Lucent Technologies
Bell Labs Innovations

CellPipe™ IAD 4S/8S

User's Guide

Part Number: 7820-0715-001
For software version 2.10.2
April 2000

Notice

Every effort was made to ensure that the information in this document was complete and accurate at the time of printing. However, information is subject to change.

Safety, Compliance, and Warranty Information

Before handling any Lucent Access Networks hardware product, read the *Access Networks Safety and Compliance Guide* included in your product package. See that guide also to determine how products comply with the electromagnetic interference (EMI) and network compatibility requirements of your country. See the warranty card included in your product package for the limited warranty that Lucent Technologies provides for its products.

Interference Information: Part 15 of FCC Rules

NOTE: This equipment has been tested and found to comply with the limits.

Security Statement

In rare instances, unauthorized individuals make connections to the telecommunications network through the use of access features.

Trademarks

CellPipe, DSLPipe, DSLTNT, NavisAccess, PathStar, and Stinger are service marks of Lucent Technologies. Other trademarks, service marks, and trade names mentioned in this publication belong to their respective owners.

Limited Warranty

Lucent Technologies provides a limited warranty to this product. See the warranty document included in your product package.

Ordering Information

You can order the most up-to-date product documentation and computer-based training online at http://www.lucent.com/ins/bookstore.

Support Telephone Numbers

For a menu of support and other services, call (800) 272-3634. Or call (510) 769-6001 for an operator.

Feedback

Lucent appreciates your comments, either positive or negative, about this manual. Please send them to techpubs@ascend.com.

Lucent Technologies

Customer Service

Customer Service provides a variety of options for obtaining information about Lucent products and services, software upgrades, and technical assistance.

Finding information and software on the Internet

Visit the Web site at `http://www.lucent.com/ins` for technical information, product information, and descriptions of available services.

Visit the FTP site at `ftp.ascend.com` for software upgrades, release notes, and addenda to this manual.

Obtaining technical assistance

You can obtain technical assistance by telephone, email, fax, modem, or regular mail, as well as over the Internet.

Enabling Lucent to assist you

If you need to contact Lucent for help with a problem, make sure that you have the following information when you call or that you include it in your correspondence:

- Product name and model
- Software and hardware options
- Software version
- If supplied by your carrier, Service Profile Identifiers (SPIDs) associated with your line
- Your local telephone company's switch type and operating mode, such as AT&T 5ESS Custom or Northern Telecom National ISDN-1
- Whether you are routing or bridging with your Lucent product
- Type of computer you are using
- Description of the problem

Calling Lucent from within the United States

In the U.S., you can take advantage of Priority Technical Assistance or you can call to request assistance.

Priority Technical Assistance

If you need to talk to an engineer right away, call (900) 555-2763 to reach the Priority Call queue. The charge of $2.95 per minute does not begin to accrue until you are connected to an engineer. Average wait times are less than three minutes.

Other telephone numbers

For a menu of Lucent's services, call (800) 272-3634. Or call (510) 769-6001 for an operator.

Calling Lucent from outside the United States

You can contact Lucent by telephone from outside the United States at one of the following numbers:

Telephone outside the United States	(510) 769-8027
Austria/Germany/Switzerland	(+33) 492 96 5672
Benelux	(+33) 492 96 5674
France	(+33) 492 96 5673
Italy	(+33) 492 96 5676
Japan	(+81) 3 5325 7397
Middle East/Africa	(+33) 492 96 5679
Scandinavia	(+33) 492 96 5677
Spain/Portugal	(+33) 492 96 5675
UK	(+33) 492 96 5671

For the Asia Pacific Region, you can find additional support resources at `http://apac.ascend.com`

Obtaining assistance through correspondence

Lucent maintains three email addresses for technical support questions. One is for customers in the United States, one is for customers in Europe, the Middle East, and Africa, and one is for customers in the Asia Pacific Region. If you prefer to correspond by fax, BBS, or regular mail, please direct your inquiry to Lucent's U.S. offices. Following are the ways in which you can reach Customer Service:

- Email from within the U.S.—support@ascend.com
- Email from Europe, the Middle East, or Africa—EMEAsupport@ascend.com
- Email from the Asia Pacific Region—apac.support@ascend.com
- Fax—(510) 814-2312
- Customer Support BBS (by modem)—(510) 814-2302

Write to Lucent at the following address:

Attn: Customer Service
Lucent Technologies
1701 Harbor Bay Parkway
Alameda, CA 94502-3002

Important safety instructions

A. GENERAL

1 Read and follow all warning notices and instructions marked on the product or included in the manual.

2 There are no operator serviceable parts within the unit. Refer all servicing to trained service personnel.

3 Product installation should be performed by trained service personnel only.

4 Install only in restricted-access areas in accordance with UL1950, C22.2 No. 950, and IEC60950

5 The maximum recommended operating ambient is 122° F (50° C). Allow sufficient air circulation or space between units when installed in a closed or multiple-rack assembly.

6 Slots and openings in the cabinet are provided for ventilation. To ensure reliable operation of the product and to protect it from overheating, these slots and openings must not be blocked or covered. Installation without sufficient airflow can be unsafe.

7 Equipment mounted in a rack should be distributed to prevent a possible hazardous condition due to uneven loading. The rack should safely support the combined weight of all equipment. This product weighs 2 lbs.

8 The power source has to be adequately rated to assure safe operation of the equipment. The building installation and/or power source must provide overload protection.

9 Protective earth (PE) connection is essential to ensure safe operation before connecting to the power supply and telecommunication network. Do not defeat the purpose of the grounding-type plug by modifying the plug or using an adapter. Use an outlet tester or a voltmeter to check the ac receptacle for the presence of earth ground. If the receptacle is not properly grounded, the installation must not procede until a qualified electrician has corrected the problem.

If the power supply is fed from a power source with no protective-earthing path (such as in certain Nordic countries), connect an earth-grounded copper wire to the dedicated wiring terminal marked with ⏚ (PE symbol) on the chassis. The minimum size of the wire for a CellPipe unit with rated input current not exceeding 6A is AWG 18 and cross-sectional area 0.75 mm^2.

Models with ac power inputs are intended for use with a single-phase three-wire power cord (which includes earthing conductor).

For models with dc power inputs, the protective earth connection must be established by using the dedicated earthing terminal marked with the PE symbol or, if provided, the earthing pin of the input terminal block.

10 Models with dc power inputs must be connected to a -48V dc supply source that is electrically isolated from the ac source in accordance with UL1950, C22.2 No. 950, and IEC60950.

11 For products installed in Nordic countries (except Central Office equipment), a type B plug or permanent connection must be used for connections to the main power supply.

12 Before installing wires to the dc power terminal block, verify that these wires are not connected to any power source. Installing live wires (that is, wires connected to a power source) is hazardous.

13 Do not allow anything to rest on the power cord, and do not locate the product where people will walk on the power cord.

14 Do not attempt to service this product yourself. Opening or removing covers can expose you to dangerous high voltage points or other risks. Refer all servicing to qualified service personnel.

15 General purpose cables are provided with this product. Special cables, which might be required by the regulatory inspection authority for the installation site, are the responsibility of the customer.

16 When installed in the final configuration, the product must comply with the applicable safety standards and regulatory requirements of the country in which it is installed. If necessary, consult with the appropriate regulatory agencies and inspection authorities to ensure compliance.

17 A rare phenomenon can create a voltage potential between the earth grounds of two or more buildings. If products installed in separate buildings are interconnected, the voltage potential might cause a hazardous condition. Consult a qualified electrical consultant to determine whether or not this phenomenon exists.

In addition, if the equipment is to be used with telecommunications circuits, take the following precautions:

- Never install telephone wiring during a lightning storm.
- Never install telephone jacks in wet locations unless the jack is specifically designed for wet locations.
- Never touch uninsulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.
- Use caution when installing or modifying telephone lines.
- Avoid using equipment connected to telephone lines (other than a cordless telephone) during an electrical storm. There is a remote risk of electric shock from lightning.
- Do not use a telephone or other equipment connected to telephone lines to report a gas leak in the vicinity of the leak.

Warning: To reduce the risk of fire, communication cable conductors must be 26 AWG (0.13 mm^2) or larger.

Avertissement: Afin de réduire les risques d'incendie, les fils conducteurs du câble de communication doivent être d'un calibre minimum de 26 AWG (American Wire Gauge), c'est-à-dire d'un minimum de 0,13 mm².

Warnung: Um Feuer-Risiko zu reduzieren, müsssen die Querschnitte der Kommunikationskabel-Leiter 0,13 mm² oder größer sein.

B. SPECIAL REQUIREMENTS

18 Lithium batteries:

Warning: The battery can explode if incorrectly replaced. Replace the battery only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.

Avertissement: Il y a danger d'explosion si la batterie n'est pas remplacée correctement. Remplacer uniquement avec une batterie du même type ou d'un type recommandé par le fabricant. Mettre au rebut les batteries usagées conformément aux instructions du fabricant.

Warnung: Die Batterie kann eventuell explodieren, wenn sie nicht ordnungsgemäß ausgetauscht wird. Ersetzen Sie die Batterie nur mit einer Batterie des gleichen oder eines ähnlichen vom Hersteller empfohlenen Typs. Entsorgen Sie gebrauchte Batterien gemäß den Anweisungen des Herstellers.

19 Mains Disconnect (no power switch):

Caution: The power supply cord is used as the main disconnect device. Make sure that the outlet socket is located/installed near the equipment and is easily accessible.

Attention: Le cordon d'alimentation est utilisé comme interrupteur général. La prise de courant doit être située ou installée à proximité du matériel et être facile d'accès.

Vorsicht: Zur sicheren Trennung des Gerätes vom Netz muß der Netzstecker gezogen werden. Stellen Sie sicher, daß sich die Steckdose in der Nähe des Gerätes befindet und leicht zugänglich ist.

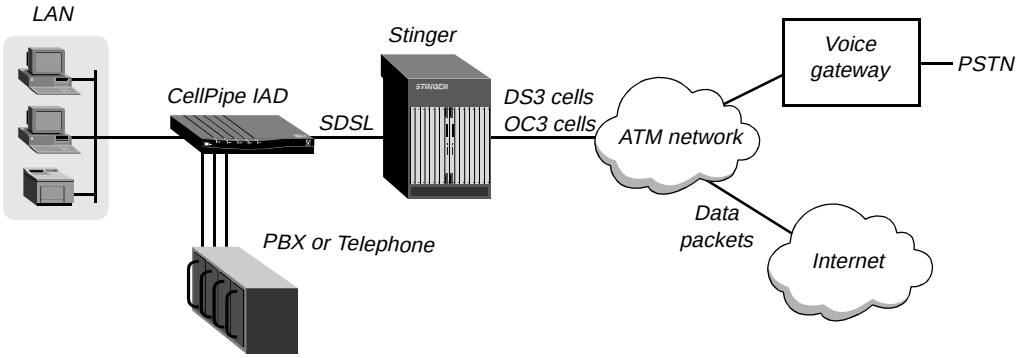
Contents

Introduction

1

What is the CellPipe IAD 4S/8S unit?

The CellPipe™ IAD is a Symmetrical Digital Subscriber Line (SDSL) device that supports bridging and/or routing over the following protocols: Point-to-Point Protocol (PPP), Frame Relay, Asynchronous Transfer Mode (ATM), and HDLC. The CellPipe IAD 4S supports four POTS lines; the CellPipe IAD 8S supports eight POTS lines. The diagram below shows an example of how the CellPipe IAD can fit into your network.



You can use the IAD to create a dedicated, physical connection to Digital Subscriber Line (DSL) equipment at the telephone company. You first attach your computer or Ethernet hub to the IAD unit. Then, you connect the unit to a standard telephone line. The other end of the line connects to DSL equipment at the telephone company. Your DSL circuit is dedicated to your IAD unit. The connection is "always on" at speeds from 144 Kbps to 2.3 Mbps.

With DSL, you have the capacity to transfer data at very high rates. The actual rate can vary according to the type of IAD you use, the distance between the IAD and the DSL equipment, and the line quality of the connection.

You can use the IAD for Internet access, telecommuting, remote office connectivity, multimedia, web hosting, e-commerce, and videoconferencing.

IAD features

The CellPipe IAD 4S/8S includes the following features:

- Support for ATM, PPP over ATM, Frame Relay, HDLC, Voice over DSL
- Support for data rates from 144 Kbps to 2.3 Mbps
- Managed via RS-232 console port, TELNET or SNMP
- Offers static and dynamic IP routing and bridging
- Supports Routing Information Protocol (RIP)
- Management using console port, Telnet, and SNMP
- Network Address Translation (NAT) allows a single IP address to be shared among multiple users
- DHCP provides easy management of LAN addresses
- Support for four POTS lines (IAD 4S) or eight POTS lines (IAD 8S)
- Compatible with the PathStar™ (Lucent's IP-based Class 5 Switch), and the CopperCom and Jetstream voice gateways

IAD management

The IAD is managed through navigating a hierarchy of menus. You set up a serial connection and use VT100 emulation software to display configuration information on your computer monitor and use the computer to enter any changes. Chapter 2 provides details.

Getting Ready to Configure

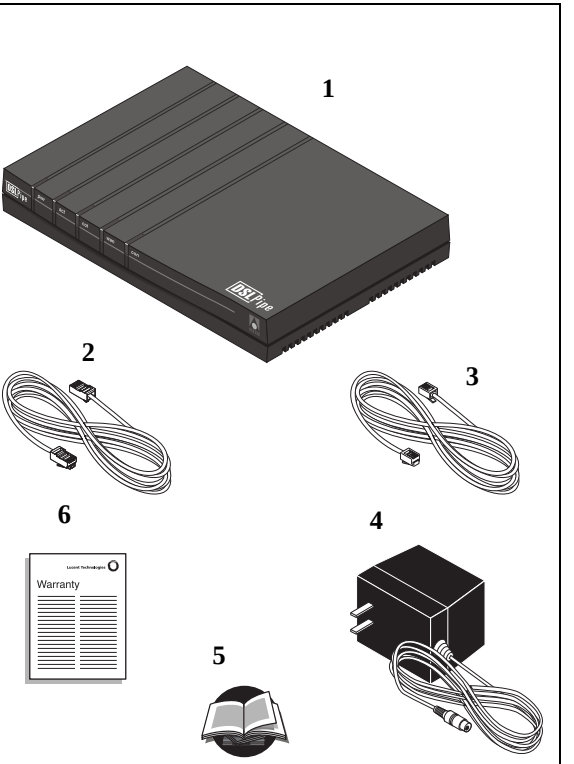
2

The IAD unit is easy to install. Open the package and identify the package contents. Then, set up the cables and verify the activity of the status lights. To configure the unit, establish a serial connection with the IAD and use the command-line interface to specify the configuration.

Checking box contents

The box in which you received your IAD unit should contain the items shown in Figure 2-1.

Figure 2-1. Box contents

1 IAD unit **2** 10BaseT Ethernet crossover cable (yellow) **3** DSL WAN cable with RJ11 modular plug connectors (blue) **4** Power supply ***5*** *CellPipe IAD 4S/8S User's Guide* **6** Warranty card	

Items you need for installation

In addition to the items provided with your IAD unit, you will also need an Ethernet interface and TCP/IP software. If you connect the unit to an Ethernet hub, you also need a straight-through Ethernet cable.

An Ethernet interface

For the IAD to transmit data to and receive data from your computer, your computer must have a properly configured Ethernet interface. The interface can be built into the computer, as it is on many recent Dell, Apple Macintosh, and Macintosh-compatible personal computers, or it can be an add-on circuit board or PCMCIA card (PC card). To install and configure the interface in your computer, follow the documentation included with your computer.

TCP/IP software

To communicate with a remote network, your computer must have the necessary networking software, often referred to as a *stack*.

A TCP/IP stack enables you to connect to the Internet and to other networks that use the same networking standards as the Internet. Many operating systems include software for TCP/IP. If TCP/IP software is not included in your operating system, you need to obtain a separate TCP/IP software package. For information about configuring the TCP/IP software, see the documentation for your operating system or TCP/IP software package.

Straight-through Ethernet cables

If you are connecting a single computer to the IAD and the computer has a 10BaseT (twisted-pair) Ethernet interface, you do not need any additional Ethernet cabling. In this case, you can use the special crossover cable that came with your IAD unit.

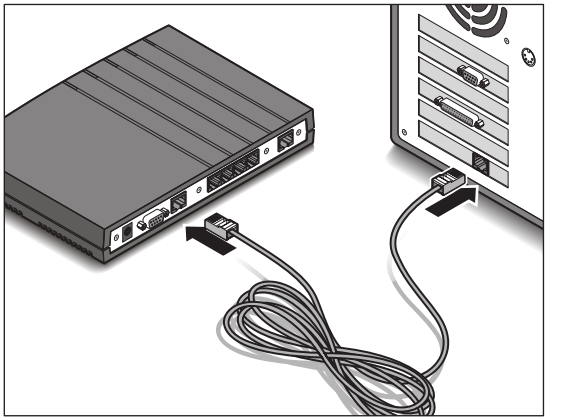
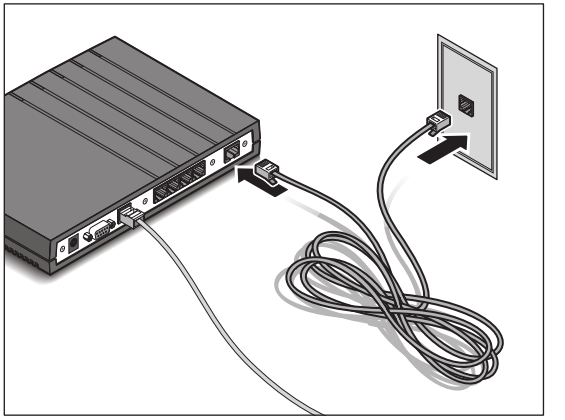
If you are connecting to a 10BaseT Ethernet network that includes a hub, you need one standard 10BaseT cable to connect the IAD unit to the 10BaseT hub and another standard 10BaseT cable to connect the computer to the hub.

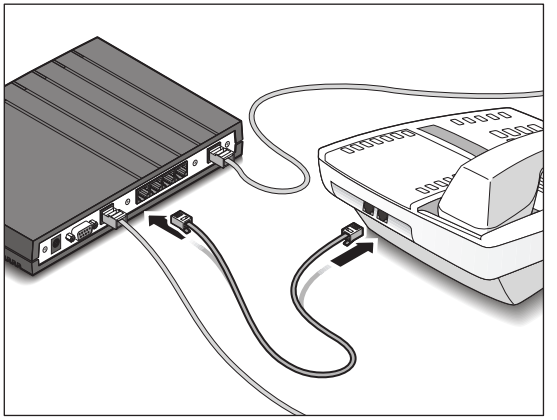
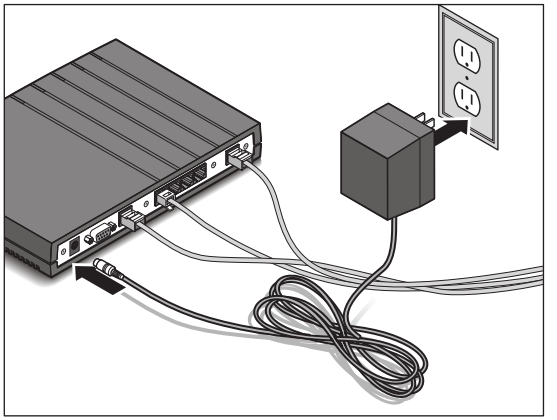
Note: You *cannot* use the 10BaseT crossover cable included in your IAD package for these connections. You can use the crossover cable only for a direct connection between a computer and the IAD, not for a connection to a 10BaseT hub.

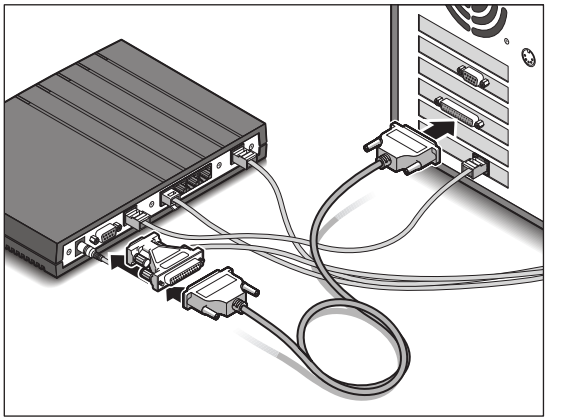
For information about proper cables and termination for a Thicknet (10Base5) or Thinnet (10Base2) Ethernet network, see the documentation for your network.

Connecting CellPipe IAD 4S cables

Follow the instructions in the Description column to connect to the IAD 4S unit.

Description	Illustration
1 Connect the labeled crossover Ethernet cable from the port labeled LAN on the IAD 4S to the Ethernet adapter in your computer. **Note:** To connect the IAD 4S to an Ethernet hub, use your own straight-through Ethernet cable.	
2 Connect the labeled WAN cable to the port labeled WAN on the IAD 4S, and plug the other end into the wall jack.	

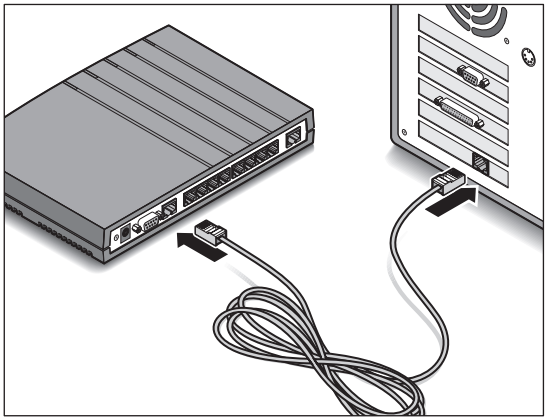
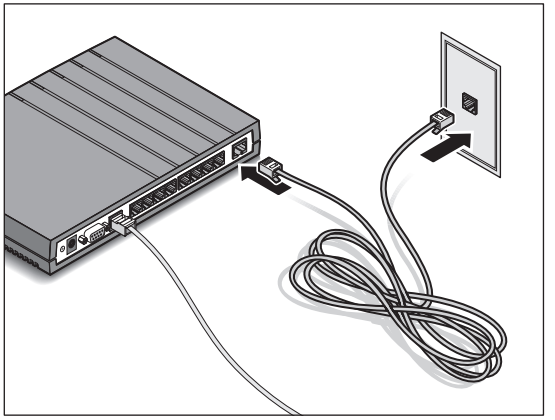
Description	Illustration
3 Connect up to four telephone lines to the four POTS ports.	
4 Connect the power cable to the IAD 4S and plug the other end into a wall outlet. Connect to the wall outlet last. There is no power switch. Connecting the power cable turns on the IAD.	

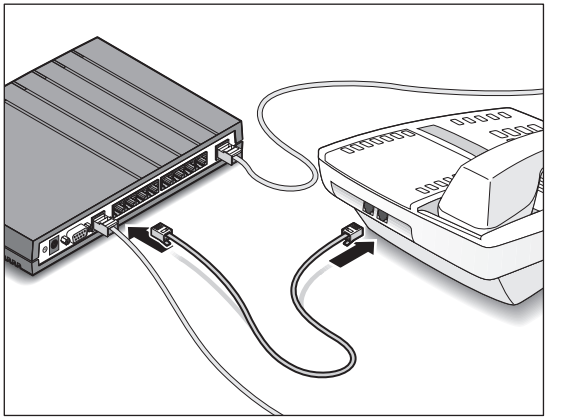
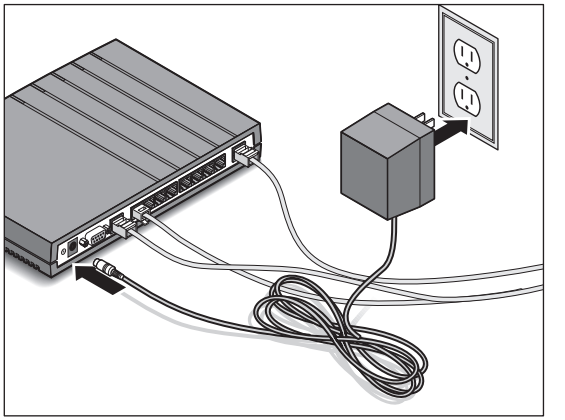
Description	Illustration
5 To configure the IAD 4S, connect a serial cable from the IAD 4S to your computer. You must provide your own serial cable.	

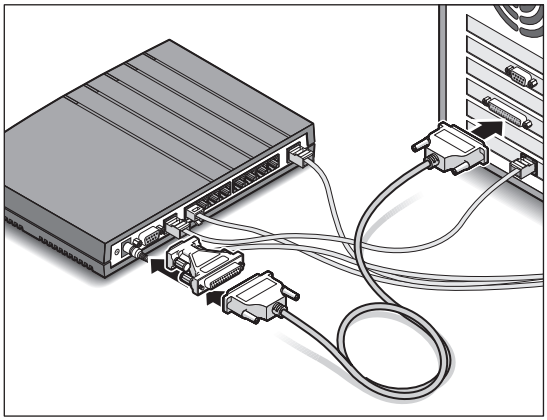
After connecting the cables, go to page 2-10 to check the activity of the status lights.

Connecting CellPipe IAD 8S cables

Follow the instructions in the Description column to connect to the IAD 8S unit.

Description	Illustration
1 Connect the labeled crossover Ethernet cable from the port labeled LAN on the IAD 8S to the Ethernet adapter in your computer. **Note:** To connect the IAD 8S to an Ethernet hub, use your own straight-through Ethernet cable.	
2 Connect the labeled WAN cable to the port labeled WAN on the IAD 8S, and plug the other end into the wall jack.	

Description	Illustration
3 Connect up to eight telephone lines to the eight POTS ports.	
4 Connect the power cable to the IAD 8S and plug the other end into a wall outlet. Connect to the wall outlet last. There is no power switch. Connecting the power cable turns on the IAD 8S.	

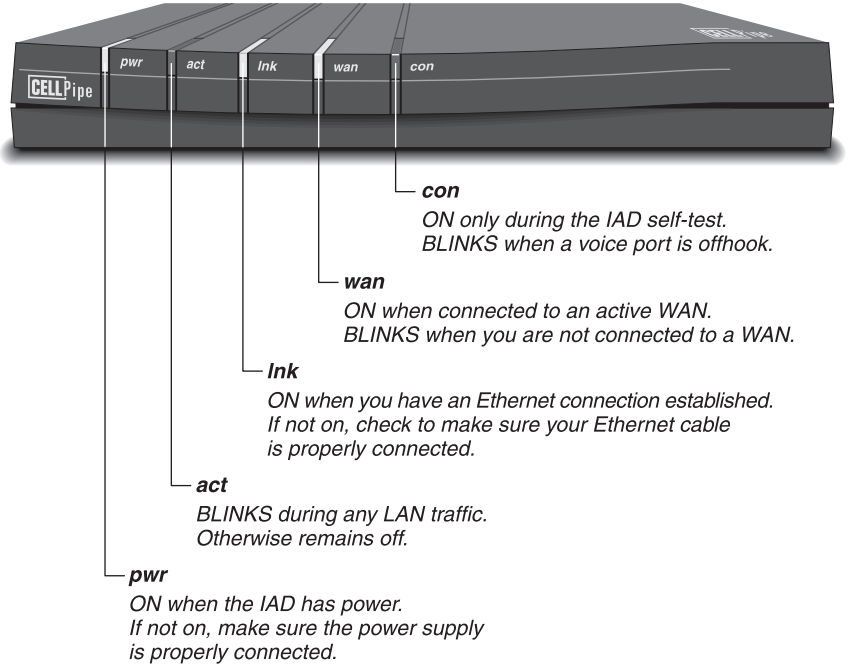
Description	Illustration
5 To configure the IAD 8S, connect a serial cable from the IAD 8S to your computer. You must provide your own serial cable.	

After connecting the cables, go to page 2-10 to check the activity of the status lights.

Checking the activity of IAD status lights

Observe the activity pattern of the lights at the front of the IAD unit to verify that your unit is connected properly. When all the cables are connected, verify that:

- The `pwr` light is on initially and remains on.
- The `wan` light is on initially, blinks until a connection is established, and then remains on.
- The `lnk` light is on if there is an Ethernet connection.
- The `con` light is on initially but does not remain on.



Establishing a connection to the IAD

Before you configure the IAD unit, you must connect to the unit via an American National Standards Institute (ANSI) compatible terminal emulation program (such as HyperTerminal). Once you have assigned the unit an IP address, you can perform further configuration through a telnet connection.

Establishing a connection with an ANSI terminal emulation program

To establish a serial connection with the IAD, you will need a computer with a serial port, a serial cable, and communication software.

A computer with a serial port

To change the default configuration or monitor the IAD, you need a computer with a serial communication port capable of transmitting data at 9600 bps.

The serial communication port is normally one you could use to connect an external modem. If you are not already familiar with your computer's serial ports, see your computer's user guide for more information.

If no serial port is currently free and you cannot add a serial port to your computer, disconnect from one of the serial ports a device that you can temporarily do without (for example, an external modem).

A serial cable

To connect the IAD to your computer's serial port, you need a serial cable (a serial communication cable designed for connecting an external device). The cable must be a *high-speed* cable, that is, one that supports the *hardware handshaking* technique used by almost all recently manufactured modems. The cable must have the appropriate plug for connecting to a serial communication port on your computer and either a 9-pin male D connector at the other end.

Note: When you have finished making configuration changes, you can disconnect the serial cable.

Communications software

Use a communications program (such as HyperTerm, PROCOMM PLUS, Zterm, or any other program that supports VT100 terminal emulation) to open a session directly with the port to which the IAD unit is connected.

Set your communications software to connect with the following settings. If you are not already familiar with the settings listed, see the documentation for your communications software. If you are using the software for the first time, going through an online or printed tutorial is a good way to get started.

- Direct connection—Tell the software that there is a serial cable connecting the IAD directly to the computer.
- Serial port— Specify which of the computer's serial ports the software uses. If the only serial port available is currently used by an internal modem, you may need to use your computer's setup software to specify an external connector for the port that will be used in place of the internal modem. In some cases, you also may need to remove the modem. See the manual for the modem and your computer's user manual for details.
- Terminal type— Specify VT100.
- Duplex— If the software lets you choose, specify Full. Because this is by far the most common choice, most communications software sets this by default.
- Bits per second— Specify 9600.
- Data bits—Specify 8.
- Parity— Specify None.
- Stop bits— Specify 1.
- Flow control— Turn *off* software flow control (XON/XOFF) and, if possible, hardware flow control (RTS/CTS). Specify None.

When you establish the connection, the command-line interface appears.

Establishing a Telnet connection

To set up an IP address, proceed as follows:

Setting up an IP address

To set up an IP address, follow these steps:

1. Follow the instructions in "Establishing a connection with an ANSI terminal emulation program" on page 2-11 to establish a connection.
2. From the Main Menu, choose Configure IP Router.
3. Choose Configure Port IP Address.
4. Choose 100BaseT Ethernet.
5. Specify the connection number. Each connection specifies a PVC. You can configure up to eight PVCs per port.
6. Type the IP address.
7. Type the subnet mask address.

Note: The IAD interface displays a default or last-used value in parentheses to the left of the command prompt. To accept the value, press the Enter key. For example:

```
Enter a new subnet mask for this interface:
(255.255.255.0) ->
```

When you press the Enter key, the IAD sets 255.255.255.0 as the subnet mask value.

8. To save the configuration, choose Yes. To discard changes, choose No.
9. Press Esc until the Main Menu appears. Choose R to restart the IAD. Changes made are stored in Flash ROM. You must restart the IAD for the changes to register.

Using Telnet to connect

After you set up an IP address, you can use Telnet to connect to and configure the IAD.

Command-line interface

After you establish a connection to the IAD through the Hyperterminal program or Telnet, your VT100 terminal displays the following command-line interface:

```
Main Edit Menu
1. Reports Menu
2. Configure IP Router
3. Configure Bridge
5. Configure WAN
6. Configure LAN
7. Configure SNMP
8. Configure Login
9. System Utilities
D. Configure DHCP Server
N. Configure NAT

S. DSP Utilities

R. Reset System

M. Set Ethernet MAC
T. Display Fast-ENET Controller
P. VoicePath Configure
```

There are no initial values for the User ID and password. If you are accessing the command-line interface for the first time, press Enter twice. Use the Configure Login menu to set values for the User ID and Password. The default password for Supervisor is `supervisor`.

Navigating within the IAD window

Opening a menu

To open a menu, type the number or letter that corresponds to the menu. For example, type 1 to choose the Reports menu.

Assigning a value

To assign a value in a menu option, type the value and press the Enter key. If an existing value displays and you want to accept this value, just press the Enter key.

Returning to a previous menu

Press Escape to return to the previous menu.

Saving changes

When you change a configuration setting, the changes are automatically saved as you make them. However, the changes are not activated until you reset the IAD. Select Reset System from the Main Menu to reset the IAD.

Configuring the IAD

3

In order to configure the IAD unit, you must first choose ATM or Frame Relay as the datalink protocol, and configure the PVCs. You must then configure IP addresses for each port you defined. You can also enable or disable bridging by port. You can then configure RIP, DHCP, or NAT.

You can also enable SNMP and configure a login/password for the IAD.

Note: In order for any configuration changes to take effect, you must reset the IAD. From the Main Menu, choose Reset System.

Configuring physical ports (datalink protocols)

You can choose ATM or Frame Relay as the datalink protocol. Your choice determines the method you use to set up PVCs. If you choose ATM, you must specify a VPI and a VCI. If you choose Frame Relay, you must specify the DLCIs. You can

establish up to eight PVCs (permanent virtual connections) with your IAD. Each PVC establishes a port.

To choose the datalink protocol, follow these steps:

1 From the Main Menu, choose Configure WAN.

2 Choose Configure Datalink Protocol.

3 Choose ATM or Frame Relay.

4 Press Esc to return to the WAN Configuration menu. If you selected ATM encapsulation, see "Using ATM" on page 3-2. If you selected Frame Relay encapsulation, see "Using Frame Relay" on page 3-3.

Using ATM

If you selected ATM, follow these steps to set up the ATM PVCs:

1 From the WAN Configuration menu, choose Configure PVCs.

2 Choose Add New PVC.

3 Type a value for the VPI (virtual path identifier).

4 Type a value for the VCI (virtual circuit identifier).

5 Choose the ATM encapsulation. If you are configuring a voice PVC, follow these steps:

- If you are using a CopperCom or Jetstream voice gateway, you *must* choose the Proprietary Voice option. The ATM Peak Cell Rate (PCR) is automatically determined by the IAD.
- If you are using Lucent's PathStar, choose the RFC 1483 option.
  - You must choose CBR (Constant Bit Rate) as the service category. This guarantees that voice has priority.
  - Specify an ATM PCR. The PCR will depend on the number of POTS ports you are using, and the number of POTS ports supported by the voice gateway. The IAD automatically computes a value for you. You can select this value or you can enter another value. If you are configuring only one voice PVC and using four POTS lines, you can specify a PCR of 2000. If

you are configuring one voice PVC and using eight POTS lines, you can specify a PCR of 4000.

Note: For more information on configuring the IAD for voice, refer to Chapter 4, "Voice Gateway Configuration."

6 If you are configuring a data-only PVC, choose RFC 1483 and then choose the UBR (Unspecified Bit Rate) service category. You can also specify PPP over ATM (RFC 2364).

7 If Payload Scrambling is enabled in the Stinger (Lucent's DSLAM), you must also enable Payload Scrambling in the IAD. Payload Scrambling is normally enabled in the Stinger. From the WAN configuration menu, choose Payload Scrambling and type E to enable this option.

Using Frame Relay

1 From the WAN Configuration menu, choose Configure DLCIs.

2 Choose Add New DLCI.

3 Choose the port number.

4 Type a value for the DLCI.

5 Choose the Frame Relay encapsulation.

- If you are configuring a voice PVC and you are using a CopperCom or Jetstream voice gateway, you must choose the Proprietary Voice DLCI option. You cannot use Lucent's PathStar with Frame Relay.
- If you are configuring a data-only PVC, you can select RFC 1490.

6 Set the transmit rate, receive rate, and congestion parameters as needed. Ask your Service Provider for the values supported.

7 Repeat step 2 through step 6 for each Frame Relay PVC you want to set up.

Configuring the IAD for bridging

Bridging is used primarily to provide connectivity for protocols other than IP although it can be used to join segments of IP networks. Because a bridging connection forwards packets at the hardware-address level (link layer), it does not distinguish between protocol types, and it requires no protocol-specific network configuration.

Bridging is very easy to configure. It is commonly used to:

- Provide nonrouted protocol connectivity with another site
- Link two sites so that their nodes appear to be on the same LAN

Since bridges examine all packets on the LAN, they incur greater processor and memory overhead than do routers. On heavily loaded networks, the increased overhead can result in slower performance.

How the IAD unit initiates a bridged WAN connection

When you configure the IAD unit for bridging, it accepts all packets on the Ethernet network and forwards only those that have one of the following:

- A physical address that is not on the segment connected to the IAD unit
- A broadcast address

Bridging uses physical or broadcast addresses, not logical (network) addresses.

Physical addresses and the bridge table

A physical address is a unique, hardware-level address associated with a specific network controller. A device's physical address is also called its Media Access Control (MAC) address. On an Ethernet network, the physical address is a six-byte hexadecimal number assigned by the Ethernet hardware manufacturer, as in:

```
0000D801CFF2
```

If the IAD unit receives a packet whose destination MAC address is not on the local network, it checks its internal bridge table. If it finds the packet's MAC address, the unit bridges the packet. If it does not find the address, the unit checks for active sessions that have bridging enabled. If there are active bridging links, it forwards the packet across *all* active sessions that have bridging enabled. Otherwise, it drops the packets.

Broadcast addresses

A broadcast address is recognized by multiple nodes on a network. For example, the Ethernet broadcast address at the physical level is FFFFFFFFFFFF. All devices on the same network receive all packets with the destination address.

As a router, the unit discards broadcast packets. As a bridge, it forwards packets with the broadcast destination address across all active sessions that have bridging enabled.

Enabling bridging

The IAD unit has a global bridging parameter that must be enabled for any bridging connection to work. The bridging parameter causes the IAD unit's Ethernet controller to run in promiscuous mode. In promiscuous mode, the Ethernet controller accepts all packets, regardless of address or packet type, and passes them up the protocol stack for a higher-layer decision on whether to route, bridge, or reject the packets.

To enable bridging globally, follow these steps:

1 From the Main Menu, choose the Configure Bridge menu.

2 Choose Enable/Disable Bridging globally.

3 Type Y to enable bridging.

To enable bridging by port, follow these steps:

1 Verify that the Enable/Disable Bridging globally parameter is set to Y.

2 Choose Enable/Disable Bridging by Port.

3 Choose 100BaseT Ethernet.

4 Choose Y to enable the port for bridging.

5 Choose Enable/Disable Bridging by Port.

6 Choose SDSL.

7 Choose the port for which you want to enable bridging. For example, you can choose to bridge to your corporate network.

8 Choose Y to enable the port for bridging.

9 Repeat step 5 through step 8 for any other ports that will be bridging.

10 You must reset the IAD for these changes to take effect. Choose Reset System from the Main Menu.

You can also enable Spanning Tree and Configure Spanning Tree by Port. For a description of these parameters, see "Configure Bridge menu" on page 5-10.

Assigning IP addresses to ports

If your IAD will only be bridging, you do not need to assign IP addresses. If you are routing, however, you must define the PVCs more specifically.

A router moves data toward its destination over the most efficient path it knows. The router keeps track of the source and destination addresses of packets it handles, builds tables with this information, collects information from the routing tables of other routers, and can advertise its own routes.

The most common uses for IP routing connections in the IAD unit are to:

- Enable IP connections to the Internet (through Internet Service Providers).
- Connect distributed IP subnets to a corporate backbone (telecommuting and remote office hubs).

The IAD supports IP routing over Frame Relay and ATM connections. IP routing connections have a level of built-in authentication, because the IAD matches its own configured IP address to the source IP address.

How the IAD uses its routing table

The IAD creates a routing table when it powers up. It adds all known routes to the table, including connected routes and routes configured in its resident profiles and Static Routes profiles. If RIP is enabled in the Ethernet network, it supplies the routing table with information about routes learned from local routers.

When the IAD receives an IP packet whose destination address is not on the local network, it checks its routing table for the destination network and:

- If it finds a route to that network, it forwards the packet to the gateway indicated by that route. If the gateway is not local, the IAD forwards the packet.
- If it does not find a route to that network, it forwards the packet to the default router.
- If it does not find a route to that network and no default route has been configured, it drops the packet.

Configuring ports

To configure the IAD unit's WAN port, follow these steps:

1. From the Main Menu, choose Configure IP Router.
2. Choose Configure Port IP Address.
3. Choose SDSL.
4. Choose the port for which you want to assign an IP address.
5. Enter an IP address, a subnet mask, and type Y to save.

To configure the IAD unit's LAN port, follow these steps:

1. From the Main Menu, choose Configure IP Router.
2. Choose Configure Port IP Address.
3. Choose 100BaseT Ethernet.
4. Choose the connection for which you want to assign an IP address.

Note: If you are using a DHCP server to dynamically obtain an IP address for a port, do not enter an IP address for that Ethernet port.

5. Enter an IP address, a subnet mask, and type Y to save.
6. Repeat step 1 through step 5 for each LAN port you want to configure. You can configure up to eight ports.
7. You must reset the IAD for these changes to take effect. Choose Reset System from the Main Menu.

You can also create a static route, enable/disable RIP, and configure a DNS client from the Router Configuration menu.

Static and dynamic routes

A static route is a path from one network to another. The route which specifies the destination network and the router to use to get to that network. A dynamic route is a network-to-network path to another network that is *learned* dynamically rather than configured in a profile. A router that uses RIP broadcasts its entire routing table every 30 seconds, updating other routers about which routes are usable. Hosts that run ICMP can also send ICMP Redirects to offer a better path to a destination network.

Configuring static routes

To configure a static route, follow these steps:

1. From the Main Menu, choose Configure IP Router.
2. Choose Add/Remove a Static Route.
3. Choose Add a Static Route.
4. Enter the destination address, the network mask, and the IP address of the gateway.
5. Choose Y to save.
6. You must reset the IAD for these changes to take effect. Choose Reset System from the Main Menu.

Configuring the default route

If no routes exist for the destination address of a packet, the IAD forwards the packet to the default route. Most sites use the default route to specify a local IP router (such as a UNIX host running the `route` daemon).

Note: If there is no default route, the IAD drops packets for which it has no route.

To configure the default route, follow these steps:

1. From the Main Menu, choose Configure IP Router.
2. Choose Add/Remove a Static Route.
3. Choose Add/Change the Default Route.
4. Type the gateway address for the default route.
5. Type Y to save.
6. You must reset the IAD for these changes to take effect. Choose Reset System from the Main Menu.

Configuring RIP

Routing Information Protocol (RIP) is a way in which a router periodically broadcasts the contents of its table to other routers in order to maintain a synchronized database.

To enable RIP in the IAD, follow these steps:

1. From the Main Menu, choose Configure IP Router.
2. Choose Enable/Disable RIP.
3. Choose Y to enable RIP.

To enable RIP by port, follow these steps:

4. Choose Configure RIP Version by Port.
5. Choose 100BaseT Ethernet, and choose a port number.
6. Choose from the following settings:
   - Disabled
   - Version1 Broadcast
   - Version 2 Broadcast
   - Version 2 Multicast.
7. Type Y to save.
8. You must reset the IAD for these changes to take effect. Choose Reset System from the Main Menu.

Configuring the DNS server

Domain Naming System (DNS) is a mechanism for translating names of computers into IP addresses. DNS enables you to, for example, use the Internet without remembering long lists of IP addresses. To make DNS services available to the IAD, you must specify the IP address of a DNS server.

To specify the DNS server's IP address, follow these steps:

1. From the Main Menu, choose Configure IP Router.
2. Choose Configure DNS Client.
3. Choose Configure DNS Server IP Address.
4. You must reset the IAD for these changes to take effect. Choose Reset System from the Main Menu.

You can also use the DNS Client menu to specify the DNS server timeout value. The default value is 5 seconds.

Configuring DHCP

Dynamic Host Configuration Protocol (DHCP) allows workstations to get temporary IP addresses from centrally administered servers. The IP addresses are assigned or *leased* to the workstation on the fly.

You can configure the IAD to be a DHCP server or a DHCP client.

Configuring the IAD to be a DHCP server

To configure the IAD to be a DHCP server, follow these steps:

1 From the Main Menu, choose Configure DHCP Server.

2 Choose Enable/Disable DHCP.

3 Choose Y to enable DHCP. If this setting is set to N, all other DHCP settings are ignored.

To specify DHCP configuration, follow these steps:

1 From the Main Menu, choose Configure DHCP Server.

2 Choose Configure DHCP Server parameters.

3 Choose 100BaseT Ethernet.

4 Identify the DHCP server that will assign a temporary IP address to the IAD. Type a value for each of the following parameters:

- Gateway IP Address
- DNS Server IP Address
- Subnet Mask Address
- Domain Name
- Lease time. The duration for which an IP address will be leased to the IAD. Enter a value in seconds. An interval of at least 3600 seconds (1 hour) is recommended. For a permanent DHCP lease, specify a value of `-1`.

5 Choose Configure DHCP Address Range Pool. Specify a high IP address and a low IP address. The DHCP server will assign IP addresses based on this range.

6 You must reset the IAD for these changes to take effect. Choose Reset System from the Main Menu.

Configuring the IAD to be a DHCP Client

To configure the IAD to be a DHCP client, follow these steps:

1 From the Main Menu, choose Configure IP Router.

2 Choose Configure DHCP Client.

3 Choose SDSL.

4 Choose the port number.

5 Choose Y to enable DHCP for the port. Repeat for each port that will be enabled for DHCP.

6 You must reset the IAD for these changes to take effect. Choose Reset System from the Main Menu.

Configuring NAT

To connect to the Internet or any other TCP/IP network, a host must have an IP address that is unique within that network. The Internet and other large TCP/IP networks guarantee the uniqueness of addresses by creating central authorities that assign official IP addresses. However, many local networks use private IP addresses that are unique only on the local network. To enable a host with a private address to communicate with the Internet or another network that requires an official IP address, an IAD unit can perform a service known as Network Address Translation (NAT). NAT works as follows:

- When the local host sends packets to the remote network, the IAD automatically translates the host's private address on the local network to an official address on the remote network.
- When the local host receives packets from the remote network, the IAD automatically translates the official address on the remote network to the host's private address on the local network.

The IAD can perform NAT in the following ways:

- For more than one host on the local network, without borrowing IP addresses from a DHCP server on the remote network.
- When the remote network initiates the connection to the IAD.

- By routing packets it receives from the remote network, for up to 10 different TCP or UDP ports, to specific hosts and ports on the local network.

With NAT, the IAD is the only host on the local network that is visible to the remote network.

Note: NAT automatically turns RIP off, so the address of the IAD is not propagated to the Internet or remote networks.

Address translation

The IAD can perform NAT for multiple hosts on the LAN by using its own IP address. The IAD can route incoming packets, for up to 10 different TCP or UDP ports, to specific servers on the local network. Translations between the local network and the Internet or remote network are static and need to be preconfigured. You need to define a list of local servers and the UDP and TCP ports each server is to handle.

For example, you can configure the IAD to route all incoming packets destined for TCP port 80 (the standard HTTP port) to port 80 of the World Wide Web server on the local network.

When you configure the IAD to route incoming packets destined for a particular TCP or UDP port to a specific server on the LAN, multiple hosts on the remote network can connect to the server at the same time. The number of connections is limited by the size of the translation table.

NAT has an internal translation table limited to 500 addresses. A translation-table entry represents one TCP or UDP connection.

Note: A single application can generate many TCP and UDP connections.

The IAD removes entries from the translation table on the basis of the following timeouts:

- TCP translations time out after 300 seconds.
- UDP translations time out after 300 seconds.

Configuring NAT

To configure NAT on the IAD, follow these steps:

1. From the Main Menu, choose Configure NAT.
2. Choose Enable/Disable NAT Translation by Port.
3. Choose SDSL.
4. Choose each port for which you want to enable NAT and type Y.
5. From the Main Menu, choose Reset System to reset the IAD.

After enabling the ports for NAT, you are ready to specify NAT configuration by port. Follow these steps:

1. From the Main Menu, choose Configure NAT.
2. Choose Configure NAT Local Server Entry.
3. When prompted for Local Server Entry to Configure, type 1. (You can configure up to 10 TCP or UDP ports.)
4. Type the NAT Local Server Translated IP address. This is the IP address that will be translated to a TCP or UDP port number when the IAD unit operating in NAT mode.
5. Type the number of the port that will be translated.
6. Type the number of the port that it will be translated to.
7. Choose either the TCP or UDP protocol.
8. Repeat step 1 through step 6 for each port you want to configure for NAT. You can configure up to 10 entries.
9. Use the Configure NAT Port Range parameter to specify the lowest and highest port value that you will use.

Note: To delete any entries you have configured, choose Delete NAT Local Server Entry from the NAT Configuration menu.

10. (Optional) Use the Configure NAT TCP Timeout or the Configure NAT UDP Timeout parameters to change timeout values for TCP or UDP, respectively. The default timeout value is 300 seconds.
11. You must reset the system for the changes to take effect. From the Main Menu, choose Reset System.

Configuring SNMP

The IAD supports Simple Network Management Protocol (SNMP). An SNMP management station can query the IAD, set some parameters, sound alarms when certain conditions appear in the IAD, and so forth.

To configure SNMP, follow these steps:

1 From the Main Menu, choose Configure SNMP.

2 Choose Enable/Disable SNMP, then choose Y to enable SNMP.

3 Enter the value for the System Contact, System Location, System Name, SNMP Community. Type a value for the SNMP Trap Host IP Address.

4 You must reset the IAD for these changes to take effect. Choose Reset System from the Main Menu.

Configuring Login

When the IAD unit is shipped from the factory, its security features are set to defaults that enable you to configure and set up the unit without any restrictions. When prompted for the login and password the first time you access the Command-Line interface, just press the Enter key.

To set up a login and password, follow these steps:

1 From the Main Menu, choose Configure Login.

2 Set the User ID, User Password, and NetMan Password parameters.

Voice Gateway Configuration

4

Your IAD configuration will vary depending on the voice gateway on the remote side. Currently, three gateways are supported:

- PathStar (from Lucent)
- Jetstream
- CopperCom

Using PathStar

If PathStar is supported at the remote end, you cannot use Frame Relay. You must use ATM.

If you are connecting to a Stinger DSLAM and a PathStar at the remote end, make sure the IAD unit is synchronized with the Stinger DSLAM, that you are using RFC 1483 encapsulation and that you have specified the Constant Bit Rate (CBR) service category. You must also specify PathStar as the voice gateway and configure some parameters in the Manage MGCP/NCS Embedded Client menu.

Synchronizing the IAD with the Stinger DSLAM

From the Main menu, choose Configure WAN, Configure Physical Interface. Make sure the settings in this menu match the settings for the Stinger.

Choosing RFC 1483 encapsulation and CBR service category

When you are setting up the voice PVC, choose ATM. Specify RFC 1483 in the ATM Encapsulation Configuration menu. Specify Constant Bit Rate (CBR) as the service category. These settings ensure that voice transmission is the highest priority.

Specifying PathStar as your voice gateway

To enable the IAD to identify PathStar as the voice gateway, follow these steps:

1 From the Main menu, choose VoicePath Configure.

2 Choose the Set Voice Gateway menu option.

3 Choose PathStar.

4 From the Main menu, choose Reset System. You must reset the IAD for the changes to take effect.

Configuring parameters in the Manage MGCP/NCS Embedded Client menu

After you specify PathStar and reset the IAD, the Manage MGCP/NCS Embedded Client menu appears as the last item in the Main menu.

To configure the voice PVC for PathStar, follow these steps:

1 Choose Manage MGCP/NCS Embedded Client menu to configure the IP address of the PathStar's call agent (or notified entity).

2 Choose Configure MGCP/NCP parameters.

3 Choose RTP Transport (voice). Enter the IP address you assigned to the voice PVC when you configured it for RFC 1483 and CBR. Enter the same IP address for the MGCP Signalling parameter.

4 From the Main menu, choose Reset System. You must reset the IAD for the changes to take effect.

Using Jetstream or CopperCom

The Jetstream and CopperCom voice gateways support both Frame Relay and ATM. When using Jetstream or CopperCom with Stinger, select ATM. When using Jetstream or CopperCom with the Max20 or the DSLTNT, use Frame Relay.

To enable the IAD to work with the Jetstream or CopperCom voice gateways, you must configure the unit as follows. These configuration settings assume you are using ATM and the Stinger DSLAM.

Choosing Proprietary Voice encapsulation

Choose ATM encapsulation from the ATM Encapsulation Configuration menu. Specify Proprietary Voice as the encapsulation.

Note: You should only configure *one* voice PVC for Proprietary Voice.

Specify Jetstream or CopperCom as your voice gateway

To enable the IAD to identify Jetstream or CopperCom as the voice gateway, follow these steps:

1. From the Main menu, choose VoicePath Configure.
2. Choose the Set Voice Gateway menu option.
3. Choose Jetstream or CopperCom.
4. From the Main menu, choose Reset System. You must reset the IAD for the changes to take effect.

Command-Line Interface Menus

5

The Main Menu provides access to all the other menus. The Main Menu appears when you first access the command-line interface of the IAD unit. Depending on your access level (User, Supervisor, or Administrator), some of the menus described may not be visible.

This chapter describes each of the menus under the Main Menu. Use these menus to specify your configuration.

Note: After making any configuration changes, you must restart the IAD unit. Use the Reset System command from the Main menu to restart the unit.

Reports menu

Use the Reports menu to generate reports about the status of the IAD unit. Table 5-1 describes each of the menu options available.

Table 5-1. Reports menu options

Menu option	Description
Display Current Configuration	Displays the following information: • Software version • ICTRL • I-Cache—Instruction cache, enable or disable • D-Cache—Data cache, enable or disable • SYPCR register SWRI bit —hard reset or not • RIP —Enable or disable • Bridging —Enable or disable • Bridge Database Aging Time—from 1 to 3600 seconds. The default is 300 seconds. • Spanning Tree —Enable or disable • Spanning Tree Bridge Priority—From 1 to 65,535. The default is 32, 768 seconds. • Spanning Tree Hello Time —From 1 to 10 seconds. The default is 2 seconds.

Table 5-1. Reports menu options (continued)

Menu option	Description
Display Current Configuration (continued)	• Spanning Tree Max Age —From 6 to 40 seconds. The default is 20 seconds. • Spanning Tree Forward Delay —From 4 to 30 seconds. The default is 15 seconds. • SNMP—Enable or disable • SNMP System Contact —User-defined, up to 39 alphanumeric characters • SNMP System Name —User-defined, up to 39 alphanumeric characters) • SNMP System Location —User-defined, up to 39 alphanumeric characters • SNMP Community Private • SNMP Trap Host IP Address • DNS Server IP Address • DNS Server Timeout • Application Information • Support File Information • Module Name/Slot Number —IP address, IP subnet mask • Slot number —Datalink Protocol, SDSL mode, and line rate • Port number: – Bridging —Enable or disable – Spanning Tree—Enable or disable – Port Priority —From 0 to 255; the default is 128

Table 5-1. Reports menu options (continued)

Menu option	Description
Display Current Configuration (continued)	– Path Cost (between 1 and 65, 535; the default is 32, 768 – RIP —Enable or disable – Poisoned Reverse —Enable or disable – Nat Translation – DHCP Client – VPI/VCI or DLCI – 100BaseT Ethernet Interface
Display Network Statistics	Includes the following options: • Display ICMP statistics • Display IP statistics • Display TCP statistics • Display UDP statistics • Clear a network statistic
Display Interface Statistics	Displays statistical information about the total packets handled at Layer 3 on a per-port basis. Choose a port number, and then choose a command from the Interface Statistics menu. The commands include the following: • Display Interface Statistics • Display Bridge Statistics • Display DLCI Statistics (or Display ATM PVC statistics) • Clear a Statistic Some of the commands listed might not appear depending on the modules installed. For example, Display Bridge Statistics appears only if bridging is enabled.

Table 5-1. Reports menu options (continued)

Menu option	Description
Display Media Statistics	Displays statistical information about the total packets handled at Layer 2 on a per-port basis. Choose either SDSL or 100BaseT Ethernet or POTS and then choose a command from the list that appears. Depending on the option you selected, the following menu options may be available: • Display ATM (or Frame Relay) Statistics • Clear ATM (or Frame Relay) Statistics • Display ENET Statistics • Clear ENET Statistics • Display POTS Statistics • Clear POTS Statistics
Display Route Table	Displays the following information about statically configured and dynamically learned routes: • Network address —destination address • Netmask —IP subnet mask • Gateway Address—IP address for packets sent to destination • Interface—IP address for outgoing interface • Metric —Numbers of hops required per gateway • Type —Static or dynamic

Table 5-1. Reports menu options (continued)

Menu option	Description
Display Arp Table	Displays the following information about mappings between Ethernet addresses and devices connected to the LAN: • IP Address —Corresponds to MAC address • Ethernet Address —Assigned by the manufacturer • Interface —Number of the physical port
Display Bridge Forwarding Database	Displays the following information about mappings between Ethernet addresses and devices connected to the LAN: • Ethernet Address —Assigned by the manufacturer • Interface —Number of the physical port • Port Timer —Number of seconds pending before an entry deletes from the database **Note:** You must enable bridging for this option to appear.
Display Bridge Status	Displays the following information about bridging: • Interface —SDSL or 100BaseT Ethernet • Port —Port for the bridging interface • STP —Enabled or disabled • State —Disabled, blocking, listening, learning, or forwarding • Root —Yes or no • Designated • Timers —Current value of the state timer and the hello timer • Root priority • ID

Table 5-1. Reports menu options (continued)

Menu option	Description
Display PPP Authorization Entries	If PPP was authorized, displays the following information about PPP authorization entries: • Authorization Type —None, PAP client, PAP server, CHAP client, or CHAP server • Port # —Active port for the PPP interface

Configure IP Router menu

Use the Configure IP Router menu to assign an IP address for each port you configured with the Configure WAN menu. You can also assign an IP address for the SDSL port, enable and configure RIP by port, configure the DNS server, enable the IAD to act as a DHCP client, and display the route table. Table 5-2 describes each of the options available.

Table 5-2. Configure IP Router menu

Menu option	Description
Configure Port IP Address	Sets the IP address and subnet mask for the SDSL port or the selected 100BaseT Ethernet interface.
Unconfigure Port IP Address	Deletes the IP address for the selected interface.

Table 5-2. Configure IP Router menu (continued)

Menu option	Description
Add/Remove a Static Route	Displays the Router Modification menu which includes the following options: • Add a Static Route —Creates a static route and adds it to the Route table • Remove a Route • Add/Change the Default Route • Remove the Default Route • Display Route Table—Displays the following information about statically configured and dynamically learned routes: – Network address – Netmask – Gateway address – Interface – Metric – Type **Note:** A static route takes precedence over routes chosen by all dynamic routing protocols.
Enable/Disable RIP	Enables or disables the Routing Information Protocol (RIP). RIP sends routing information from one router to adjacent routers, dynamically "learning" network topology. **Note:** You must enable RIP before you can configure RIP by port.

Table 5-2. Configure IP Router menu (continued)

Menu option	Description
Configure RIP Version by Port	Sets the RIP version for the specified port. You can select from the following versions: • Disabled • Version 1 Broadcast (Transmit) • Version 2 Broadcast (Receive) • Version 3 Multicast (bi-directional)
Configure RIP Poisoned Reverse by Port	Enables or disables RIP Poisoned Reverse for the specified interface (port).
Configure DNS Client	Displays the DNS Client Menu: • Configure DNS Server IP Address • Configure DNS Server Timeout —A value between 5 and 20 seconds. The default value is 5 seconds. • Configure DNS Cache and Statistics—Displays information about the data in the DNS cache.
Configure DHCP Client	Use this menu to enable an IAD port to act as a DHCP client.
Display Route Table	Displays the following information about statically configured routes and dynamically learned routes: • Network address • Subnet mask • Gateway address • Interface • Metric • Type

Configure Bridge menu

Use this menu to enable bridging in the IAD. You can then bridge by port, and configure spanning tree options. Table 5-3 describes each of the options available.

Table 5-3. Configure Bridge menu

Menu option	Description
Enable/Disable Bridging Globally	Enables or disables bridging for all ports. **Note:** You must turn on this option before you can bridge by port.
Enable/Disable Bridging by Port	Choose the port for which you want to enable bridging.
Configure Bridge Aging Timer	Sets the bridge database aging time, a value from 1 to 3600 seconds. The default value is 300 seconds.
Enable/Disable Spanning Tree Globally	Enables or disables the Spanning Tree protocol for all configured ports. When multiple paths exist, Spanning Tree lets the IAD choose the most efficient path.
Enable/Disable Spanning Tree by Port	Enables or disables the Spanning Tree protocol for a selected port.
Configure Spanning Tree Bridge Priority	Sets the Spanning Tree bridge priority, a value from 1 to 65, 565. The default value is 32, 768.
Configure Spanning Tree Port Priority	Sets the Spanning Tree priority by port — the lower the value, the higher the priority. The value can be from 0 to 255. The default is 128.
Configure Spanning Tree Hello Time	Sets the Spanning Tree hello time, a value from 1 to 10 seconds. The default value is 2 seconds.
Configure Spanning Tree Max Age	Sets the Spanning Tree max age, a value from 6 to 40 seconds. The default value is 20 seconds.
Configure Spanning Tree Forward Delay	Sets the Spanning Tree forward delay, a value from 4 to 30 seconds. The default value is 15 seconds.

Table 5-3. Configure Bridge menu (continued)

Menu option	Description
Configure Spanning Tree Path Cost	Sets the Spanning Tree path cost, a value from 1 to 65,535. The default value is 32,768. When there are multiple paths to the Root Bridge, the Spanning Tree algorithm selects the port with the lowest total path cost as the route port.
Delete Bridge Forwarding Database Entry	Deletes the Ethernet address from the bridge database.

Configure WAN menu

Use this menu to specify your datalink protocol (ATM or Frame Relay). You then define the PVCs for the protocol you selected. Currently, the IAD supports only one voice PVC.

You can use this menu to manually specify an SDSL line rate.

Table 5-4 describes each of the options available. Your settings display in the Display Current Configuration command in the Reports menu.

Table 5-4. Configure WAN menu

Menu option	Description
Quick Configuration	Allows you to configure the IAD more quickly than choosing the other menu options in the Configure WAN menu. You must have supervisor privileges to see this option. Choose from the following options: • Stinger (Lucent Autobaud and Payload Scrambling) • Auto Cycle (Nokia) • Auto Sense (Copper Mountain) • Unframed ATM (1152 Kbps fixed) • Frame Relay (784 Kbps fixed) After you select an option, the IAD automatically reboots.
Configure Datalink Protocol	Allows you to choose between ATM or Frame Relay.

Table 5-4. Configure WAN menu (continued)

Menu option	Description
Configure Physical Interface	Displays the SDSL Configuration menu: • Set SDSL Mode to CPE • Set SDSL Mode to CO • Set SDSL Speed to Auto Cycle (Nokia) • Set SDSL Speed to Auto Sense (Copper Mountain) • Enable Conexant AutoBaud Mode • Set SDSL Sync Delay (Lucent) • Set SDSL Speed Manually • Restart SDSL Activation Sequence • SDSL Interface Mode (Bit Order) • Enable/Disable SDSL Autobaud Debug Messages • Enable/Disable SDSL Debug Messages • Enable/Disable Sync Msgs • Preactivation Debug Mode Set SDSL options as needed. **Note:** Depending on the port type, some of these menu options may not appear.

Table 5-4. Configure WAN menu (continued)

Menu option	Description
Configure PVCs (if ATM)	Displays the ATM PVC Configure menu: • Add New PVC – Type the VPI and VCI values. – If you are defining a voice PVC and either Jetstream or CopperCom is the voice gateway, choose Proprietary Voice as your encapsulation. If you are defining a voice PVC and Lucent's PathStar is the voice gateway, choose RFC 1483 as the encapsulation and then choose CBR as the service category. – If you are defining a data PVC, choose RFC 1483 encapsulation and UBR as the service category. You can also choose RFC 2364 if you are using PPP over ATM. – Specify the ATM Peak Cell Rate in bps. • Modify Existing PVC • Delete PVC • Show Current PVCs (displays information about the currently configured PVCs)
Configure DLCIs (if Frame Relay)	Displays the FR DLCI Configure Menu: • Add New DLCI – Type the DLCI. – Choose RFC 1490 as the encapsulation. – Configure the congestion parameters. • Modify Existing DLCI • Delete DLCI • Show Current DLCIs **Note:** You cannot define voice PVCs with Frame Relay encapsulation.

Table 5-4. Configure WAN menu (continued)

Menu option	Description
Configure Maintenance Protocol (if Frame Relay)	Allows you to choose a Frame Relay Maintenance Protocol.
Configure Payload Scrambling (if ATM)	Enables or disables payload scrambling.

Configure LAN menu

The Configure LAN menu contains only one command, Set/Clear Full Duplex, which enables or disables full duplex Ethernet mode. Full duplex allows simultaneous transmission and receipt of Ethernet packets. The command applies on a port-by-port basis.

Configure SNMP menu

Use the Configure SNMP menu to set up your SNMP options. Table 5-5 describes each of the options available.

Table 5-5. Configure SNMP menu

Menu option	Description
Enable/Disable SNMP	Enables or disables SNMP.
Configure System Contact	The maximum length cannot exceed 39 alphanumeric characters.
Configure System Name	The maximum length cannot exceed 39 alphanumeric characters.
Configure System Location	The maximum length cannot exceed 39 alphanumeric characters.
Configure SNMP Community	The maximum length cannot exceed 39 alphanumeric characters. Must match the name of the SNMP host.

Table 5-5. Configure SNMP menu (continued)

Menu option	Description
Configure SNMP Trap Host IP Address	Allows you to configure a new host address.

Configure Login menu

Use the Configure Login menu to set up your login and password options. Table 5-6 describes each of the options available.

Table 5-6. Configure Login menu

Menu option	Description
Change User ID	The maximum length cannot exceed 17 alphanumeric characters.
Change User Password	The maximum length cannot exceed 17 alphanumeric characters.
Change Netman Password	The maximum length cannot exceed 17 alphanumeric characters.
Change Supervisor Password	The maximum length cannot exceed 17 alphanumeric characters.

System Utilities menu

Use the System Utilities menu to set up system utilities. Table 5-7 describes each of the options available.

Table 5-7. System Utilities menu

Menu option	Description
File Transfer Utilities	Use this menu to upgrade to the most recent software version.
Ping Utility	Uses the Ping protocol to check for the presence of a host on the Internet.

Table 5-7. System Utilities menu (continued)

Menu option	Description
Update ACOS (ACOS.BIN)	Displays the File Transfer Method menu which allows you to upgrade the IAD software.
Load Boot ROM	Allows you to upgrade your BOOT ROM.
Make a UIS Module a UART port	Factory use only.
File System	Choose from one of the following options: • Directory of all files • Copy file • Rename File • Remove File by Name • Format File System Drive (deletes all files in the system, including the configuration file). Do not use this menu option unless you are prompted to do so by Lucent's Technical Support team. • Space left in File System
Configure CPU	Factory use only.
Enable Application Debug Support	Factory use only.
Set System Defaults	Switches to the factory default configuration.
Config PPP Debug Mode	Enables or disables the display of PPP debug messages.
Config STP Debug Mode	Enables or disables the use of the Spanning Tree Protocol (STP) debug messages.
Config DHCP Client Debug Mode	Enables or disables the display of DHCP debug messages.

Table 5-7. System Utilities menu (continued)

Menu option	Description
Set Ethernet MAC	Allows you to change the factory default Ethernet MAC address of your IAD.
Hard Reset or Reload ACOS from Flash	Restarts the IAD. You must use a hard reset after you upgrade to a newer version of the ACOS.BIN or the BOOT.BIN file.
Print Error Dump	Displays all error messages encountered during the active session.

Configure DHCP Server menu

Use the Configure DHCP menu to configure the IAD to act as a Dynamic Host Configuration Protocol (DHCP) server. Table 5-8 describes each of the options available.

Table 5-8. Configure DHCP menu

Menu option	Description
Enable/Disable DHCP	Enables or disables DHCP.
Enable/Disable DHCP Debug Messages	Factory use only.
Configure DHCP Server Parameters	Allows you to set the DHCP Server parameters. This includes the Gateway IP address, the DNS address, the subnet mask, the domain name and the DHCP lease time.
Configure DHCP Address Range Pool	Allows you to set the DHCP IP address range. Type the high IP address and the low IP address. Both IP addresses must be on the same subnet.
Configure DHCP Client Entry	Forces the IAD to always assign the same IP address to a specific client. Choose the Client Entry Number, the DHCP Client MAC Address, the Host Name, Lease Time, IP Address, Subnet Mask, Default Gateway and DNS Server.

Table 5-8. Configure DHCP menu (continued)

Menu option	Description
Display DHCP Configuration	Displays the following information about the DHCP configuration: • Network interface – Default gateway (IP address for packets sent to DHCP clients) – Default DNS server – Default subnet – Domain name (defines the entity that owns the IP address) – Default lease (duration to keep internet connection active) – High address – Low address
Display DHCP Server Statistics	Displays DHCP server statistics.
Display DHCP Server Assigned Addresses	Displays information about the DHCP clients with dedicated IP addresses: • IP address for the device, assigned by the IAD • Client ID—Ethernet MAC address for the device • Status —whether the device is configured through DHCP or manually

Table 5-8. Configure DHCP menu (continued)

Menu option	Description
Display DHCP Entry Details	Displays the following information about each of the DHCP entries: • IP address • Client ID • Status • Subnet • Gateway • DNS • Lease • Type • Name
Delete a DHCP Client Entry	Deletes a client entry.
Delete a DHCP Assignment Entry	Deletes an assigned IP address.

Configure NAT menu

Use the Configure NAT menu to set up a Network Address Translation (NAT) protocol. NAT allows you to use one IP address for every workstation in a LAN. The IP address hides your internal intranet addresses.

Table 5-9 describes each of the options available.

Table 5-9. Configure NAT menu

Menu option	Description
Enable/Disable NAT Debug Messages	Enables or disables NAT debugging messages.

Table 5-9. Configure NAT menu (continued)

Menu option	Description
Enable/Disable NAT Translation by Port	Enables or disables NAT by port. You can, for example, enable NAT for all ports that connect to the Internet.
Configure NAT TCP Timeout	Sets the NAT TCP connection timeout, a value from 60 to 3600 seconds. The default value is 300 seconds.
Configure NAT UDP Timeout	Sets the NAT UDP connection timeout, a value from 60 to 3600 seconds. The default value is 300 seconds.
Configure NAT Port Range	Sets the range of port numbers to assign to IP connections, with a low range from 1to 65, 534 and a high range from 50,000 to 65,535. The default low value is 50,000 and the default high value is 65,535.
Configure NAT Local Server Entry	Choose a value for each of the following: • Local Server Entry Number • NAT Local Server Translated IP Address • NAT Local Server Translated Port Number • NAT Local Server Standard Port Number • NAT Local Server Protocol

Table 5-9. Configure NAT menu (continued)

Menu option	Description
Display NAT Statistics	Displays the following information about the NAT configuration: • Local IP • Timeouts —TCP and UDP timeout values • Local to INET —Number of bytes and packets transferring to the Internet • INET to local —Number of packets and bytes being received from the Internet • Maxmss (N/A) • MAX TCP window (N/A) • Connections —Number of active TCP, UDP, and ICMP connections, as well as the number created and deleted • Errors —Number of cksum, retries, and bad packets • Total IP packets • Reserved addresses
Display NAT Connection Table	Displays the following information about the NAT connections: • TCP —Ethernet MAC address of the device • Out_port • Ppkts —in and out • State • Idle
Display NAT Connection Details	Displays details about each NAT connection. Information includes seconds in use, state, retries, and the number of ports.

Table 5-9. Configure NAT menu (continued)

Menu option	Description
Display NAT Local Server Table	Displays the following information about the local server: • Entry —table entry number • Local IP address • Local port • Internet port • Protocol —TCP or UDP
Delete IP Address from NAT Tables	Deletes an IP address. The IP address is no longer listed when the following menu options are invoked: Display NAT Statistics, Display NAT Connection Table, and Display NAT Connection Details.
Delete NAT Local Server Entry	Deletes a NAT local server entry. The NAT local server entry is no longer listed when the following menu options are invoked: Display NAT Statistics, Display NAT Connection Table, and Display NAT Connection Details.

Reset System

Use the Reset System option to restart the IAD.

Set Ethernet MAC

Use this option to change the factory MAC address of the IAD.

Display Fast-ENET-Controller

Displays the status of the Ethernet controller card.

VoicePath Configure menu

Use the VoicePath Configure menu to set up voice options.

Table 5-10 describes each of the options available.

Table 5-10.VoicePath Configure menu

Menu option	Description
Set Voice Gateway	Choose PathStar, Jetstream, or CopperCom as the voice gateway. Choose Reset System for the configuration to take effect.
Set Jitter Delay	Sets the jitter delay, a value from 0 to 50 ms. The default value is 0 ms. "Jitter" is introduced if your network provides different waiting times for different cells. It is particularly disruptive to voice communications because it can cause audible clicks.
Display Jitter Delay	Displays the jitter delay value.
Set Start Mode	Select from the following options: • Set all Ports to Loop Start • Set all Ports to Ground Start • Display Start Mode • Configure Individual Port
Set SLIC Control Mode	Specifies the control mode for the Subscriber's Line Interface Circuit (SLIC). Select from the following options: • Auto control mode • Manual control mode

Table 5-10.VoicePath Configure menu

Menu option	Description
Set Compander Mode	Companding is the process of compressing a signal for economical transmission and then expanding it back to its original form at the receiving end. Select from the following options: • u-Law Mode • a-Law Mode
Set On Hook Transmission Mode of Ground Start Lines	Enables or disables on-hook transmission mode of ground start lines. **Note:** With an on-hook line, you can only receive incoming calls.
Set Debug Mode	Enables or disables debugging.
Configure Echo Cancellation Default Settings	Echo cancellation enables the filtering of unwanted signals caused by echoes. Select from the following options: • Set Echo Cancellation default setting for all ports (enable or disable) • Display current Echo Cancellation default settings • Configure Echo Cancellation default setting by port (enable or disable).
Set Loop Gain	Set the transmit and receive loop gain settings for each IAD port.

Call Control Debug menu

This menu is intended primarily for diagnostic purposes. This menu is only enabled if you are using the Jetstream voice gateway. See Table 5-11 for a description of each of the menu options.

Table 5-11.Call Control Debug menu

Menu option	Description
Enable Ring Test	Enter the port number, the number of seconds for the port to stay onhook and the number of seconds for the port to stay offhook.
Display IAD State	Describes the state of the IAD.
Trace	Sets tracing and displays the results of the trace.

Hardware Specifications

A

Following are the specifications for the IAD 4S unit:

Physical connectors	RJ-11 for xDSL WAN Four RJ-11 connectors for POTS lines RJ-45 Ethernet connector
Power input	18Vdc @ 1A
Dimensions	5.6 in. wide x 10.7 in. long (14.2 cm x 27 cm)
Weight	Approximately 2 lbs.
Humidity	0–90%, noncondensing
Operating temperature	32–122° F (0–50° C)

Following are the specifications for the IAD 8S unit:

Physical connectors	RJ-11 for xDSL WAN Eight RJ-11 connectors for POTS lines RJ-45 Ethernet connector
Power input	18Vdc @ 1A
Dimensions	5.6 in. wide x 10.7 in. long (14.2 cm x 27 cm)

Weight	Approximately 2 lbs.
Humidity	0–90%, noncondensing
Operating temperature	32–122° F (0–50° C)

FCC Regulations

B

FCC Part 15 Notice

Warning: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a residential environment. This equipment generates, uses, and can radiate radio frequency energy, and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is unlikely to cause harmful interference. But if it does, the user will be required to correct the interference at his or her own expense.

The authority to operate this equipment is conditioned by the requirement that no modifications will be made to the equipment unless the changes or modifications are expressly approved by Lucent Technologies.

IC CS-03 Notice

The Industry Canada label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective, operational, and safety requirements as prescribed in the appropriate Terminal Equipment

Technical Requirements document(s). The Department does not guarantee that the equipment will operate to the user's satisfaction.

Before installing this equipment, users should make sure that it is permissible to be connected to the facilities of the local telecommunications company. An acceptable method of connection must be used to install the equipment. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be coordinated by a representative designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines, and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

Warning: Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.