in the BOOTP configuration file (**bootptab** under Unix) before proceeding as follows:

1. Connect a terminal to port A on the IOCOMM.

2. Power off the IOCOMM and then power on while holding in the TEST button to obtain the IOCOMM bootstrap menu. Then follow either step 3 or step 4 below, depending upon whether you wish to test the new firmware before writing it to FLASH.

3. To write the new firmware directly to FLASH, select option 7 from the bootstrap menu.

4. To test the new firmware before writing it to FLASH, copy it to RAM first.

5. To store the firmware in RAM, select option 6 from the bootstrap menu.

6. If the new firmware works correctly and produces the expected results, reload the firmware and write it directly to FLASH (as in step 3 above) for permanent use.

Note: Use of the bootstrap menus is detailed in the *Bootstrap* section.

Upgrading Firmware without BOOTP

If the network BOOTP server is not available at the time of downloading a new firmware file, you can still run the download manually using the IOCOMM bootstrap menu:

1. Connect a terminal to port A on the IOCOMM.

2. Power off the IOCOMM and then power on while holding in the **TEST** button. The IOCOMM bootstrap menu will appear on the terminal.

3. From the main bootstrap menu, select 6 to download to RAM or 7 to download to FLASH, then press ↵.

   When the IOCOMM detects that the BOOTP server is unavailable, the bootstrap menu prompts you to enter details of the network, IOCOMM and firmware file.

4. At the prompt **Ethernet interface**, select the option relevant to your network and press ↵.

5. For **Unit IP address**, enter the IOCOMM's IP address and press ↵.

6. For **Netmask**, enter the IP netmask for the IOCOMM and press ↵.

7. For **Boot host IP address**, enter the IP address for the network host where the download file is located and press ↵. If you enter a boot host address which is on a different network to the IOCOMM, go to step **9.**

8. At **Setup IP gateway ?**, enter y if you want to specify a gateway or n if you do not. If you entered n, go to step **10**.

9. For **Default gateway**, enter the gateway address and press ↵.

10. For **Boot file**, enter the name of the firmware file and press ↵.

The new firmware file will be downloaded to either RAM or FLASH (as selected in **3**. above).

Checking Firmware Upgrade

You can check firmware before permanently downloading it to FLASH.

1. Download the firmware as instructed in the previous section and store in RAM. This is a temporary measure.

2. Test that the new firmware works correctly and produces the expected results.

   If the new firmware works as expected;

3. Reload the firmware. Store in FLASH for permanent use.

Upgrading Firmware Remotely

The IOCOMM firmware can also be upgraded via the Web interface. This facility allows the administrator to download firmware to an IOCOMM without having to be at the same location as the unit and does not require a terminal connection. Remote Firmware Upgrade is available only on units running both firmware version 1.06 or later and bootstrap version 1.02 or later.

1. On the **IOCOMM Main menu** page, select **Special operations**.

2. Select **Remote Firmware Upgrade**.

3. In the **Download host** field, enter the IP address or name of the host system from which you want to download the firmware.

4. In the **Filename of download image** field, enter the tftp path and filename for the firmware file.

5. To download the new firmware to FLASH, select **Download to FLASH and then discard download parameters if the download is successful**. This option means that once the download has been successfully completed, the IOCOMM will revert to loading its firmware from FLASH on subsequent reboots.

6. To download the new firmware to RAM, select **Download to RAM and apply these download parameters on every power-up**. This option means that the firmware will be downloaded to RAM from the selected host each time the IOCOMM is rebooted.

7. Select **Submit** to save the parameters only. The download will then happen the next time the IOCOMM is rebooted. Alternatively, select **Submit and Reboot** to trigger the download immediately. During the reboot, the following will appear on screen:

```
Reset

The IOCOMM will now reset.

All connections will be dropped.

Will download firmware to FLASH

Please wait for 4 minutes and then
reconnect to the IOCOMM.
```

Note: When the IOCOMM is being re-booted, the Web browser connection is terminated.

8. Wait four minutes (two if loading to RAM), then on the browser re-enter your hostname or IP address to access the **IOCOMM Administration** page. If the download was successful, at the top of the page you will see the message:

```
RFU download to FLASH OK
```

Disabling Remote Firmware Upgrade

1. On the **IOCOMM Main menu** page, select **Special operations**.
2. Select **Remote Firmware Upgrade**.
3. Select **Download disabled**.
4. Select **Submit**.
5. Select **Return to the Main menu**.

Configuring TFTP Access on Unix

Note: Ensure that the TFTP daemon is running (enabled from `/etc/inetd.conf`).

There are 3 types of TFTP Access possible:

- Insecure TFTP, where files may be downloaded from anywhere on the file system: The full path of the file will be required.
- Secure TFTP, where files may only be downloaded from /tftpboot: The full pathname is required, i.e: / tftpboot/iocomm.dl.
- Secure TFTP, where files may only be downloaded from /tftpboot: Only the filename is required, i.e: iocomm.dl.

Note: Make sure that the firmware file on the server has correct read permissions, as if this is not the case the IOCOMM may not be able to read the file. To make the file readable, it may be necessary to execute the following command:

```
    chmod +r iocomm.dl
```

Configuring TFTP Access on Windows® NT

The method employed for configuring TFTP on a Windows® NT server will depend upon the particular version of TFTP used. Check the vendor's documentation.

Saving / Copying Configuration File

This procedure allows you to save an IOCOMM's configuration to a network host. This information can be used as a back-up in case the configuration information is lost from the IOCOMM, or it can be read back to a second unit, giving the second IOCOMM the same configuration as the first. This procedure can be useful where you require subsequent IOCOMMs to have the same or similar configuration.

The one parameter that *must* be changed when copying configuration files is the IP address, which must not be duplicated. There are two ways of dealing with the required change to the IP address for the configuration file.

- You can copy the configuration file completely (including the IP address) and then edit the configuration file on the remote host before copying it to the new IOCOMM. To use this method, follow the instructions from 3 to 8 below.
- You can blank the IP address field on the browser page of the current IOCOMM before you copy the configuration file, in which case it can be read to the new unit without the need to manually edit the file. This option is the easier and preferred method. To use this method, follow the instructions from 1 to 9 below.

1. On the **IOCOMM Main menu** page, select **Global configuration**, then **LAN interface**.

2. The **IP address** is shown in the top box. Highlight the IP address and delete text to blank the field. Select **Submit** to confirm the change.

3. Select **Return to the main menu**.

4. On the **IOCOMM Main menu** page, select **Special operations**.

5. Select **Read or write configuration**.

   The **Read or write configuration** page allows you to copy the complete configuration information from the current IOCOMM to a file on a remote host.

   Before proceeding with this operation, you should first create a file on the target system (remote host) with the name you require for the configuration file.

   Ideally, the file should have zero contents (an example is given below):

   ```
   /usr/tftpboot/access_server1.db
   ```

6. In the **Name or IP address of host** field, enter the IP address or host name for the target system (to which you want to copy the configuration file).

7. In the **Configuration file name** field, enter the full path and filename for the configuration file.

   You should have already created the file to which you want to copy the configuration.

8. Select **Write configuration to host**. The file will then be copied to the selected remote host and the following will appear on the page:

```
~~~~~~~~~~~~~~
Writing file /etc/tftpboot/access_server1.db
To remote host hostname or IP address
~~~~~~~~~~~~~~
```

9. When the file has been successfully copied, the two page links at the bottom of the current page will be re-displayed. If there is an error while copying the file, the following message will be displayed:

```
Transfer failed. Please check the parameters and try again
```

10. Check and if necessary re-enter the host name or IP address and file name, then re-submit the Write command.

    If the copy procedure fails continuously, re-check the host name (and that a correct DNS entry exists), IP address and directory / filename for the target file on the remote host and then re-submit the Write command.

11. When the operation is completed, select **Return to the main menu.**

12. Select **Global configuration**, then **LAN interface**.

13. Click the cursor in the IP address box, re-enter the unit’s IP address which you blanked in step 2. and then select **Submit** to confirm the change.

14. Select **Return to the main menu**.

The configuration including the IP address, for the IOCOMM you copied the configuration file from, should now be back to its original state.

Copying Configuration File to New Unit

This is the procedure to copy the IOCOMM’s configuration (file on remote host) to a second or subsequent IOCOMM unit.

Follow the instructions in the previous section to copy the required configuration file to a remote host, edit the file to change the IP address. If you chose to use this option, see Notes in the previous section and proceed as follows.

Note: You must have previously entered and saved the IP address for the IOCOMM to which you wish to copy the configuration, in order to establish a web connection to the unit.

1. On the IOCOMM you wish to copy the configuration to, on the **Main menu** page, select **Special operations**.

2. On the **Special operations** page, select **Read or write configuration file**.

3. In the **Name or IP address of host** field, enter the IP address or host name for the system (from which to copy the configuration file).

4. In the **Configuration file name** field, enter the full path and filename for the configuration file to read (having previously edited the file to change the IP address if you chose this method).

5. When you are happy with your entries, select **Read configuration from host**. The file will then be read back from the remote host to the IOCOMM and text similar to the following example will appear on the page:

```
~~~~~~~~~~~~~
Reading file /etc/tftpboot/iocomm2.db
From remote host hostname or IP address

Please reboot system to activate the downloaded
configuration.
~~~~~~~~~~~~~
```

The Read operation is complete.

6. Select **Return to the Main menu**.

7. Reboot the IOCOMM to make the configuration download effective.

8. On the **Main menu**, select **Global configuration**, then **LAN interface**.

9. Check that the IP address shown in the **IP address** field is correct for this unit. If it is, select **Submit** to save the configuration.

Note: The configuration will be written directly to non-volatile RAM. If after reading a configuration file back to a new unit you select any action button, the subsequent configuration information will overwrite the newly copied version and you will be back to a default or limited configuration status.

It is vitally important that you reboot the IOCOMM as soon as the configuration file has been read to the new unit. Both NV-RAM and operating RAM will then reflect the new configuration information.

If you read a configuration file which had the IP address field blanked when it was written to the remote host, this IOCOMM unit will automatically detect its IP address through the bootstrap.

Changing Passwords

When the IOCOMM is first installed it will have a factory default password set to iocomm. You should change this password as soon as possible and issue it to only those people who are authorised by you to make changes.

To change the password follow the procedure below:

1. On the **IOCOMM Main menu** page, select **Special operations**.

2. Select **Change administration password**.
3. Enter the old password in the **Current administration password** field.
4. Enter the new password twice in the subsequent fields.

   Note: This password allows full administration access to the IOCOMM via the Web or the admin login of the CLI.
5. Select **Submit**.
6. Select **Return to the main menu**.

Overview

The IOCOMM bootstrap, provides firmware upgrade to FLASH memory, run-time firmware load via the network (TFTP), and hardware diagnostic.

Normal Power-up

When the unit is powered-up (without the TEST switch being pressed), the bootstrap tests the hardware before normal operation starts. The progress of the tests can be monitored by viewing the cluster of six indicators to the left on the front panel.

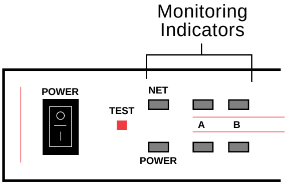


Figure 7: The Six Monitoring Indicators.

On powering up, the following tests and operations are performed:

- Power-on self-test.
- Attempts to discover the following network configurations (using BOOTP, DHCP and RARP).

  IP address

  Boot host

  Boot file

  Default gateway

  Subnet mask

  Domain Name Server

Note: If the IOCOMM fails to get a response, the unit continues to boot using the IP address and firmware stored in FLASH memory.

Power-on self-test

The IOCOMM power-on self-test, performs various hardware checks to establish that critical unit components and assemblies are functioning correctly. The main hardware checks performed are:

- CPU check
- Memory check (RAM and FLASH)
- Main hardware components
- Validity of on-board firmware

Note: During the power-on self-test, the green LEDs located on the front of the IOCOMM indicate test progress and any error conditions detected. If an error is detected, the IOCOMM self-test stops and the configuration and status of the front panel

LEDs indicate the likely cause. See *Indicators*.

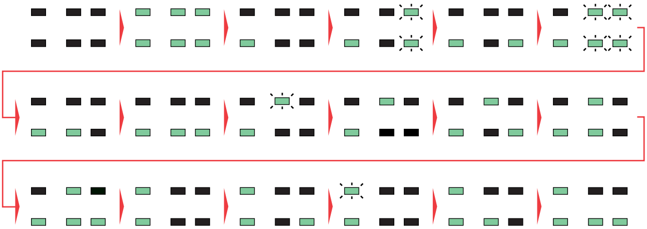


Figure 8: The sequence of LEDs during start up.

Diagnostic start-up

The IOCOMM has a diagnostic menu facility, which can be called up by booting the IOCOMM while the TEST switch is held pressed until the diagnostic menu appears. During this type of boot-up, the power-on self-test is not fully performed.

Using the Diagnostic menu

The diagnostic menu can be viewed by connecting a PC or terminal to the console (Port A).

To call up the menu, with the IOCOMM powered-off, press in and hold the **TEST** switch, then power-on the unit still holding in the **TEST** switch until the diagnostic menu appears. The diagnostic menu looks like this:

```
FLASH boot x.yy (build date)

Bootstrap and diagnostic monitor

(error message here-if detected)

CPU speed25 MHz
RAM size        4096 Kbytes
FLASH size      1024 Kbytes
Special serial  2
                (interface types)
Standard serial 8 (or 16)
                (interface types)

Operations menu

  1.  Hardware diagnostics
  2.  Display exception information
  3.  Factory reset
  4.  Request password reset
  5.  Clear request flags
  6.  Download to RAM and run
  7.  Download to FLASH and run
  q.  Quit. Unpack FLASH and run

: q
```

Note: Throughout the Operations menus, pressing either Q or ESC will return you to the previous menu. ESC will also abort the current test(s).

1. Hardware diagnostics

The Hardware diagnostics sub-menu, can be displayed by typing `1`. The sub-menu will be displayed as shown below:

```
Hardware diagnostics

   a.  Serial port A
   b.  Serial port B
   e.  Ethernet interface
   g.  Port B generator tests*1
   l.  LED panel
   n.  Non-volatile (FLASH) memory
   p.  Processor
   r.  RAM
   s.  Standard serial ports
   v.  Version information
   c.  Continuous test
   f.  Factory test (silent continuous)
   d.  Diagnostic monitor
   q.  Quit

   : q

   *1 Special testing use only
```

1.a Serial port A

The Serial port A diagnostics, check for correct operation of the port (used primarily for management functions with an attached console). To complete the test, the port A loopback (red, supplied) should be plugged into the port. To start the test, type `a`. The following messages will appear on the screen.

```
Probing interface type
Multi standard sync board
Loopback or no cable attached
Please install data pass through loopback on port A
Press Y to continue: y
```

The tests will then be performed and the results displayed on the console.

1.b Serial port B

The Serial port B diagnostics, check for correct operation of the port (Port B is software configurable as either synchronous or asynchronous for the connection of a wide range of devices). To complete the test, the port B loopback (supplied) should be plugged into the port. To start the test, type `b`. The following messages will appear on the screen.

```
Probing interface type
Multi standard sync board
Loopback or no cable attached
Please install DB26 loopback on port B
Press Y to continue: y
```

The tests will then be performed and the results displayed on the console.

1.e Ethernet interface

The Ethernet interface tests, check for correct operation of the three types of Ethernet interface (10BASE5, 10BASE2 and 10BASE-T). To start the tests, type `e`. The following sub-menu will appear on the screen.

```
Ethernet interface tests

1.  Internal loopback tests
2.  Data test on 10BASE5 (AUI)
3.  Data test on 10BASE2 (BNC/thin)
4.  Data test on 10BASE-T (twisted pair)
5.  Scope test pattern on AUI
6.  Scope test pattern on BNC
7.  Scope test pattern on TP

q.  Quit
```

1.e.1 Internal loopback test

During the Internal loopback test, two tests are performed; the first test loops data internally within the QUICC processor and the only requirement for correct operation is a valid data clock which is obtained from the 82503 TXC output. The second test, loops back at the 82503 serial interface, exercising data and the clock interfaces within the chip.

Note: Both of these tests may be run safely with the network interfaces connected.

```
QUICC based loopback
Testing [...................] OK

82503 based loopback
Testing [...................] OK
```

1.e.2 Data test on 10BASE5 (AUI)

The Data test on 10BASE5 (AUI), loops data back via the AUI interface and requires the fitting of an AUI loopback connector (Chase part no. 802-0046).   A typical screen output is shown below:

```
Please install AUI loopback and press Y to
continue. Y
10BASE5 (AUI) loopback test
Testing [...................] OK
```

The output below shows a test failure:

```
10BASE5 (AUI) loopback test
Testing          [
Eth: Tx error 0001, Carrier lost
Eth: Tx error 0001, Carrier lost
Eth: Tx error 0001, Carrier lost
Eth: Tx error 0001, Carrier lost
Eth: Tx error 0001, Carrier lost
FAILED
```

1.e.3 Data test on 10BASE2 (BNC/thin)

The Data test on 10BASE2 (BNC/thin), loops data back via the BNC interface and requires the fitting of a BNC loopback connector. This connector can be constructed simply from standard components by attaching two 50 Ohm BNC network terminators to a standard T-piece and then plugging this assembly into the 10BASE2 connector. A typical screen output is shown below:

```
Please install BNC stub and press Y to continue. Y
10BASE2 (BNC) loopback test
Testing [...................] OK
```

The ouput below shows a test failure:

```
0BASE2 (BNC) loopback test
Testing           [
Eth: Tx error 8000, Not sent
Eth: Tx error 8000, Not sent
Eth: Tx error 8000, Not sent
Eth: Tx error 8000, Not sent
Eth: Tx error 8000, Not sent
FAILED
```

1.e.4 Data test on 10BASE-T (twisted pair)

The Data test on 10BASE-T (twisted pair), tests the twisted pair interface. This test does not require the fitting of a loopback connector, as the interface has an internal loopback fitted.

```
10BASE-T (TP) loopback test
Testing [..................] OK
```

The output below shows a test failure:

```
10BASE-T (TP) loopback test
Testing          [
Eth: Tx error 8000, Not sent
Eth: Tx error 8000, Not sent
Eth: Tx error 8000, Not sent
Eth: Tx error 8000, Not sent
Eth: Tx error 8000, Not sent
FAILED
```

1.e.5 Scope test pattern on AUI

The Scope test pattern on AUI allows a continuous test to be run and the results monitored on a scope screen.

If you select this option, the following warning message will be displayed on the console.

```
WARNING:  THESE TESTS WILL JAM COMMUNICATIONS ON
ANY CONNECTED NETWORK.
```

Run this test on a test LAN or at a time when it will not compromise your network.

1.e.6 Scope test pattern on BNC

The Scope test pattern on BNC allows a continuous test to be run and the results monitored on a scope screen.

If you select this option, the following warning message will be displayed on the console.

```
WARNING:  THESE TESTS WILL JAM COMMUNICATIONS ON
ANY CONNECTED NETWORK.
```

Run this test on a test LAN or at a time when it will not compromise your network.

1.e.7 Scope test pattern on TP

The Scope test pattern on TP. allows a continuous test to be run and the results monitored on a scope screen.

If you select this option, the following warning message will be displayed on the console.

```
WARNING:  THESE TESTS WILL JAM COMMUNICATIONS ON
ANY CONNECTED NETWORK.
```

Run this test on a test LAN or at a time when it will not compromise your network.

1.e.q Quit

The Quit option exits the Ethernet interface tests menu and returns to the main **Hardware diagnostics** menu.

1.l LED panel

The LED panel test, checks all IOCOMM front panel LEDs for correct functioning. To start the tests, type `l`. The following messages will appear on the screen.

```
Walking LED test

Test switch will light all LEDs

Press any key to stop
```

1.n Non-volatile (FLASH) memory

The Non-volatile (FLASH) memory test, checks the IOCOMM FLASH for correct functioning. When the test is started, the FLASH chips are reset and the write protection bits for each bank are checked and reported, followed by the test menu itself.

To start the tests, type n. The following messages will appear on the screen.

```
FLASH write protection status

Bank     Odd            Even

0        Read only      Read only
1        Writeable      Writeable
2        Writeable      Writeable
3        Writeable      Writeable
4        Writeable      Writeable
5        Writeable      Writeable
6        Writeable      Writeable
7        Writeable      Writeable

WARNING: Tests are destructive and may require
         new firmware to be downloaded

      b. Blank check
      c. Clear configuration database
      e. Erasure check
      p. Program check
      q. Quit
```

Bank 0 contains the bootstrap itself and should be read only. An error message will be displayed if this is not the case. The tests operate on banks 1 to 6, normally used to store the main firmware. Only the **Blank check** will leave these banks intact.

The **Erasure check** and **Program check** will destroy the contents of the banks and will require new firmware to be downloaded before the IOCOMM can be used.

1.n.b Blank check

The Blank check, examines each memory location and checks that it is set to the blank state of 0xFF. If errors are detected, the first five offending locations are detailed together with their contents.

1.n.c Clear configuration database

The Clear configuration database option.

1.n.e Erasure check

The Erasure check, erases the FLASH sectors and then runs the blank check.

Note: All firmware data will be lost.

```
FLASH erase    [..........................]
Checking       [..........................] OK
```

1.n.p Program check

The Program check, erases the sectors, programs them with a count and then checks that the contents are correct.

Note: All firmware data will be lost.

Note: Repeated programming of FLASH is detrimental to its life, so only the protection bit check is performed in the normal continuous testing.

1.p Processor

The Processor tests, check the CPU for correct operation. To start the tests, type p. The following messages will appear on the screen.

```
Testing CPU clock speed
Target speed 25000000 Hz: correct
Motherboard loop check: OK
Press any key to continue
```

1.r RAM

The RAM tests, check the IOCOMM internal DRAM memory for correct operation. To start the tests, type `r`. The following sub-menu will appear on the screen.

```
DRAM tests

1.  Boundary alignment test
2.  Data bit walk
3.  Address fill test
4.  Random fill test / refresh check
a.  All tests
b.  Quit
```

1.r.1 Boundary alignment test

This test checks the DRAM boundary alignment.

```
DRAM Boundary alignment test

Filling 32/8   [...................]
Checking 32/24 [...................] OK

DRAM Word alignment test

Filling 16/8   [...................]
Checking 32/16 [...................] OK
```

1.r.2 Data bit walk test

This test checks the DRAM in data bit walk mode.

```
DRAM Zero Bit walk test

Filling        [......................]
Walking bit    [......................] OK

DRAM One Bit walk test

Filling        [......................]
Walking bit    [......................] OK
```

1.r.3 Address fill test

This test checks the DRAM under address fill mode.

```
DRAM Address Fill test

Filling         [.........................]
Checking        [.........................] OK

Inverse Address Fill test

Filling         [.........................]
Checking        [.........................] OK
```

1.r.4 Random fill test/ refresh check

This test checks the DRAM using random fill and refresh.

```
DRAM Random Fill test|
Filling         [.........................]

Processor off bus. Press test switch to continue

Checking        [.........................]OK
```

1.r.a All tests

This option, runs all tests shown (1. - 4.). The on screen information for each test is the same as that shown above.

1.s. Standard serial ports

The Standard serial port tests, check the main IOCOMM asynchronous serial ports for correct operation. The tests require a loopback / loopbacks (available from your supplier) to be fitted to the ports for the tests to run. To start the tests, type `s`. The following sub-menu will appear on the screen.

```
Standard serial port tests

1.  Host interface check
2.  Loopback test all ports
3.  Loopback test one port at a time

q. Quit
```

1.s.1 Host interface check

This test checks the UART host interface.

```
Testing UART host interface
UART host interfaces OK
```

1.s.2 Loopback test all ports

This test checks all serial ports. A full set of loopbacks is required (Authorised Re[pair centres only).

```
Please install loopbacks on all standard serial ports
```

(install loopbacks as required, and then)

```
Press Y to continue. Y

Testing standard serial ports
Testing port [port number(s)]

Testing standard serial ports
All standard serial ports OK
```

(or error message(s), if appropriate)

1.s.3 Loopback test one port at a time

This test checks individual serial ports as required (with a loopback connector fitted).

Install loopback for testing on port 1

```
t.  Test this port
s.  Skip this port
p.  Previous port
q.  Quit
```

(install loopback and select t if port1 is to be tested)

```
Press Y to continue. y
```

(select s if you wish to skip this port)

Repeat the above procedure for each port in turn

1.v. Version information

The Version information page, displays details of the current IOCOMM firmware version and build date. This information is useful if you have a technical support issue. To view the Version information, type `v`. The following messages will appear on the screen.

```
FLASH boot V(x.yy) (build date)
Built by rjj on inferno
Copyright 1997-1998 Chase Research PLC

Z-lib compression version 1.0.4 patch 1
Copyright 1995-1996 Jean-loup Gailly and Mark Adler

Searching main firmware for version strings

Decompress [...........*.............]
Version 0.90
Built by rjj on inferno (build date)

Press any key to continue
```

1.c. Continuous test

Only Authorised Repair Centres will have a full set of loopback connectors.

The Continuous test carries out all tests that can be run without user intervention (once any required loopback connectors have been fitted) in a continuous loop. The tests display the normal progress information for each test. It is also possible to run different selections of tests repeatedly or for a fixed number of times using the command line based diagnostic monitor, which can be accessed by selecting option **1.d Debug monitor** below.

To run the Continuous test, type `c`. The following messages will appear on the screen.

```
QUICC based loopback
Testing [...........................] OK

82503 based loopback
Testing [...........................] OK

Please install BNC stub and press Y to continue
```

Follow the on screen messages for the remainder of the tests

1.f Factory test (silent continuous)

The Factory test (silent continuous) carries out all tests that can be run without user intervention (once any required loopback connectors have been fitted). These tests only display information when an error is detected. It is also possible to run different selections of tests repeatedly or for a fixed number of times using the command line based diagnostic monitor, which can be accessed by selecting option d. Debug monitor (see below). To run the Factory test, press `f` on the keyboard. The following messages will appear on the screen.

```
Please install BNC stub and press Y to continue: y

Please install DB26 loopback plug in port B

Please install loopbacks in all standard serial ports

Press Y to continue: y
```

1.d Diagnostic monitor

The Diagnostic monitor allows you to customise the Factory tests and Continuous tests to check specific areas for correct operation. To view the Diagnostic monitor options, type `d`. The following messages will appear on the screen.

```
Diagnostic monitor

Enter ? for command summary

>
```

1.? For command summary

This option displays all of the commands that can be used in the Debug monitor routines. To display the command summary, type ?. The following will be displayed.

```
> ?

      About                          Information about software
      Clear [type] start size [value]  Clear memory
      Dump device                    Device register dump
      Exit                           Return to menus
      Forever command                Repeat command forever
      Goto address                   Jump to code
      Help                           Print this summary
      Memory [[type] start [size]]   Display block of memory
      Poke [type] address value      Poke one address with list of values
      Quit                           Return to menus
      Repeat count command           Repeat a command count times
      Set [type] address value       Set consecutive locations from list
      Test device                    Hardware tests

      All numbers in hexadecimal and must start with digit (0-9)
      Types are Byte, Word or Quad
      Separate commands on line with ;
```

Note: All commands should be entered using their initial letter only and any numeric parameters in hexadecimal with a leading numeric digit. Spaces should be used to separate parameters.

1.q Quit

The Quit option takes you back to the main Operations menu.

```
Operations menu

          1.  Hardware diagnostics
          2.  Display exception information
          3.  Factory reset
          4.  Request password reset
          5.  Clear request flags
          6.  Download to RAM and run
          7.  Download to FLASH and run
          q.  Quit. Unpack FLASH and run

: q
```

2. Display exception information

The Display exception information option, can be displayed by typing 2. The menu enables you to check status information from the last detected software or hardware error or exception (this information can aid diagnosis of faults and should be reported in full when exceptions occur). Any exception status recorded will be displayed automatically on first entry to the bootstrap monitor or it may be displayed at any time by selecting 2 from the main menu.

```
No exception recorded. Normal hardware restart

Exception 0

         Normal powerup
Location 00000000 00000000 00000000 00000000
```

3. Factory reset

The Factory reset sub-menu can be displayed by typing 3. This enables you to return IOCOMM to its original factory default settings. The following sub-menu will be displayed:

```
Factory reset menu

h. Hard reset. Default and save all settings now

s. Soft reset. Delay save to allow existing
   configuration upload

q. Quit
```

3.h Hard reset

This option will reset IOCOMM to its factory default settings and save the changes to FLASH memory immediately. You will see the following output on the console:

```
Clearing odd database

FLASH erase    [........................]
Programming    [........................] OK

Clearing even database

FLASH erase    [........................]
Programming    [........................] OK

Factory reset on restart flag set
```

Select `q. Quit. Unpack FLASH and run` to start the IOCOMM with factory defaults.

3.s Soft reset

As a safety measure, a soft reset will not be committed to FLASH memory until a configuration Web page is submitted to the IOCOMM.

When this option is selected, the following message will be displayed on the console:

```
Factory reset on restart flag set
```

Note: Using **Soft reset**, if you decide not to continue with the factory reset, before typing `q`, select `5. Clear request flags`.

When you select `q. Quit. Unpack FLASH and run`, the factory reset will be performed upon start-up.

3.q Quit

The `Quit` option takes you back to the main Operations menu.

4. Request password reset

The Request password reset option, can be displayed by typing `4`. This option enables you to return the IOCOMM to its factory default password (iocomm) if ever the password is forgotten.

When this option is selected, the following message will be displayed on the console:

```
Password reset on restart flag set
```

When you then select `q. Quit: Unpack FLASH and run`, a password reset will be performed upon start-up.

Note: If you have selected `4. Request password reset` and before typing `q`, you decide you do not wish to continue, select item `5. Clear request flags`. This will prevent the password reset from being performed.

5. Clear request flags

The Clear request flags option, is selected by typing `5`. This option enables you to clear the request flags which have been set for the factory reset and password reset options (see also **`3.`** and **`4.`** above).

6. Download to RAM and run

The Download to RAM and run option, is selected by typing `6`. The option allows you to download firmware into RAM without it being permanent.

Consequently, this option is very useful for checking out new or updated versions of firmware, or re-loading an older version which is known to work if you are trying to identify a fault. The new firmware downloaded to RAM will not be permanent until you run option 7.

7. Download to FLASH and run.

The Download to FLASH and run option, is selected by typing 7. This option enables you to upgrade the firmware on the IOCOMM. The operation will attempt DHCP/BOOTP discovery of the network configuration and the location of a TFTP host and file to download the new firmware from. Once the discovery has been performed, you will be prompted with each parameter in turn and allowed to confirm, override or if necessary, provide each value.

q. Quit. Unpack FLASH and run

The Quit. Unpack FLASH and run option, can be selected by typing `q`. This option implements any changes made in the Operations menu, decompresses the IOCOMM firmware and reboots the unit.

IOCOMM Front Panel

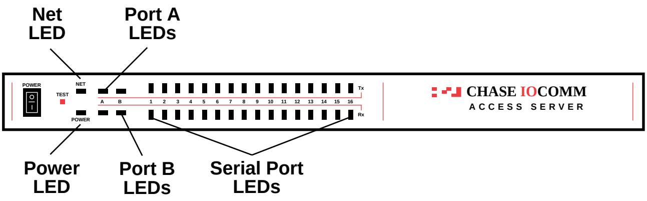


Figure 9: IOCOMM Front Panel indicators.

The indicators provide status information.

- The POWER indicator shows the unit is powered.
- The NET indicator shows the unit is communicating on the LAN.
- The Port A indicators show when port A is transmitting (Tx) or reveiving (Rx) characters.
- The Port B indicators show when port B is transmitting (Tx) or reveiving (Rx) characters or frames.
- The Serial port indicators show when ports 1-16 are transmitting (Tx) or reveiving (Rx) characters.

Status Codes

The Serial Port indicators are used to show progress during the power-up sequence:

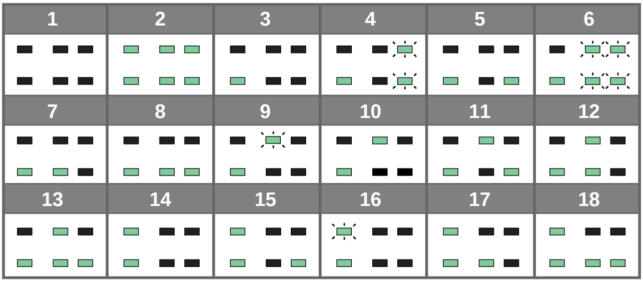


Figure 10: Power-up Progress indication.

If the unit stops during power-up sequence, the state of the indicators (off, on or flashing) can help an Authorised Repair

Centre to locate a possible fault. Refer to the table below:

1. Unit is not powered, or
2. Main processor and/or FLASH failure.
3. Power on, but bootstrap FLASH corrupt .
4. Processor dual port RAM failure.
5. Main RAM check in progress.
6. Main RAM check failed.
7. Main RAM check OK. Copying bootstrap to RAM.
8. Serial port A (console) checked.
9. Paused (awaiting test switch to be operated).
10. Checking standard ports 1 to 4.
11. Checking standard ports 5 to 8.
12. Checking standard ports 9 to 12.
13. Checking standard ports 13 to 16.
14. All serial ports OK. Initialising LAN interface.
15. LAN interface checked.
16. LAN probing in progress.
17. Decompressing main firmware.
18. Firmware checksum OK. Firmware started.

Note: There are no user serviceable parts inside.

WARNING
Do not remove the casing from the IOCOMM. There is a danger of electric shock. Any attempt to remove the cover will also invalidate the Chase Research warranty.

IOCOMM does not Boot

Symptom

Front panel POWER indicator is not lit.

Action

Check that the power switch is on; check that the power cable is connected to the supply and that the supply is switched on. If still not lit, check the mains supply fuse.

If LED is still unlit, the internal power supply or internal fuse may be at fault and the complete unit must be returned to your supplier, Chase Research or an Authorised Repair Centre.

Note: Any attempt to remove the IOCOMM cover or effect a repair will invalidate the Chase Research warranty.

Symptom

Front panel monitoring LEDs have stopped mid sequence.

Action

Check the Error Codes section to determine at which point in the sequence it has stopped. Refer to the *Bootstrap* section for further details.

If the bootstrap LEDs indicate an error early in the sequence, check the relevant hardware using the bootstrap diagnostics.

If the bootstrap LEDs indicate an error late in the sequence, this could indicate corrupt FLASH memory or contents. See section on **FLASH corruption** below.

Symptom

Monitoring LEDs have completed the cycle but the IOCOMM is still not functional.

Action

Check the LAN connection. Attach a terminal to port A (or any other enabled serial port): you should see a login prompt. If not, the firmware image in IOCOMM's FLASH memory may be corrupt. See section on **FLASH corruption** below.

Symptom

FLASH appears to be corrupt.

Action

Check the currently installed firmware, attach a terminal to port A on the rear of the IOCOMM (with the settings 9600 baud, 8 data, no parity, 1 stop) and run the bootstrap manually (option `q` from the main menu) to check for error messages.

If there are no error messages before the 'Calling firmware' message, the original download may have been corrupted. Download replacement firmware (from either the original CD or from the Chase Research FTP site) to RAM and check if this runs successfully. If this version of the firmware is OK, download it to the IOCOMM FLASH. See *Configuration* for details of downloading and saving new firmware.

Symptom

Newly downloaded firmware not running correctly.

Action

This could be a configuration problem. Carry out a factory reset by powering on the unit with the **TEST** button held in and then select Option `3`, then option `s` from the menu (note that this is not permanent until saved).

If the unit now boots, upload the corrupt configuration to a network host for diagnosis and download and save the last known working configuration (from backup copies).

Symptom **IOCOMM still not booting correctly.**

Action If you have carried out all of the above tests and the IOCOMM will still not boot, contact your supplier for further assistance.

Serial Port(s) not Working

Symptom **Device connected to port is not functioning.**

Action Establish that it is the serial port which is at fault and not the connected device by attaching the device to a correctly configured and known working port, or attach a known working terminal and cable to the faulty port.

Symptom **Multiple ports not working.**

Action If it is multiple ports, the pattern of non-working ports could be useful in diagnosing the problem. The following combination of failed ports could suggest the shown faults:

Port failures	**Possible cause**
Block of four ports	Faulty UART
Block of eight ports	Faulty serial board
All standard ports	Faulty bridge board
All ports	Faulty power supply

Note: Some software or configuration errors could produce a similar pattern of results.

Symptom **Single port not working.**

Action Check the wiring between the serial port and the connected device. Refer to the appropriate wiring specification given in *Connectors & Cabling*.

Perform a software reset of the port(s) using the web browser or CLI `hangup` command.

Substitute a terminal and known working cable and check if you get a login prompt. If you get 'garbage' data, check baud rate and character framing settings. Garbage data is possibly a PPP start-up negotiation problem. Check the serial port network protocol configuration.

Check the port configuration to ensure settings are correct, e.g. *Access enabled*. Copy the configuration from a known working port.

Check the port using the Status and statistics display page.

Check to see if any of the hardware lines are stuck in an unexpected state.

Symptom **None of the above checks fail to locate or resolve the problem.**

Action Reboot the IOCOMM and run the hardware diagnostics using a loop-back connector. Refer to Using the *Diagnostic Menu* section in *Bootstrap*.

If any of the above faults are confirmed, the unit must be returned to Chase Research or an Authorised Repair Centre. **Any attempt to remove the IOCOMM cover or effect a repair will invalidate the Chase Research warranty**.

Printing not Working

Symptom

Unable to print using LPD

Action

First check the correct operation of the serial port. If these checks have been made and printing still does not work, check that the printer cable being used is correctly wired. Many printer problems arise from incorrectly wired cables or poor connections within the plug housing. The correct pin assignments are shown in *Connectors & Cabling*.

Symptom

Printer doesn’t communicate with the host machine.

Action

Telnet from the host machine to the access server’s LPD port. For example:

```
telnet fred 515 (connecting to the IOCOMM’s LPD)
```

The following message should be displayed:

```
>>telnet fred 515
trying 194.32.85.44..
escape character is ‘^]’.
Connection closed by foreign host
```

If the telnet session will not connect, check that the network is performing correctly. If the telnet session still refuses to operate, re-configure the port for terminal operation and repeat the telnet operation. If this works, it confirms that the network is not at fault.

Check if flow control is set to the same setting at both the printer and in **IOCOMM Serial ports configuration**. Check if the host software is configured correctly for printing.

Check the **Status and statistics display** page on the IOCOMM web interface and ensure that the table of all connections in the netstat utility shows that local address *.515 is in the listen state. Also check that the port is receiving data in Serial port of the **Status and statistics display** page. If the status does not indicate any sign of LPD and data transfer on the port, you need to reconfigure the serial port and LPD.

Symptom

Unable to print using iocommd.

Action

Many of the general issues raised above for LPD printing also apply here. Check cables, connections, network, etc. If a printing problem still exists, check to see if the daemon is running. On Unix this would be:

```
ps -ef |grep iocommd
```

This should show an iocommd daemon in the table for each printer. If it is not listed by this command, invoke it now. If it is listed, it is probably incorrectly configured.

Kill iocommd using the Unix kill command, then run the command again.

Check to see if the spooler is configured correctly. Test the printer without relying on your spooler by sending data direct to the port you created and named, if you ran the iocommd daemon, by typing:

```
cat data_file > /dev/laser1
```

If the command returns, then the Unix system believes it has sent the data and there is a good chance it has been printed successfully. This would indicate that your print spooler has not been configured correctly.

If you have checked all connections and tried all of the above tests and printing is still not working, you are advised to contact your supplier for further assistance.

IOCOMM Unable to Access Other Network Devices

Symptom

Unable to access a device on local and remote networks.

Action

Check that the cable / connector from the LAN is securely fastened into the correct port on the rear panel of the IOCOMM. If you have changed the type of LAN media / connector (e.g. from 10BASE2 to 10BASE-T), restart your access server.

Check that the IP address for the access server has been set correctly. Set the correct IP address permanently using the IOCOMM web browser configuration page. Check also that the correct IP Netmask has been set. See *Configuration* for further information.

Check that routing is configured correctly. If there is more than one IP network, routes to the other networks should be set-up. Routing information can be checked through the web browser pages.

To check routing information:

On the **IOCOMM Main menu** page, select **Status and statistics display**, then **Netstat utility**, then **Routing information**. The page will display all routes which have been set-up using the **Static routes configuration** page and all those identified through **RIP** (listening).

Note: netstat can also be run on the CLI (Port A).

If there are routes which are missing from the table, these can be entered using the **Static routes configuration** page or by ensuring that **RIP** is enabled and that **RIP listening** (minimum requirement) is selected (RIP will then learn the appropriate addresses). The RIP options are set-up on the **Dynamic routing** page.

Check DNS host tables to ensure that all network server hostname entries are correct and up-to-date.

Symptom

Unable to access remote systems over a WAN interface, such as synchronous or asynchronous outgoing PPP/SLIP links.

Action

Check the **Remote sites configuration** pages to verify the correct configuration of the remote site information, including the log-in method, user name, password and if required, the log-in script.

Check the **Serial ports configuration** pages to check that the ports which have been configured for remote sites are set to enable outgoing services. Also re-check the physical configuration for the port(s) to ensure that baud rate, word format and flow control settings are correct. Finally, re-check the modem initialisation and dialling strings.

Check to see if the routing information table shows static routes to the remote host concerned using a serial link. This can be checked by either using `netstat -r` in the CLI or via the web browser by selecting **Status and statistics display** from the **IOCOMM Main menu** page, then **Netstat utility** then **Routing information**.

Within the Routing information table, serial links are denoted by either `ppp<n>` or `slp<n>` , where `<n>` is the link number. If a route cannot be identified to the remote host concerned, go back and re-check the **Remote sites configuration** pages for the host.

Check the **System log** file to identify any dial-out errors occurred when attempting to connect to the remote system. If the connection appears to be successful, check that the remote machines routing information is correct.

Dial-up User Unable to Access IOCOMM

Symptom

Unable to connect to the IOCOMM via a modem connection.

Action

Check the set-up on the user's remote machine.

Check the **IOCOMM System log** file to see if there are any authentication failure messages for the user concerned. To do this, on the **IOCOMM Main menu** page, select **Status and statistics display**, then **Event logging**, then **System log**. If an authentication failure has been detected, check the RADIUS configuration and the login information for the user concerned on the RADIUS server. Check that the RADIUS server is accessible by the IOCOMM using the LAN or a configured WAN connection (try pinging it).

Check that the settings in the **Serial ports configuration** page are correct, in particular the **Access options** settings. Check that the correct modem initialisation strings have been specified.

Check the **IOCOMM System log** file to see if there are any modem initialisation and test failure messages. Check that the modem(s) are correctly connected to the telephone line and correctly configured for auto-answer.

Dialup User Can Connect to IOCOMM But Not Onwards (to other hosts)

Symptom

Unable to gain access to a host via the IOCOMM.

Action

If RADIUS authentication is being used, check that the user has the correct permissions, either `login` or `admin` on the RADIUS server.

If local authentication is being used, check that the user has the required permissions for connecting to the local machines. To check this:

> On the **IOCOMM Main menu** page, select **Global configuration** then **Local authentication** to check if local authentication is being used. If it is, check the appropriate user entry to ensure that the permissions are correct.

Check that the port has the necessary permissions set to allow the user to connect to the local machines. To check this:

> On the **IOCOMM Main menu** page, select **Global configuration** then **Serial ports configuration**, **Access options**, then **Expert** mode. Check the page settings for the port(s) in question.

Dialup User Unable to Access Remote Machines

Symptom

A remote machine is inaccesssible through IOCOMM.

Action

Check the items in **IOCOMM Unable to Access Other Network Devices** to establish that the remote machine is accessible .

Check the routes on the dial-up user's machine. These should be configured to use the IOCOMM as the default gateway.

Configuration Web Pages Not Accesible

Symptom

Web browser cannot be used to access the IOCOMM configuration pages.

Action

Check if you can access the IOCOMM from your PC using other network protocols such as ping, finger and telnet.

If these network protocols also fail, it is likely that you have a more general networking fault. See **IOCOMM Unable to Access Other Network Devices**.

Symptom

Proxy web server cannot reach the IOCOMM.

Action

Try using, ping, finger and telnet from the proxy server to check if this route works. If in doubt, disable the proxy server option on your web browser and see if this resolves the problem.

DNS failure, either at the proxy or at your PC could also produce the same problem. To check this, substitute the IP address of the IOCOMM for the host name in the URL.

If the IOCOMM web server has been configured for a non-standard (non-default) TCP port for web access, remember to add the new port number to the end of the URL.

The HTTPD page provides an administration setting, enabling the web server port number to be changed from the default port number of 80. If you change the port number from 80, you will need to add the new port number to the end of the URL line for the IOCOMM when you try to connect using a web browser. If you change the port number, it is advisable to keep a note of it. However, if you forget the new port number, it can be checked using the `netstat -a` command from the IOCOMM CLI.

Check that the firewall or other routing / bridging device is letting traffic through on the relevant TCP port. This is especially relevant if the IOCOMM web server is on a non-standard port.

If you have checked all areas covered above and carried out all of the tests and IOCOMM is still not accessible from the web, contact your supplier.

Initial Bootstrap ARP Jamming

Symptom

Unable to use ARP Jamming.

ARP is the protocol used to initially set the IP address of a newly installed IOCOMM. The procedure for this ARP jamming operation is covered in *Getting Started*.

To use ARP jamming, the system whose ARP table you are using must be on the same LAN as the IOCOMM. If you are accessing the LAN via a router or other gateway, then it is **this** device's ARP table that should be jammed.

Action

Use the ARP command with the IOCOMM's host name or IP address to check the information that has been set. You can also add the pub flag to the jamming command to make sure that the information is broadcast for other devices on the LAN.

Symptom

You can ping the IOCOMM but cannot get web access

Action

It may indicate that the browser is using a proxy that cannot find the IOCOMM. Try jamming the ARP table on the proxy system or disable the proxy operation. See also **Configuration Web Pages Not Accessible** for more information.

Symptom

ARP Jamming still does not work.

Action

If after trying the above, ARP jamming still does not work, you can set the IOCOMM IP address using an attached terminal or PC on port A of the IOCOMM. See *Getting Started* for details.

Event Logging (syslog)

The access server features an extensive problem and event logging system (syslog), which is useful for general system maintenance and trouble-shooting.

Syslog configuration is described in *Configuration, First Time Configuration Tour* and *Configuring Status Logging*.

There are three possible destinations for logged events:

- **Console** (port A)
- **Internal buffer** (accessible by local or remote administrators)
- **Remote host** (running the syslog utility)

If you have selected to log events to the internal buffer or to the console, the logged messages will not show the correct time or date unless a syslog host is specified. Without a syslog host, the date and time will be reset to midnight, Jan 1.

Note: You can use a syslog host to obtain date and time information even if you are not logging to that host.

Viewing logged events

The logged events can be viewed by using either `syslog display [no.]` from the Command Line Interface or by using the web browser interface (from the **IOCOMM Main menu**, select **Global configuration** then E**vent logging**).

An example of an event log display is shown below:

OCOMM System log

```
User Notice Jan 01 00:00:07 iocomm System started
Dialer Info Jan 01 00:01:27 iocomm System initialisation complete
Auth Warning Jan 01 00:07:19 iocomm Multiple logon attempts failed on port A
```

Description of syslog fields

`User`	`Notice`	`Jan 01 00:00:07`	`iocomm`	`System started`
Facility	**Severity level**	**Date and Time**	**Source**	**Description**

The syslog file contains information regarding the event or problem. It includes the severity level and facility level, the data and time the log was recorded, the source (always iocomm for the internal buffer), and a plain text description of the reason for the log .

Tables below define and describe facility and severity codes.

Facility codes

Message	**Description**
`Kern`	Kernel message
`User`	Random user-level messages
`Daemon`	System daemons
`Auth`	Security / authorization messages
`Syslog`	Messages generated internally by syslog
`Print`	Line printer subsystem
`Dialer`	UUCP subsystem
`Private`	Security / authorization messages (private)
`TFTP`	TFTP transfers

Severity codes

Message	**Description**
`Panic`	System is unusable
`Alert`	Action must be taken immediately
`Urgent`	Critical conditions
`Error`	Error conditions
`Warning`	Warning conditions
`Notice`	Normal but significant condition
`Info`	Informational
`Debug`	Debug-level messages

Exception Display

The **IOCOMM Exception display** provides details of critical errors which in most cases will cause the unit to halt operation and then perform an automatic re-boot. The only time when automatic re-boot does not happen is when an exception occurs during initial boot-up. In this case, the re-boot will be delayed for approximately 30 minutes. This is to prevent the unit from entering a continuous cycle of exception, re-boot, initialisation, exception, etc.

Should an exception occur on your IOCOMM unit, wait until the automatic reboot has been performed and check the status. If the exception re-occurs, make a note of the exception number together with details of what operation was being performed.

IOCOMM Exception Display

The most recent exception can be viewed from the web browser interface. From the **IOCOMM Main Menu**, select **Status and statistics**, **Event logging**, then **Exception display**. An example is given below:

```
Hardware detected exception

Exception 7

TRAP Bus Error

Location 0000c008 0000002c 00000000 00000000

D0-7 0000001c 00000001 0050c982 00000000
00000001 005b6dfe 005b6e36 005b6df2
A0-7 0073ca34 00649aa4 00000000 0073ca34
00740064 00649aa4 005b6de7 00678a0c
PC 0054666a
SR 00002600

Stack 0050c982 00000001 00000002 005b6d95
0054f26a 0054f2a0 0050c982 00000001
00000010 00554f8a 00000001 0073ca34
00740064 0050a182 005b6d90 005b6dc0
```

All of the information contained in the Exception display is important for fault diagnosis. The complete contents of the frame, together with details of the firmware version, should be passed to your supplier or Technical Support contact.

Re-occuring Exception

If the exception reoccurs, there are several options which can be tried to remove the fault.

Hardware reboot

Perform a hardware reboot / power cycle the unit. This may overcome a hardware problem not cleared by the automatic software reboot.

Factory reset

If a hardware reboot does not correct the problem, perform a factory reset. With the IOCOMM powered off, press and hold the **TEST** switch, then power-on the unit, holding in the **TEST** switch until the bootstrap diagnostic menu appears (as shown below).

```
Operations menu
1. Hardware diagnostics
2. Display exception information
3. Factory reset
4. Request password reset
5. Clear request flags
6. Download to RAM and run
7. Download to FLASH and run
q. Quit. Unpack FLASH and run
: q
```

From the menu, select option 3. Factory reset, then q to Quit. Unpack FLASH and run. If this is successful, upload the faulty configuration to a network host for analysis.

Check for FLASH / firmware corruption

Follow the instructions given in *Troubleshooting*. If you have recently changed to a new version of firmware, revert back to the previous version to check if the problem persists.

iocommd is a Unix tty port redirector. It is suitable for legacy applications (that open tty devices) and can also be used for printing, although LPD is normally a much better solution.

The procedure for configuring iocommd printing on the IOCOMM is given in *Configuration*.

This section provides information on setting up and using iocommd on host machines.

The IOCOMM peripheral daemon (iocommd) provides a client process with a full-duplex and transparent interface to a server port of its choice, via a pseudo-tty device. This presents a tty-like interface to the application in much the same way as a serial port.

The iocommd daemon is primarily intended as an interface between the client process and a printer, modem or data acquisition device. In the case of printers, it is recommended that the LPD protocol is used where possible.

By default, the daemon will fork into two processes during the start of a data transfer. The parent process will transfer data from the client to the server while the child process will transfer data from the server to the client. The parent also handles all the control aspects of the client-server link. The child process is normally terminated when the client process closes the slave pseudo-tty unless the -p option is used. In this case, the child is created at startup time and remains.

If the daemon is started without any arguments it will try and open the configuration file `/etc/iocommd.conf` which contains instructions on which daemons to start, for which peripherals, plus any optional arguments. Alternatively, a single daemon can be started from the shell with various arguments specified.

There are three mandatory arguments the daemon requires to mediate between the client and server port:

Server: The host name of IOCOMM that has the attached printer or terminal.

Port: The TCP port on which the IOCOMM port is listening for connection requests.

Link: A mnemonic filename in /dev which shall be linked to the slave pseudo-tty selected by the daemon. This should be used as the interface device for client processes since the pseudo-tty may change during the daemon lifetime.

The other optional arguments modify the behaviour of the daemon in the way it controls connections and processes data to and from the peripheral. They are defined as follows:

Note: iocommd does not support the `-t` (and consequently `-s`) switches. It supports raw data transfer mode only.

`-p` The daemon maintains a continuous TCP connection to the access server port. This is useful for applications that require exclusive and uninterrupted access to a device. Note that no other daemon will be able to access such a port if any daemon is running to that port with this option.

`-h` Hangs up the pseudo-tty if the TCP connection is lost. This mimics the situation in which a real serial port loses a signal such as DCD. In the same manner as the serial port, a SIGHUP signal will be sent to all processes that have the slave pseudo-tty as their controlling tty. See also -w.

`-n` Converts all carriage returns read from the client process to carriage return and line feed. This is useful if using iocommd for printing and the print job is off the right margin (i.e. stair stepping).

`-m` Push the STREAMS tty modules onto the slave pseudo-tty. This is useful for applications that expect to modify tty parameters as if a hardware device was attached. The modules pushed are the line discipline (normally called /dterm) and the hardware emulation (if supported). This option requires that the pseudo-tty architecture is based on the STREAMS I/O mechanism. The recommended Unix variants for using this option are those based on System V Release 3.Variants based on System V Release 4 should first try the -a option. Variants such as HP-UX, AIX, Xenix and SunOS do not require either option.

`-a` Use the autopush facility to push STREAMS modules onto the slave pseudo-tty. This facility is supported on Unix System V Release 4 variants.

`-u` Discard all data received from the peripheral. This is useful in cases where the peripheral is sending unwanted data to the host, which is not being read by the client and therefore may cause blockage problems on the pseudo-tty.

`-w` Used with the -h and -p options. By default, on a hang-up, the daemon will open a new pseudo-tty before it has reconnected to the access server port. This option does the opposite and tries to re-establish the TCP connection first.

`-o` Used with the -p option. This option prevents the slave pseudo-tty from closing so as to prevent any flushing of data that may occur. With this option set, the daemon will not close the TCP connection so its use is not advised for modems, as line hang-ups may not be initiated. It is useful for slow printers that may lose data on pseudo-tty close.

`-f<file>` Specify a different configuration file. If the pathname is relative, the current working directory will be used.

`-k<n>` This option checks if the TCP connection is still alive every n seconds. If the test fails, the child daemon process dies and signals the parent daemon that the connection is lost.

`-x<n>` Set the daemon debug/diagnostic level to n. On startup, a log file called `/var/iocommd.log` is created (if not already there). All daemons on the host will write their debug and diagnostic messages to this file with a timestamp, daemon process ID and arguments attached to the actual diagnostic. The debug and diagnostics levels are:

`0` Lets the world know we're alive, but nothing else.

`1` Reports startup options.

`2` Reports connection and disconnection events.

`4` Reports numbers of characters being sent / received.

`8` Displays data written to the client process.

`16` Displays data written to IOCOMM.

`32` Reports telnet negotiations.

`64` Displays data read from IOCOMM.

`128` Displays data read from the client process.

Adding the desired level numbers together can combine these levels. Care should be taken when a high debug level is set, because the log file could grow too large.

`-c<n>` Network connection timeout option. The daemon will try for n seconds to establish a TCP connection, after which time, it will abort and discard any pending data. The default is to try forever. An example of daemon configuration file is given below:

```
-x3 IOCOMM1 10011 IOCOMM1.11
-x35 -a -h xxx -c60 IOCOMM1 10013 IOCOMM1.13
-x39 -p -h -a -k60 IOCOMM2 10009 IOCOMM2.9
```

Each line represents a daemon to be started with the argument on that line.

The first line is a simple printer configuration. The second line is a complex modem configuration. The third line shows a configuration more suited to a daemon with a terminal attached and a getty running as the client process.

Normally, the debug level is set to a minimal level such as 3.

Unix notes: On some System V Release 4 variants, if the daemon writes to a non-existent client, the pseudo-tty may irretrievably hang up. In general, make sure there is always a client process running if there is the possibility of data being received for it.

On SunOS, if a getty is the client process running to a terminal then the login prompt may be corrupted on the screen, but this goes when the user name is typed in. The UUCP command uucico may not work with iocommd on Solaris 2.1 (Intel).

Some systems may not properly propogate the SIGHUP signal associated with the -h option.

A Command Line Interface (CLI) is provided for administrators and is available to authorised users who make telnet or serial port connections to the device.

Line Editing

This interactive interface supports prompting, input echoing and line edit.

CLI Prompt

The CLI will prompt for each line of input with a prompt consisting of the assigned host name followed by the character '>' if the user is unprivileged, and '#' if the user has administrative permissions, and finally a single space.

Note: If no host name is entered on the DNS page, the host name will default to iocomm.

Line Edit

Character echo is provided and the backspace and delete characters can be used to delete the last character entered.

Use ^U to abandon the current input buffer.

^C can be used to force early termination of commands.

The maximum input line length is 120 characters.

Commands

The use of commands is limited by the access options set on the port from which they are to be invoked. Until a port is reset all access options are available. Access options are described in Changing Serial Line Configuration.

The following commands are provided:

`admin` Enable administration permission

Syntax:

```
admin
```

Description: Verifies the user's administration permission by asking for and verifying the unit administration password. Until this command has been run successfully no other commands requiring the administration permission can be run. `Exit` cancels the effect of this command.

See also: **`exit`**

Permission: *admin*

`arp` Address Resolution Protocol

Syntax:

```
arp hostname
arp -a
arp -d hostname
arp -s hostname ether_addr [temp] [pub]
```

Description: Display and manipulate information stored in the ARP table, to correlate hardware and IP addresses. When `hostname` is the only argument, the command displays the current ARP entry for `hostname`. The host may be specified using name or number.

`-a`	display all the current ARP entries
`-d`	delete the entry specified by `hostname`
`-s`	create a new entry for the network address `hostname` with ethernet address `ether_addr`

`temp`	the table entry shall be permanent unless keyword `temp` supplied.
`pub`	the entry shall be 'published'. I.e. this system shall act as an ARP server, responding to requests for hostname even though the host address does not belong to this system.

See also: **`ifconfig`**

Permission: *admin*

`except`

Display last exception information

Syntax: `except`

Permission: *admin*

`exit`

Leave administration mode or exit CLI

Syntax: `exit`

Description: Terminates administration permissions following a successful `admin` command, otherwise terminate CLI. The command shall also have the aliases of `quit` and `logout`.

See also: **`admin`**

Permission: *admin, nas*

`hangup`

Drop serial port connection

Syntax: `hangup [port] .. [port]`

Description: Force a serial port to perform hangup actions as if a loss of carrier was detected. Calling this command with no argument causes the port running the current CLI to hangup.

port is an integer port number from 1 to the number of standard ports, A (for the first advanced port) or B (for the second advanced port). Alternatively, these simple port identification can be preceded by the text 'port' (e.g. port1, portA).

Permission: *admin*

`help`

Provide helpful information to user

Syntax: `help`

Description: Display a list of commands that are currently available to the user. This command has the alias of `?`.

Permission: *admin, nas*

`ifconfig`

Configure a network interface

Syntax: `ifconfig interface address_family [address [dest_addr]] [up|down] [netmask mask] [broadcast broad_addr] [arp|-arp]`

Description: Assign an address to a network interface and/or configure network interface parameters.

The *interface* parameter is the network interface name (see `netstat` command) and does not correspond to the physical port numbering.

The name used will be `quicc0` for the ethernet interface, `sl0-sl20` for configured SLIP connections and `ppp0-ppp20` for configured PPP connections or `lo0` for IP loopback.

`address_family` is the address family, only `inet` (Internet address family) is supported. `address` is the IP address of this interface, this can be a host name or an address specified in Internet standard dot notation. `dest_addr` is the IP address of the entity at the other end of a point-to-point link.

The following parameters can be used

`up` Mark an interface *up*. This may be used to enable an interface after an `ifconfig` down command. It happens automatically when setting the first address on an interface. If the interface was reset when previously marked down, the hardware shall be re-initialised.

`down` Mark an interface `down`. When an interface is marked down, the system will not attempt to transmit messages through that interface. If possible, the interface will be reset to disable reception as well. This action does not automatically disable routes using the interface.

`netmask` Specify how much of the address to reserve for subdividing networks into sub-networks. The mask includes the network part of the local address and the subnet part, which is taken from the host field of the address. The mask can be specified as a single hexadecimal number with a leading 0x or with a dot-notation Internet address.

The mask contains 1's for the bit positions in the 32-bit address which are to be used for the network and subnet parts, and 0's for the host part.

`broadcast`

Specify the address to use to represent broadcasts to the network. The default broadcast address is the address with a host part of all 1's.

`arp` Enable the use of the Address Resolution Protocol in mapping between network level addresses and link level addresses (default).

See also: **`netstat, arp`**

Notes: Settings changed by this command are not saved.

Permission: *admin*

`lookmem` **Display access server memory usage**

Syntax: `lookmem`

Description: Display information on the operating system memory usage.

Permission: *admin, nas*

`lookstream` **Display access server streams resource usage**

Syntax: `lookstream`

Description: Displays the current streams sub-system buffer usage statistics. For each buffer the following is displayed:

1. Buffer size.
2. Total number of pre-allocated buffers.
3. Number of free buffers.
4. Highest number of buffers ever available.
5. Total number of buffers allocated so far.
6. Buffer allocation overflows so far.

A memory usage summary is provided at the end of the list.

Permission: *admin,nas*

`netstat` Display network statistics

Syntax: `netstat [-Aainrs] [-f address_family] [-I interface] [-p protocol] [interval]`

Description: Present network statistics.

`-a` Display state of all active connections (including servers).

`-A` Show the address of any protocol control blocks associated with sockets.

`-i` Show the state of interfaces.

`-n` Show network addresses as numbers.

`-r` Display routing information.

`-s` Show per protocol statistics.

`-I interface`
Display network information for quoted interface only (see `ifconfig` for a definition of interfaces)

`-f address_family`
Limit statistics and control block displays to `address_family`. The only family supported is *inet*.

`-p protocol`

Show statistics for that protocol (either IP, ICMP, UDP, TCP).

`interval`

Interval in seconds between redisplay of statistics

Calling the command with no argument displays the state of all of the active network connections.

Permission: *admin, nas*

`ping`

Send ICMP echo request

Syntax: `ping [-fnqrvR] [-c count] [-i wait] [-l preload] [-p pattern] [-s packetsize] hostname`

Description: Send an ICMP echo request message to a host on the network, display round trip times and packet loss. This command is intended for use in network testing, measurement and management. The default number of packets sent is 10.

`-R`	Record the route, display route buffer on returned packets.
`-f`	Flood ping the host.
`-n`	Numeric output only for hosts.
`-q`	Quiet output.
`-r`	Bypass normal routing tables.
`-v`	Verbose output.

`-c count`

Send `count` number of packets.

`-i wait`

Wait `wait` seconds between each packet.

`-l preload`

Send `preload` number of packets as fast as possible before returning to normal mode of operation

`-p pattern`

Specify pad bytes to fill out packet to be sent.

`-s packetsize`

Specify size of packet to be sent.

`hostname`

The IP address or hostname of the host to which the packets shall be sent.

See also: **`netstat`, `ifconfig`**

Permission: *admin*

ppp Configure Point to Point Protocol

Syntax:

```
ppp [-i] [-V] [-f rtscts|xonxoff|noflow]
[-d debug_level] [-m mruMRU] [-a acc_map]
[-p pap| chap|both] [-k key]
[-x noproxy|proxy] [-P] [-R remote]
[-L local] [-M mask]
```

Description: This command attaches serial lines as network interfaces using the Point-to-Point Protocol.

`-i` Disable IP address negotiation (default: `negotiate`).

`-V` Disable Van Jacobson TCP/IP header compression (default: `compress`).

`-f` Set the flow control method, `rtscts` specifies hardware flow control (default), `xonxoff` specifies software flow control and `noflow` specifies no flow control

`-d` Set the debug level, `0` for no debugging (default), `1` for logging PAP/CHAP, LCP and IPCP messages and `2` for logging all PPP messages.

`-m` Specifies the MRU in decimal (default 1500 bytes).

`-a` Sets the asynchronous control character map in hexadecimal format (default 0 unless software flow control enabled in which case software flow control characters are flagged out).

`-p` Sets the authentication protocol. Possible values are `PAP`, `CHAP` or `both`. If `both` is selected CHAP will be tried first. Default: `no authentication`.

`-k` Specifies the authentication password key.

`-x` Specifies whether the unit shall act as an ARP proxy for the PPP link.

`-P` Uses the remote address obtained from the PPP address pool.

`-R remote`

Specifies the address of the remote end of a PPP connection. Must be a valid hostname or IP address. If this is set to `0` IOCOMM will accept IPCP negotiation of the address. Negotiation is not accepted for non-zero addresses.

`-L local`

Specifies the address of the local (IOCOMM) end of the PPP link. `local` must be a valid hostname or IP address. If unspecified the local address will match that of the Ethernet interface.

`-M mask`
Specifies the netmask in IP address format (default: `255.255.255.255`).

Permission: *admin, framed*

`pppstats`

Display PPP statistics

Syntax: `pppstats`

Description: Print out PPP statistics for the IOCOMM. Should include:

The number of connection requests, those established and closed

The number of authentication failures

Number of received packets with errors

A breakdown of errors.

Permission: *admin*

`ps`

Display processes

Syntax: `ps`

Description: Display the service components, their status and resource usage.

Permissions: *admin, nas*

`pstatus`

Display port status

Syntax: `pstatus [-alhqv] [<portnumber>]`

Description: Display the logical status of a serial port (default to showing status of all active ports).

`-a`	Show all ports, even inactive ones
`-l`	Show reason for last disconnect
`-h`	Show hardware status

`-q` Quiet mode, don't show auxillary information

`-v` Verbose mode, show everything

`port number`
The serial port number, syntax of port numbers shall be as per the hangup command supporting the following; [port1] [portA] [1 2 3] [A B].

Permission: *admin, nas*

rlogin

Remote login

Syntax:

```
rlogin [-l <username>] [-T <term>] <hostname>
```

Description: Connect to a host on the network using the Rlogin protocol. Once established the connection to the remote host can be terminated from the IOCOMM end by starting an input line with the sequence ~. (tilde-dot). If it is required to send a line to the remote machine that begins with ~. then it needs to be entered as ~~. (tilde-tilde-dot). Tilde anywhere else on the line or followed by any other character has no special meaning.

`-l` Pass the username to be used for the login on the remote host

`-T` Pass the terminal type

`~.` Terminates session

Permission: *admin, login, nas*

route

Configure IP routing information

Syntax:

```
route [-n] add [-net|-host] <destination>
<gateway> [-netmask <mask>]
route [-n] delete [-net|-host] <destination>
<gateway> [-netmask <mask>]
route [-n] flush
```

Description: Manage IP routing available from the IOCOMM.

`-n` Bypass attempts to print host and network names symbolically when reporting actions.

`flush` flush the routing tables of all gateway entries.

`add` Add a new route to the routing table.

`delete` Remove a route from the routing table.

`-net` Forces the destination to be a network address

`-host` Forces the destination to be a host address

`-netmask`
Forces the mask to applied to the route

`destination`
IP address of the destination.

`gateway`
IP address of the gateway to be used when accessing the destination.

Permission: *admin*

`slip` Configure a Serial Line IP connection

Syntax:

```
slip [+c|-c] [+e|-e] [+i|-i] [+m <mtu>|-m
<mtu>] [+v|-v] [+p|-p]  <src_name>
<dst_name>
```

Description: Set up a SLIP connection.

`+c or -c`
Turns the TCP/IP header compression mode on (`+c`) or off (default).

`+e or -e`

Turns the automatic detection and the use of TCP/IP header compression on (`+e`) or off (default). If the flag `+c` is supplied then this flag has no effect. When the `+e` flag is supplied, the SLIP module does not send any compressed TCP/IP headers until it has received and successfully decompressed a TCP/IP packet.

Note: if both ends of the connection use the `+e` flag and neither end uses `+c`, the TCP/IP header compression mode will never be turned on because neither end will take the initiative to send a compressed packet.

`+p or -p`

Proxy arp flag. Default is to insert destination address into the ARP cache. The `-p` flag indicates that no entries shall be added and the `+p` flag specifies that entries will always be added regardless of the remote network.

`+i or -i`

Turns the suppression of ICMP packets on (`+I`) or off (default).

`+m or -m`

Either of these flags set the maximum transmission unit (MTU) of the network interface to `mtu` (default 296 bytes). `mtu` is specified in decimal and the recommended `mtu` value for the TCP/IP packet header is 40 plus some power of 2 (e.g. 296 = 40 + 2**8).

`+v or -v`

Specifies whether or not to turn on verbose mode (default off). This prints various messages about the interface when it is being brought up, if it is turned on.

`src_name`

Specifies the local IP address of the link (IOCOMM).

`dst_name`

Specifies the remote IP address of the link.

Permission: *admin, framed*

`syslog` Send or display a syslog message

Syntax:

```
syslog msg [-l <warning_level>] [-f
<facility_id>] <text>
syslog display [<lines>|cont]
```

Description: Manually send or display a syslog message.

`-l` Set warning level of the message being logged. Logging levels are defined in the *Event Logging (syslog)* section.

`-f` Set the facility identifier of the message being logged. Facility identifiers are defined in the *Event Logging (syslog)* section.

`msg` Send the message text to the system log.

`display` Display the current messages in the circular syslog buffer held by the IOCOMM. The oldest message is displayed first.

`lines` The number of messages to display from the buffer, if this parameter is not specified the 10 most recent messages are displayed (oldest first).

`cont` Display messages continually.

Permission: *admin*

`telnet` Connect to host

Syntax:

```
telnet [-E] [-e <char>] [-T <term>]
<hostname> [<port>]
```

Description: Connect to a host on the network using the Telnet protocol.

`-E` Stops any character being recognised as an escape character.

`-e char`
Sets the initial Telnet escape character to `char` (default ^]).

`-T term`
Set terminal type to that defined by `term`.

`hostname`
Indicates the hostname, an alias or an IP address.

`port` The network port number, default 23.

Permission: *admin, login, nas*

`tftp` Download and upload configuration files.

Syntax:

```
tftp put|get <host> <filename>
```

Description: Transfer IOCOMM configuration information to or from a host on the network.

`put` Transfer the file from the IOCOMM to the host.

`get` Transfer the file from the host to the IOCOMM.

`host` TFTP server on the network, an IP address or a host name.

`filename`
Name of file. This may or may not be the full path of the file on the server depending on whether the server is running secure TFTP and how this is implemented.

Permission: *admin*

`traceroute` Display the route IP packets are taking

Syntax:
```
traceroute [-nrv] [-w wait] [-m max_ttl]
[-p port] [-q nqueries] [-t tos] [-s
src_addr] [-g gateway] host [datasize]
```

Description: Display the route taken by IP packets from the IOCOMM to the host.

`-n` Print the hop addresses numerically.

`-r` Bypass the normal routing tables and send directly to a host on an attached network. If the host is not on a directly attached network, an error is returned.

`-v` Verbose output. Received ICMP packets other than TIME_EXCEEDED and PORT_UNREACHABLE will be listed.

`-w wait`
Set the time for a response to an outgoing probe packet to `wait` seconds (default `3`).

`-m max_ttl`
Set the maximum time-to-live (in hops) used in outgoing probe packets (default `30`).

`-p port`
Set the base UDP port number used for probe packets to `port` (default `33434`).

`-q nqueries`
Set the number of probe packets for each time-to-live setting to the value `nqueries` (default `3`).

`-s src_addr`
Use `src_addr` as the IP address which serves as the source address for outgoing packets. If the address is not one of the IOCOMM's addresses then an error is returned.

`-g gateway`
Enable the IP LSRR (Loose Source Record Route) option in addition to the Time To Live tests. This is useful for asking how somebody else at IP address `gateway` can reach a particular target.

`-t tos` Set the type-of-service in probe packets to the value defined by `tos`, default value is `0`.

`host` The destination name or IP address.

`datasize`
The data size in bytes of the probe datagram (default is `38`).

Permission: *admin*

Connectors and Cabling

This section defines the connectors on the unit and describes the cables required for problem free operation.

Connectors

The rear panel provides the following connectors:.

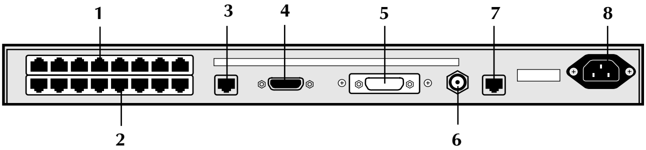


Figure 11: Rear Panel.

	Name	Type	Function
1	Serial ports 9-16	RJ45	Asynchronous device connection (RS-232)
2	Serial ports 1-8	RJ45	Asynchronous device connection (RS-232)
3	Serial port A	RJ45	Console, or dial access (RS-232)
4	Serial port B	DB26	Synchronous, or dial access V.35, X.21 or RS-232
5	AUI DB15	DB15	Ethernet LAN connection
6	10BASE2	BNC	Ethernet LAN connection
7	10BASE-T	RJ45	Ethernet LAN connection
8	Power Connector	IEC	Power input

Figure 12: Rear Panel Connector Functions.

Pin Assignments

Serial ports 1-16, Serial port A.

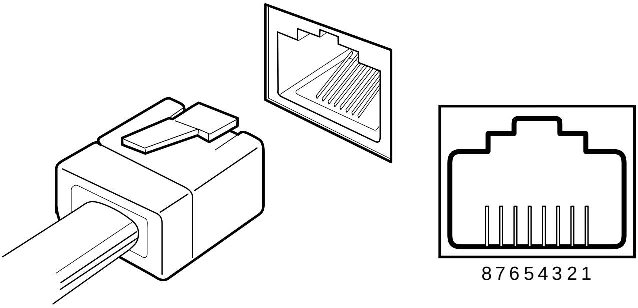


Figure 13: RJ45 Connector.

These ports are wired as a DTE.

Pin	Description	V.24	Direction
1	Data Carrier Detect	109	Input
2	Request To Send	105	Output
3	Data Set Ready	107	Input
4	Transmit Data	103	Output
5	Receive Data	104	Input
6	Signal Ground	102	Ref
7	Clear To Send	106	Input
8	Data Terminal Ready	108	Output

Figure 14: RJ45 Pinout.

Port B

Port B supports synchronous and asynchronous operation and X.21, V.35 and RS-232 physical interface standards. The physical interface will depend on the adapter cable.

V.35

The V.35 adapter cable (Chase part no. 04 011105) provides a DTE interface.

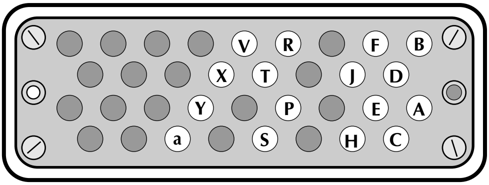


Figure 15: V.35 MRAC Male Connector.

Pin	Description	Type	Direction
A	Shield Ground	-	-
B	Signal Ground	-	-
C	Request To Send	V28	Output
D	Clear To Send	V28	Input
E	Data Set Ready	V28	Input
F	Data Carrier Detect	V28	Input
H	Data Terminal Ready	V28	Output
P	Transmit Data +	V11	Output
R	Received Data +	V11	Input
S	Transmit Data -	V11	Output
T	Receive Data -	V11	Input
V	Receive Clock +	V11	Input
X	Receive Clock -	V11	Input
Y	Transmit Clock +	V11	Input
AA/a	Transmit Clock -	V11	Input

Figure 16: MRAC - V.35 Pinout.

X.21

The X.21 adapter cable (Chase part no. 04 011106) provides a DTE interface.

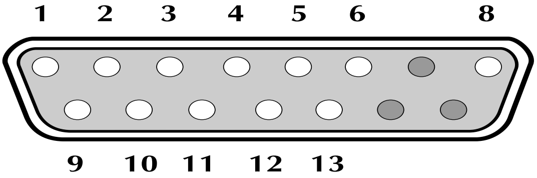


Figure 17: DB15 Male Connector.

Pin	Description	Direction
1	Shield Ground	Ref
2	Transmit Data +	Ouput
3	Control +	Ouput
4	Receive Data +	Input
5	Indicate +	Input
6	Clock +	Input
8	Signal Ground	Ref
9	Transmit Data -	Output
10	Control -	Output
11	Receive Data -	Input
12	Indicate -	Input
13	Clock -	Input

Figure 18: DB15 - X.21 Pinout.

V.24 (RS-232)

The V.24 adapter cable (Chase part no. 04 011101) provides a DTE interface and when used in synchronous mode is only suitable for speeds of up to 56kbps.

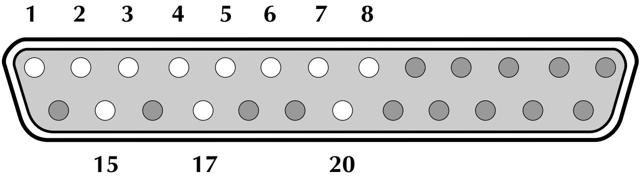


Figure 19: DB25 Male Connector.

Pin	Description	Direction
1	Shield Ground	Ref
2	Transmit Data	Output
3	Receive Data	Input
4	Request To Send	Output
5	Clear To Send	Input
6	Data Set Ready	Input
7	Signal Ground	Ref
8	Data Carrier Detect	Input
15	Transmit Clock	Input
17	Receive Clock	Input
20	Data Terminal Ready	Output

Figure 20: DB25 - V.24 (Synchronous) Pinout.

Cabling - Asynchronous Ports

Any cable used should be shielded to comply with FCC requirements. Ensure that RS-232 cables are not run near fluorescent lighting or electric motors.

Maximum cable length for RS-232 is specified at 60 metres (200 feet) but is proportional to baud rates - the higher the baud rate, the shorter the cable should be. In general, a 19200 bps connection should not be used on cables in excess of 15 metres (50 feet), whereas a 9600 bps signal operates reliably up to a distance of approximately 30 metres (100 feet). Cables of greater lengths could appear to work correctly, but the connection may be unreliable.

Modem Cables

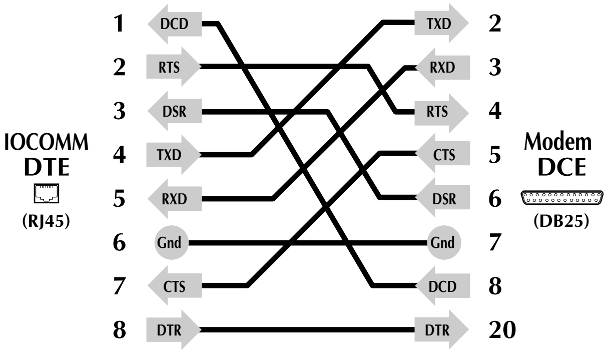


Figure 21: IOCOMM Serial Port Standard Modem Cable (except Port B).

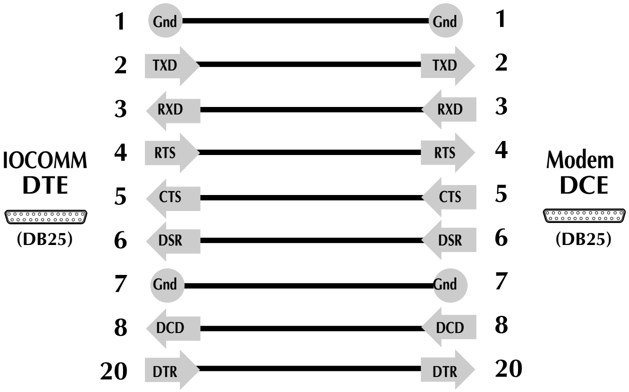


Figure 22: IOCOMM Port B Standard Asynchronous Modem Cable.

Printer / Terminal Cables

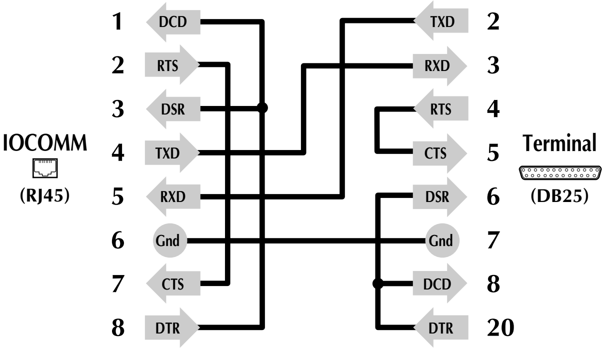


Figure 23: IOCOMM toTerminal (Software Flow Control).

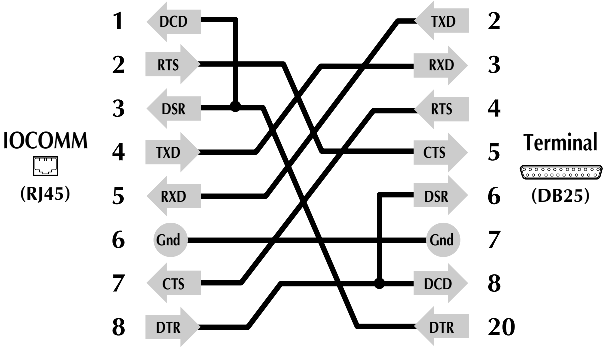


Figure 24: IOCOMM to Terminal (Hardware Flow Control).

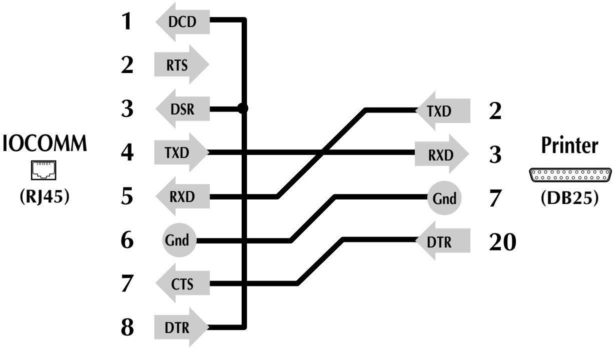


Figure 25: IOCOMM to Printer Cable (typical).

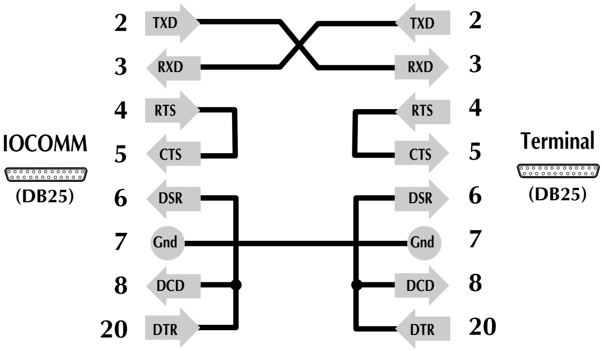


Figure 26: IOCOMM Port B to Terminal (Software Flow Control).

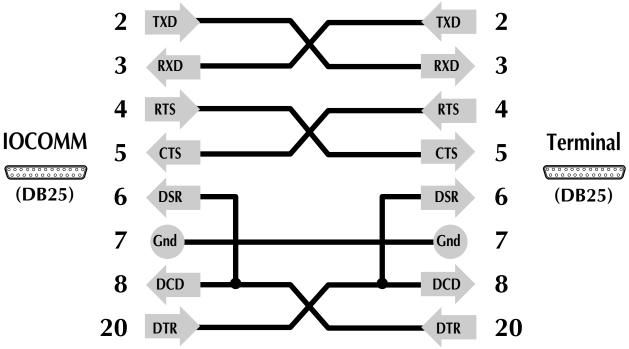


Figure 27: IOCOMM Port B to Terminal (Hardware Flow Control).

Extension Cabling - Synchronous Port B

Port B adapter cables will connect to DCE equipment.

The following cables may be used to extend the reach of the adapter cables.

X.21

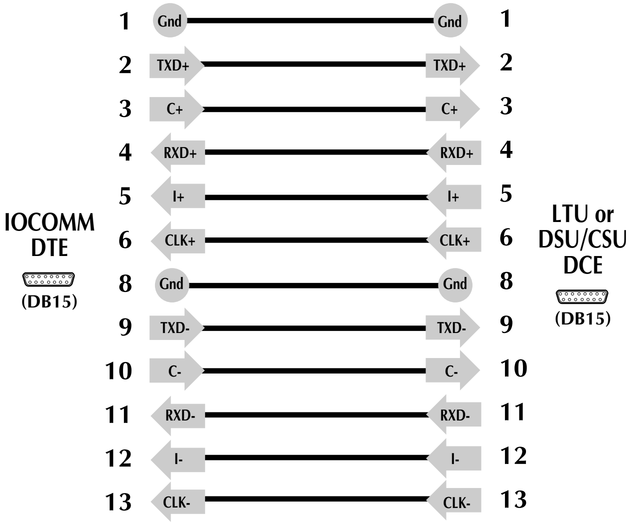


Figure 28: Extension cable from IOCOMM Port B adapter cable to X.21 DCE (e.g. LTU or DSU/CSU).

V.35

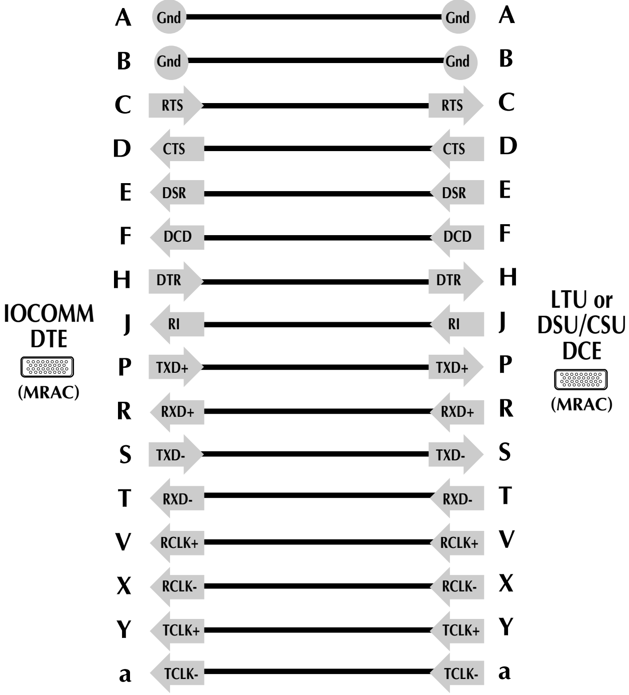


Figure 29: Extension cable from IOCOMM Port B adapter cable to V.35 DCE (e.g. LTU or DSU/CSU).

V.24 (RS-232) Asynchronous

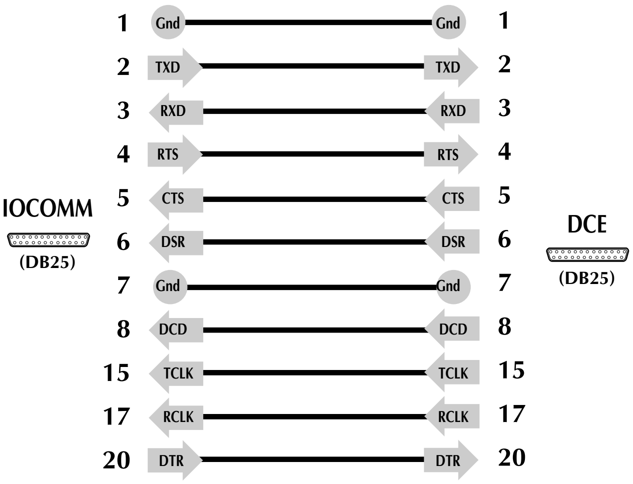


Figure 30: Extension cable from IOCOMM Port B adapter cable to V.24 (RS-232) DCE.

Technical Specification

IOCOMM is a TCP/IP access server for dialled and direct asynchronous connections with T1/E1 leased line interface and router functionality.

Power Requirements

Input range:	110-230V AC +/-10%
Frequency tolerance:	47-63Hz
Power consumption:	40W maximum

Dimensions

Length:	300mm (including BNC connector)
Width:	440mm (480mm with brackets)
Height:	46mm (43mm without feet) Suitable for 19" rack (1U) or desktop mounting
Mass:	4.0kg (unit only, 8 port) .2kg (unit only, 16 port)

Environment

Operational:

Temp:	+5 deg.C to +50 deg.C
Humidity:	0% to 90% RH non-condensing
Altitude:	-500 ft to 15000 ft

Non-operational:

Temp:	-30 deg.C to +80 deg.C
Humidity:	5% to 95% RH non-condensing

Approvals

Electromagnetic:	Emmission:	EN55022:1995, Class B
	Immunity:	EN50082-1:1992
Safety:		EN60950:1992/A2:1993 including all National Deviations CSA CAN/CSA C22.2 No:950-95 UL1950
Telecommunications:		TBR 1:October 1995 and TBR 2: January 1997 in accordance with CTR 1 and CTR 2 (97/544/6C and 97/545/6C) BABT approval number: 608707

Interfaces

Serial:	Ports 1-8/16:	RS-232 (V.24/V.28) asynchronous interface wired as DTE with TXD, RXD, DTR, DSR, DCD, RTS, CTS and GND signals. Surge suppressed. Speed range 300bps to 115.2kbps.
	Port A:	RS-232 (V.24/V.28) port wired as DTE with TXD, RXD, DTR, DSR, DCD, RTS, CTS and GND wired. Surge suppressed. Speed range 300bps to 460.8kbps.
	Port B:	X.21, V.35 or RS-232 (depending on adapter cable purchased) port wired as DTE. Asynchronous and synchronous operation. Surge suppressed. Synchronous speed range 600bps to 2.048Mbps. Asynchronous speed range 300bps to 460.8kbps.

For signals included refer to *Connectors and Cabling*.

Ethernet:

A single 10Mbps interface with the following run-time options for physical interface: 10BASE2, 10BASE-T, AUI

Protocol Support

Network protocols:	TCP/IP UDP ICMP
Address and Settings Discovery:	ARP Proxy ARP BOOTP DHCP
Download:	TFTP
Serial Line Protocols: (Ports 1-8/16, Port A and Port B)	SLIP CSLIP PPP (including PAP and CHAP and only supporting IP)
Routing:	Unit performs IP routing between interfaces, including leased line. Dial-on-demand IP routing to remote sites. RIP RIP-2
Management:	HTML/HTTP SNMP MIB1, MIBII (some restrictions on parameter manipulation) Telnet to CLI (some restrictions on parameter manipulation) FLASH upgradable firmware

Applications:	Telnet Rlogin Syslog DNS
Authentication:	RADIUS (authentication and accounting) Internal authentication database PAP CHAP
Printer:	LPD Telnet

Glossary of Terms

ARP

Address Resolution Protocol (RFC826). This is the method by which ethernet network devices match IP addresses to ethernet addresses.

BOOTP

Bootstrap Protocol (RFC951). This protocol describes how a unit which knows little or nothing about its own IP network configuration can send out a broadcast packet and a server shall respond with various network settings.

CHAP

Challenge Handshake Authentication Protocol. An authentication standard that is part of PPP.

CSLIP

Compressed Serial Line Internet Protocol. See also SLIP.

DHCP

Dynamic Host Control Protocol (RFC1531). This is the next step on from the BOOTP protocol, (see BOOTP above). It specifies extra network settings to be passed to the network device requesting the information; it also allows for a dynamic configuration environment.

DNS

Domain Name Server.

FQDN

Fully Qualified Domain Name. See also DNS.

Gateway

Historically, in the Internet culture, this has been used to refer to something which is actually an IP router, although in modern terminology it refers to a device which stores and forwards data between dissimilar networks.

HTML

Hyper Text Markup Language.

HTTP

Hyper Text Transfer Protocol.

ICMP

Internet Control Message Protocol. Implemented at the IP layer, ICMP is used between gateways and hosts to report errors and make routing suggestions.

IEEE

Institute of Electrical and Electronics Engineers. Most noteable as a standards body

IP

Internet Protocol.

Link

An HTML reference to a URL. These are embedded within most HTML documents.

Loopback

A method by which data can be transmitted and received at a unit without it appearing to the outside world. Most useful when testing interfaces.

MOTD

Message of the Day. A textual message sent to all ports that have this option enabled.

MRU

Maximum Receive Unit. The maximum packet size which can be received over an interface. See also PPP.

MTU

Maximum Transmission Unit. The maximum packet size which can be transmitted over an interface. See also PPP.

NAS

Network Access Server. See also RADIUS.

Netmask

A 32 bit number (normally represented in hex) containing one bits for the network ID and subnet ID, and zero bits for the host ID. Used to route packets between subnets.
See also **Subnet**.

Netscape A company which produces a web browser products called Navigator and Communicator.

PAP Password Authentication Protocol. An authentication standard which is part of PPP.

PPP Point to Point Protocol.

Port This term can be equally valid when referring to a serial port or a network port. The serial port shall be a hardware device with a connector, whereas the network port is an assigned number based on Internet standards. For instance, a Telnet session from serial connector 4 would be utilising serial port 4 and network port 23 (at the host end) at the same time.

RADIUS Remote Authentication Dial In User Service. A protocol designed by Livingston.

RFC Request For Comments. These are a set of documents used within the Internet Community to design protocol implementations. Although they are not strictly specifications in the same sense as an IEEE specification, they are still adhered to by the main manufacturers of Internet products. They are generated and controlled by the Internet Engineering Task Force (IETF).

RIP Routing Information Protocol.

RS232 A serial data transfer protocol.

RS422 A serial data transfer protocol, using balanced line drivers and receivers.

Rlogin Remote Login. A BSD protocol similar to Telnet.

SLIP Serial Line Internet Protocol.

SNMP Simple Network Management Protocol.

Subnet Sub-network. IP networks of the same network class address may be split into subnets using gateways or routers to communicate with other subnets. See also Netmask.

Supernet Multiple network addresses, within the same class, described by a single routing entry.

Syslog System Logger. A BSD system logging protocol.

TCP Transmission Control Protocol.

TFTP Trivial File Transfer Protocol. Used to download and upload files over the network.

Telnet The remote terminal protocol.

UART Universal Asynchronous Receiver Transmitter. A chip used to control serial data transfer. Tends to be used as a generic term referring to any serial controller, whether or not it is an asynchronous only device.

UDP User Datagram Protocol. Insecure protocol sitting above IP in the network stack, analagous to TCP.

URL Universal Resource Location. Part of the HTTP protocol.

Three cables are available to adapt port B to the synchronous (leased line) or asynchronous (dialled connections) interface required.

The Port B adapter cables are:

Description	**Chase Part No:**
V.35 DTE adapter cable with male MRAC connector (for connection to synchronous DCE)	04 011170
X.21 DTE adapter cable with male DB15 connector (for connection to synchronous DCE)	04 011180
RS-232 DTE adapter cable with male DB25 connector (for connection to synchronous or asynchronous DCE)	04 011130
RS-232 null modem adapter cable with female DB25 connector (for connection to asynchronous DTE)	04 011140
RS-232 null modem adapter cable with female DB9 connector (for connection to asynchronous DTE)	04 011150
RS-232 null modem adapter cable with male RJ45 connector (for connection to asynchronous DTE)	04 011160

RJ45 connectors are used on ports 1-8/16 and port A of the access server to save back panel. We provide convertor cables to present a DB25 DTE male interface.

Description	**Chase Part No:**
RJ45 to DB25 DTE male adapter cable (pack of 4)	04 001480

Quality Customer Service

The Chase Research story is simple - we've been able to read technology trends for over ten years and translate them into affordable, approachable products. By affordable we mean high value products uniquely backed by a lifetime warranty. By approachable, we strive for considerable ease of use in our product designs as well as in our customer service and support systems. Our ultimate goal is to help our business partners and customers win in their marketplace.

However, you may feel that there are certain aspects of our service which we could further improve or there is a matter which you would like us to investigate on your behalf. If you have reason to comment on a Chase Research product or service, or can put forward a suggestion as to how we could improve our services, please contact one of our customer services representatives:

Chase Research PLC, Basingstoke, England, UK
Tel: +44 (0)1256 352260, Fax: +44 (0)1256 810159
e-mail: cust@chaser.co.uk

Chase Research Inc, Nashville, Tennessee, USA
Tel: 800 242 7387 or +1 615 872 0770, Fax: +1 615 872 0771
e-mail: support@chaser.com

Chase Research GmbH, Stuttgart, Germany
Tel: +49 (0)711 7287 155, Fax: +49 (0)711 7287 156
e-mail: support@chaser.de

Chase Research China, Beijing, Peoples Republic of China
Te: +86 10 8685 1058, Fax: +86 10 6848 3355
e-mail: cust@chaser.co.uk

We genuinely value your feedback and we will act upon all comments as quickly and effectively as possible.

Thank You.

Illustration, Layout Design and DTP
by MicroArt, Dorney, UK.

Chase Research PLC
Cedarwood, Chineham Business Park,
Basingstoke, Hampshire, RG24 8WD, UK

Tel: +44 (0)1256 352260
Fax: +44 (0)1256 810159
e-mail: info@chaser.co.uk
Internet: http://www.chaser.co.uk

Chase Research Inc.
545 Marriott Drive, Suite 100, Nashville,
TN 37214, United States

Tel: +1 615 872 0770
Fax: +1 615 872 0771
e-mail: info@chaser.com
Internet: http://www.chaser.com

Chase Research GmbH
Zettachring 6,
70567 Stuttgart, Germany

Tel: +49 (0)711 7287 155
Fax: +49 (0)711 7287 156
e-mail: info@chaser.de

Chase Research China
Room 717, Hua Tong Building,
19a Che Gong Zhuang Xi Road,
Haidian District, Beijing 100044,
Peoples Republic of China

Tel: +86 10 8685 1058
Fax: +86 10 6848 3355
e-mail: infochina@chaser.co.uk