DataFire PRIme for Solaris SPARC / x86

Configuration and Usage Guide

Information in this document is subject to change without notice and does not represent a commitment on the part of Digi International.

Digi provides this document “as is”, without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of fitness or merchantability for a particular purpose. Digi may make improvements and/or changes in this manual or in the product(s) and/or the program(s) described in hsi manual at any time.

This product could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes may be incorporated in new editions of the publication.

Table of Contents

Introduction

In this chapter This chapter introduces Digi's Solaris driver for the DataFire PRIme adapter.

It discusses the following topics:

- Product Description
- Features
- System Requirements
- Resource Documents
- Document Conventions

Product Description

The Digi *DIGIdfp* driver allows you to use a DataFire® PRIme™ adapter with communication applications available with Solaris.

Features

Digi's driver incorporates the following features in its design:

- One PRI line per adapter. Depending on the adapter model the number of channels is either 23B + D or 30B + D
- Multiple "B" channels can be linked to increase transfer rates
- Support for up to three Digi DataFire PRIme adapters in one server
- Support for the following switches: AT&T 5ESS (now Lucent), Northern Telecom DMS-100 (now Nortel), any National ISDN-2 compatible switch, ETSI (European Telecommunications Standards Institue)

System Requirements

Successful configuration of the Digi driver requires the following:

- X Windows System™ software
- Solaris version 2.5.1 or greater, including support for PCI bus

Resource Documents

The instructions in this guide assume that related documentation is available for background information about Solaris. This guide is intended to describe the configuration process for Digi products and assumes that you are familiar with Solaris manuals.

It would be a good idea to have the following references available during installation:

- Solaris manuals
- For questions about hardware, *DataFire PRIme Installation Card*

Document Conventions

This section describes the customary styles and terms used in this document.

Inputs

A bold monotype font is used to indicate commands typed from the command prompt:

```
mlpconn
```

Special Characters

Angle brackets are used to indicate that a key on your keyboard should be typed. For example:

<Ins>	Indicates the *Insert* key should be pressed
<Enter>	Indicates the *Enter* key should be pressed

Terminology

The following terms are used throughout this manual:

adapter	The physical circuit board installed in your system.
line	Describes one ISDN interface including all D and B channels.

chapter **1**

Configuring the Driver

In this chapter

This chapter describes the steps required to configure the Solaris driver for DataFire PRIme for use on a Solaris system.
It discusses the following topics:

Before You Begin

Before you begin configuring the DataFire PRIme adapter(s), you need to be sure that you have all the information required to successfully make them work in your Solaris system.

You will need to:

Contact Your Service Provider

Some of the information required for configuration of the adapter(s) must be obtained from your ISDN service provider. You *must* have this information before configuring your Digi adapter(s).

- Use the worksheets in appendix A as a guide to the information required from your Service Provider.

Determine Your Connections

With the *DIGIdfp* driver you will be able to accept and route client calls from a variety of external sources as well as connect to other servers. It is important to plan these connections and obtain the IP addresses necessary to create the links used by the driver.

- Use the worksheets in appendix A to help you gather the information you will need about to create links between local and remote sites.
- Read the *Usage Option* information beginning on page 3-1 for more information about setting up the sessions you will need.

About the Driver

The Solaris driver for the DataFire PRIme adapter is comprised of several components. This section describes where the files are placed and how the daemons work.

Location of Files

- Driver files are located in */usr/kernel/drv*
- GUI files are located in */usr/lib/snet* and */usr/lib/snet/wancfglib*
- MLPPP network configuration files are located in */usr/lib/snet/mpd*
- ISDN network configuration files are located in */usr/lib/snet/template*
- FEP and BIOS files are located in */usr/lib/snet*
- Default template files are located in */usr/lib/snet/template*

Man page files are also copied to your system:

- Man pages are located in */usr/lib/snet/man*

There are also three monitoring utilities that you can use to gather information about the state of the PRI line or an individual link: *mlpstat*, *isdntrace* and *isdnstat*:

- Look in */etc* for *isdntrace* and *mlpstat*
- Look in */usr/bin* for *isdnstat*

For more information about using these utilities, see the *Trace and Statistics* section beginning on page 4-1.

About the daemons

There are two daemons that provide the functional backbone of your ISDN connections: *mpd*, and *netd*.

The *mpd* daemon is the multilink protocol daemon. It looks for incoming calls and establishes the links you have configured. It handles the protocol between the ISDN layer and the adapter. When you make a change to the PPP or Link parameters, you must restart the daemon for the changes to take effect. (Use the Restart MLPPP Daemon option in the Network pulldown menu of *wancfg*.)

The *netd* daemon maintains the ISDN protocol stack for all of the adapters.

Both daemons must be running for your driver to properly function.

Use the man pages

To find out more about how the driver components work together, you can view the man pages that installed with your package.

About the *wancfg* Configuration Utility

During the configuration process you must provide information about your ISDN service and properties of the ISDN line.

Also, the driver configuration requires access to the X Windows System.

Tips for using the Configuration Utility

As you navigate the Configuration Utility windows, keep the following tips in mind:

- The left-hand pane is called the Contents Pane; items listed in this pane have associated windows. Click on an item in the Contents Pane to access a window (displayed in the Properties Pane, described next).
- The right-hand pane is called the Properties Pane. When you click on an item in the Contents Pane, the associated window will be displayed in the Properties Pane, allowing you to view the configuration or make changes to it.
- There can be multiple windows available in the Properties Pane for a given item listed in the Contents Pane. The multiple windows are displayed with "Tabs" at the top of the pane.
- When configuring ISDN-PRI and PPP properties, advanced options are available by using <Ctrl> + A.
- Help files are available by clicking the Help button or pressing F1 in a specific window.

Navigating the Utility

You can use your mouse to click on items, or you can use "Hot keys" as explained below:

- You can access items in a window by holding down the <Alt> key and pressing the underlined letter in an item. Example: To pull down the File menu, press <Alt> and F simultaneously.
- Use the <Tab> key to move between fields.
- Use the space bar to toggle a check box on or off.

Special Control Key Functions

Press the <Ctrl> key along with the keys listed to get short-cut access to the functions:

<Ctrl> + U	Undo, or reset values to default
<Ctrl> + R	Remove a Digi adapter from the configuration
<Ctrl> + N	Add a Digi adapter to the configuration
<Ctrl> + K	Keep adapter configuration information when switching out an adapter
<Ctrl> + A	Advanced options for ISDN-PRI and PPP; click on Help for more information

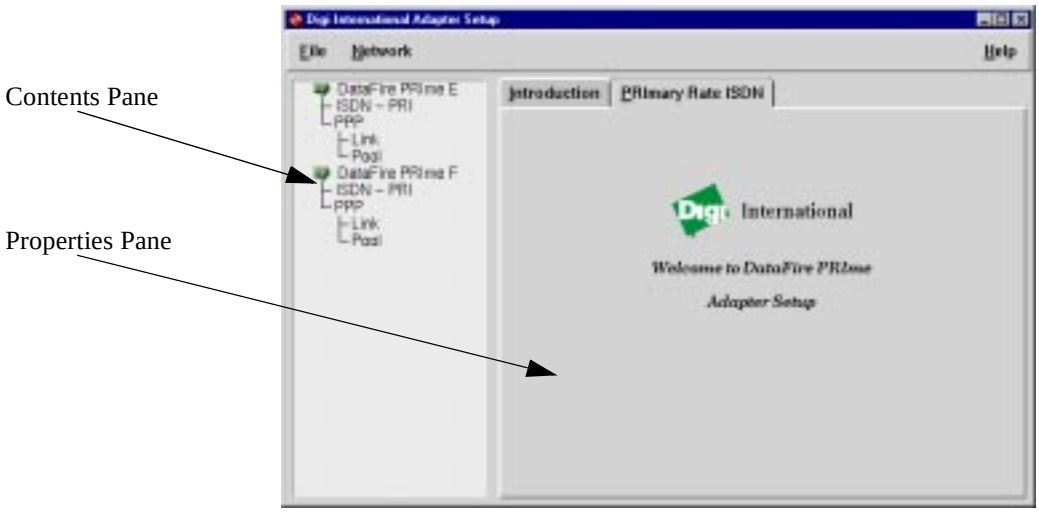

Figure 1-1. The Contents and Properties Panes

Starting the wancfg Utility

To start the configuraition utilty from the server in which the DataFire PRIme adapter is installed, type the following at the command prompt:

```
wancfg
```

If you are starting *wancfg* from a workstation on the LAN, you might need to use one of the following commands first, in order to force the utility to display the *wancfg* screen at your workstation:

For *ksh*: export DISPLAY=<IP address or name>:0.0

Example:

```
#export DISPLAY=rodger:0.0
```

For *csh*: DISPLAY=<IP address or name>:0.0
export

Example:

```
#DISPLAY=rodger:0.0
#export
```

Configuration Instructions

Starting Point

- You have installed the DataFire PRIme driver (see the *DataFire PRIme™ for Solaris Sparc / x86 Software Installation Instructions* card for information about installing the driver).
- You have contacted your service provider and obtained information for the ISDN configuration.
- You have IP addresses to use when creating Links and Pools.
- X Windows System™ is properly installed and configured on your system.

1. Login as root.

You must be superuser to make changes to the system configuration.

2. Start the Configuration Utility.

Type the following at the command prompt:

```
wancfg
```

You will see the main Configuration Utility window display. The Properties Pane will contain a tab for each installed product.

3. Choose the Primary Rate ISDN Tab.

In the Properties pane, click the tab called Primary Rate ISDN.

Figure 1-2. Primary Rate ISDN selection

Note: You will only see the Frame Relay tab, as shown above, if you have already installed Wan Links software.

The Contents pane will now list each DataFire PRIme adapter installed in your system and provide several configuration items for each adapter: ISDN-PRI, PPP, and under PPP, Pool and Link.

4. Configure ISDN properties.

In the Contents pane, click on the ISDN-PRI item under the adapter you wish to configure. You will see the ISDN-PRI window display in the Properties pane.

- Use this window to select the properties of the ISDN line connected to the adapter. This window has two tabs: Switch and CSU.
- Information for both these tabs is available from your Service Provider.

Switch tab:

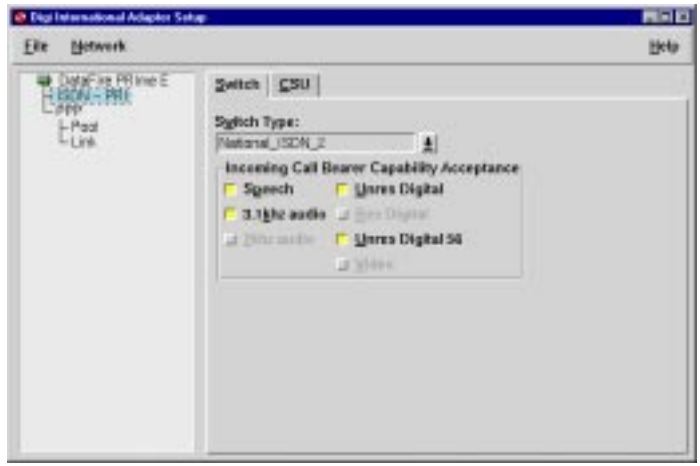

Figure 1-3. Switch Window

- You must choose the type of ISDN switch used at your Central Office.
- By default, all types of calls available through your switch will be answered by the DataFire PRIme. (Options not available through your switch will be grayed. See Figure 1-3.) If you wish to filter the types of available calls that will be accepted by the adapter, deselect the bearer capability options you DO NOT want to accept. For example, if you have no application that can use Speech data, you might want to de-select the Speech bearer capability. For most flexibility, you should leave all options that are available through the switch selected.

CSU tab: Click on the CSU tab to examine or change attributes of the line for your setup.

Figure 1-4. CSU window

Note: If this tab is grayed, it is not needed for your model of adapter.

- You must choose whether your line connection is Long Haul or Short Haul.

  Choose *Short Haul* if there is a PBX or similar device that terminates the ISDN service into the building. You must then select the number of feet between that device and the server with the DataFire PRIme, using the drop-down box. It is important to be accurate.

  Choose *Long Haul* if the DataFire PRIme terminates the ISDN service into the building. Your service provider will be able to tell you the decibels of attenuation required by the line. Choose the correct level from the drop-down menu next to the Pulse field. Pulse decibel attenuation is determined by the length of the line between the switch and the entry point into your building. This distance also determines the amount of Equalization that the line requires. Choose High or Low from the drop-down menu.
- When configuring ISDN-PRI properties, advanced options are available by using <Ctrl> + A. Click on Help for additional information.

5. Configure PPP properties. In the Contents pane, click on the PPP item for the adapter you are configuring. You will see the PPP window display in the Properties pane.

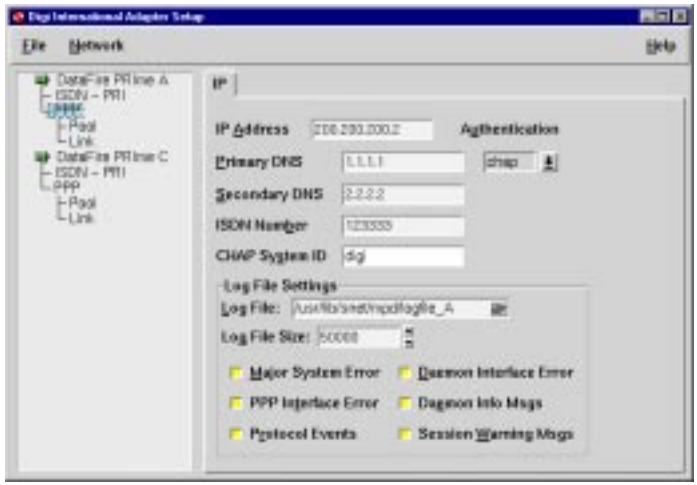

Figure 1-5. PPP Window for IP

IP tab:

a. *IP Address:* You must enter the IP address you want to assign to the DataFire PRIme adapter. This address will be used as an end-point discriminator for all sessions.

b. *Authentication:* You must select the type of authentication to be negotiated for each IP connection: PAP, or CHAP.

Note: The authentication type you choose in this window is used as a global default for all links. You can, however, override it on a link-by-link basis. See the description of Authentication Protocol Override on page 1-12.

c. *Primary/Secondary DNS:* If you are using a Domain Name Server, you must enter at least one DNS IP address.

d. *ISDN Number:* Enter the phone number assigned to the PRI line by the Central Office. Legal characters are * and digits 0 to 9 with no spaces or commas, to a maximum of 20 characters. Use the asterisk to indicate an extension.

e. *Chap System ID:* Used only with CHAP authentication, and allows you to specify an ID value used by the remote side to authenticate a call.

f. *Log File Settings:* To use a log file for errors and messages, select a directory and file name for the log file, select the maximum size of the log file (up to 1000000 bytes), and also select the type of data to be logged by clicking on one or more of the items in the list. Once the maximum log file size is reached, it will wrap to the front and overwrite the beginning of the file.

The Log file name can be a maximum of 16 alphanumeric characters.

6. Set up Pools

A Pool is a list of IP addresses that is given a name. During step 7 you will be setting up links to remote devices; when setting up inbound links, you can use a Pool Name in the Remote IP address field to provide a list of IP addresses to be assigned to remote devices that call.

Note: To use a Pool Name in the Link Entry window, you must first create the Pool.

In the Contents pane, click on the Pool item under the adapter that you are configuring. The Properties pane will display a window to add and configure pools. Click on the Add button.

The following window will display:

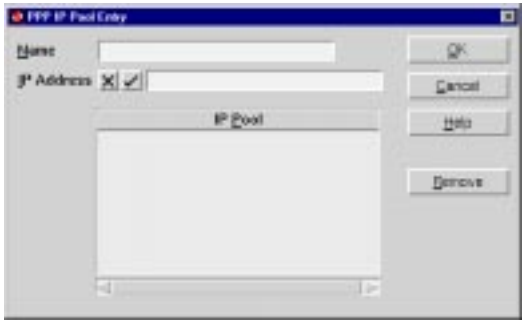

Figure 1-6. Pool Entry Screen

a. Type a name for the pool in the Name field.
b. Type a list of IP addresses, each address separated by a space, in the IP Addresses field. To accept the IP addresses in the field, click on the check symbol. (To discard the addresses, click on the cross symbol.) The addresses will appear in the IP Pool field after you accept them.
c. To remove an IP address that appears in the IP Pool field, highlight it and click the Remove button.

7. Set up Links

In the Contents pane, click on the Link item under the adapter that you are configuring. The Properties pane will display a window to add, configure, and remove Links from a list. Click on the Add button. The Link Entry window will display:

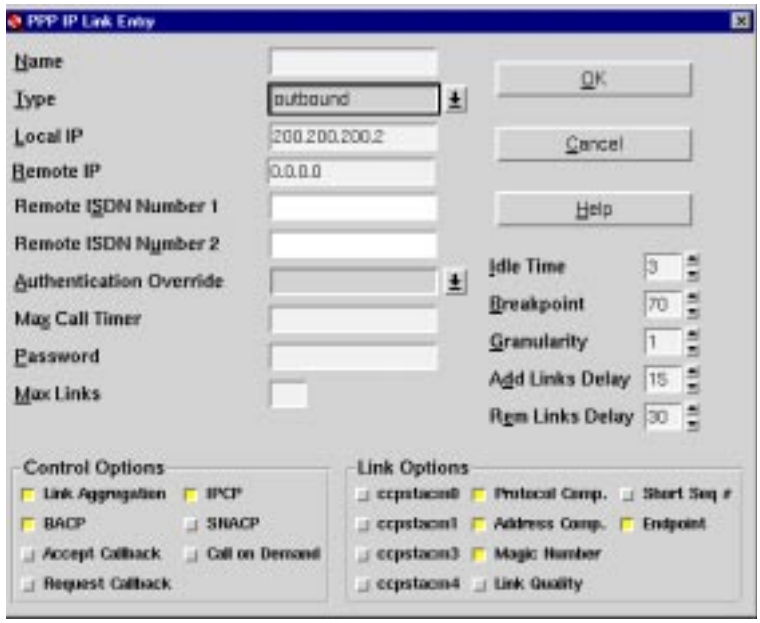

Figure 1-7. IP Link Entry Window

Use this window to set up inbound and outbound PPP links over ISDN:

a. *Name:* You must select a Name for each link. The Name of an inbound link is used by the calling client or server. The Name of an outbound link is used with the *mlpconn* command to connect using the information you provide in this window. See page 2-2 for more information about using *mlpconn*.
The name you choose is limited to 16 alphanumeric characters.

b. *Type:* You must choose an inbound or outbound type of link. Inbound links are handled automatically by the *mpd* daemon. Use *mlpconn* to initiate an outbound link. See page 2-2.

c. *Local IP:* By default, this field will contain the IP address you entered using the PPP properties. You can change the IP address on a per link basis by entering a different number in this field. For an outbound link, if you want the remote side to assign an IP address, enter 0.0.0.0 in this field.

d. *Remote IP*: For inbound calls, you can either enter a single IP address in this field or use a Pool Name that represents a list of IP addresses that can be assigned to the remote device that is calling. For outbound calls, enter the IP address of the remote device.

e. *Idle Time:* This is the number of minutes the adapter will wait on an idle line for additional traffic, before disconnecting the call. On an Outbound call that has Call On Demand enabled, use this value to indicate when the link should disconnect and wait for re-connect.
The maximum number of minutes you can choose is 60.

f. *Remote ISDN Number 1:* On an outbound link, you must provide the ISDN numbers (phone number) to call. Legal characters are * and digits 0 to 9 with no spaces or commas, to a maximum of 20 characters. Use the asterisk to indicate an extension.

g. *Remote ISDN Number 2:* This number is only used when making a two-channel call to an ISDN BRI adapter. Legal characters are * and digits 0 to 9 with no spaces or commas, to a maximum of 20 characters. Use the asterisk to indicate an extension.

h. *Authentication Override:* If you leave this field blank for an inbound link, the global default will be used (as set in the PPP window—see page 1-9.) You can override the global default by selecting one of the other options via this field. For an outbound link, the global default is to request no authentication; if the field is blank, no negotiation will be initiated. Make a selection in this field to override the global default.

i. *Maximum Call Timer:* Use this field to set a timer countdown for the link, in minutes. If the link is still up once the timer value reaches zero, a warning message will be sent to the error log from the *mpd* daemon. The message will be repeated every half hour thereafter, until the link is brought down.
Use a 0 to disable the timer.
The maximum value is 4320 minutes (72 hours).

j. *Password:* Use this field to specify a password for Authentication for PAP or CHAP. You can use a maximum of 16 alphanumeric characters for your password.

k. *Max Links:* Use this value to specify the number of B channels to use for this link (from a maximum of 23 or 30 depending on your model of adapter). The default number is the maximum number of channels available with your model of adapter and your service.

l. *Control Options:* These options specify several Multi-link PPP options to use:
Link Aggregation. (Outbound Links only) Automatically adds or subtracts channels for a session based on current channel utilization. Four factors— *Breakpoint*, *Granularity*, *Add Link Delay* and *Remove Link Delay*— work together, and with the *Max Links* value to provide automatic bandwidth control.
BACP (Bandwidth Allocation Control Protocol): Method of controlling bandwidth by placing a single channel call that establishes a connection and negotiates connection terms before

increasing the number of channels that will be used for the call. Both sides of a session must have this protocol enabled for it to function. If used with Request Callback, (Outbound Links only) requests the called side to add the channel. If used with Accept Callback, allows the called side to call back.
Call On Demand. (Outbound Links only) Allows a call to be torn down when not in use, and automatically brought back up when traffic is recognized. Used with the Idle Time value to control the no-traffic wait before tearing down the call.

Note: When using Call On Demand, if the IP address of the remote system is not specified in the Remote IP field, then a route must be added (see *route(1M)*) to indicate that a particular session is the path for the outgoing IP packets.

See the discussion beginning on page 3-1 for more information about these features.

m. *Breakpoint*: Percent of channel utilization above which the number specified by your Granularity setting will be added, or below which that number will be subtracted.

n. *Granularity:* Number of channel added or subtracted at a time to keep bandwidth under the Breakpoint value.

o. *Add Link Delay:* Number of consecutive seconds over Breakpoint required before the adapter will add the number of channels specified by Granularity. Used to ensure that the increase in traffic is not just a spike.
Maximum of 300 seconds, in five-second increments.

p. *Remove Link Delay:* Number of consecutive seconds under Breakpoint required before the adapter will remove the number of channels specified by Granularity. Used to ensure that the dip in traffic indicates a real slowdown, not just a momentary lapse.
Maximum of 300 seconds, in five-second increments.

q. *Link Options:* These options specify PPP properties. Unless you are familiar with these options, they should be left at the defaults.

r. When configuring PPP properties, advanced options are available by using <Ctrl> + A. Click on Help for additional information.

8. Configure Other Adapters

Repeat steps 4 through 7 for each DataFire PRIme adapter in your system.

9. Start the Daemons

Once you are finished setting all the parameters, you are done with the configuration utility and you can start the daemons that will handle your ISDN connections.

a. Click on Network in the menu bar, then click on Start DataFire PRIme on exit to get to a list of adapters. You can choose to start all of the adapters or any number of the adapters in the list.

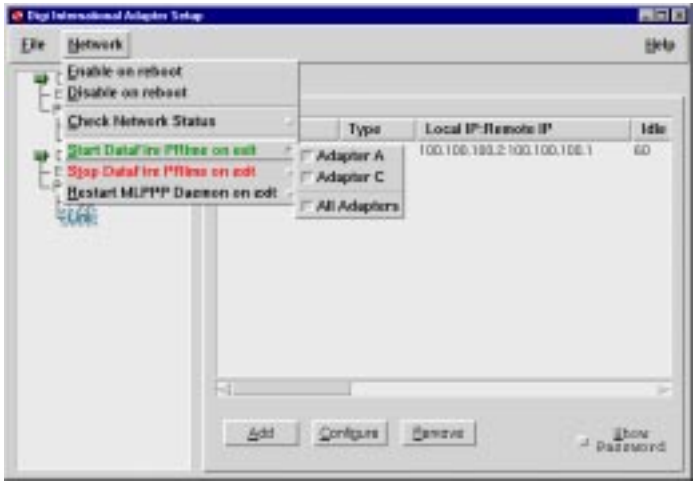

Figure 1-8. Network

b. Now click on File and choose Save Changes and Exit.

You will see messages that indicate the **`wancfg`** program is creating the configuration files for your setup.

10. Check the Network

To find out if the daemons for each of the adapters you selected has started:

a. Type **`wancfg`** at the command prompt

b. Click on Network in the menu bar, then click on Check Network Status, and choose the adapter that you want to check.

A green box next to the adapter means the *netd* daemon is running. A red box means that the network is down.

wancfg Notes

- To add/remove an adapter, click on File on the menu bar and choose Add New Adapter or Remove adapter. The changes will be visible in the Contents pane.

  Warning: You must never remove all adapters from *wancfg*. Doing so will have unforeseen consequences.
- For compatibility with the SyncPort products that have two ports, ISDN subnets always take up two subnet addresses, even though there is a single ISDN port on the adapter. If you have two DataFire PRIme adapters in your server (and no SyncPort cards), the subnet letters will be A and C.

What Next

Once the *mpd* daemon is running, incoming calls will be answered and links established. To initiate an outbound call, see the instructions on page 2-2.

chapter **2**

Making Connections

In this chapter After you install the driver components and configure the ISDN line attached to the DataFire PRIme adapter, you can use the commands described in this chapter to make an outbound connection.

The following topics are covered in this chapter:

Connection Commands

There are four commands that you can use to manage your outbound connections: *mlpconn*, *mlpadd*, and *mlpsub* and *mlpdisc*.

To make an outbound connection:

Use this command to initiate an outbound call.

At the command prompt type the following:

mlpconn -s <*subnet*> <*connection_name*>

Example:

```
mlpconn -s A boston
```

Uses adapter A to make the link you created with *wancfg* called "boston".

To add channels to an outbound connection:

Use this command to expand the number of B channels used during a connection by one.

At the command prompt type the following:

mlpadd -s <*subnet*> *connection_name*

Example:

```
mlpadd -s A boston
```

Adds one B channel to the link that is already up.

To remove channels from an outbound connection:

Use this command to subtract one B channel from an outbound connection that is currently up.

At the command prompt, type the following:

mplsub -s <*subnet*> *connection_name*

Example:

```
mlpsub -s A boston
```

Subtracts one B channel from the link called "boston".

To disconnect an outbound call:

Use this command to terminate an outbound link:

mlpdisc -s <*subnet*> *connection_name*

Example:

```
mlpdisc -s A boston
```

Disconnects the link called "boston".

chapter **3**

Usage Options

In this chapter Using the DataFire PRIme adapter and driver plus the Solaris system software, you can set up a variety of WAN connectivity solutions that are easy to maintain and use. To do this, you will need to understand how the software and hardware work, evaluate the setup options and implement the configuration that most closely fits the requirements of the site. This chapter discusses the following topics:

Overview

The DataFire PRIme has several features that you may wish to employ, depending on the needs of the environment in which it will be used. This section provides an overview of these features, and an introduction to the setup examples explained in the following pages.

Discussion of Features

BACP and "Callback"

Bandwidth Allocation Control Protocol. This standard (RFC2125) describes requirements for negotiating the number of channels used during a session. When BACP is used, a notification is made before a channel is brought up or removed from a session.

There is also a "callback" facility included that allows channels to be added by either end of the connection, without regard to which party initiated the session. This can be useful when either cost or security is a concern and you want to ensure that the majority of calls for a session are initiated in one direction.

Link Aggregation: Cost and Throughput Considerations

Because it can perform multi-link PPP, there are two ways to use the multiple B channels available on a PRI line connected to a DataFire PRIme adapter:

- single channel sessions
- aggregated channel sessions.

A client call using a single BRI B channel is an example of a single channel session. With 23 (or 30) B channels available with PRI, multiple single-channel sessions can occur simultaneously. The throughput available for each channel is affected in small amount by the additional sessions, but is chiefly limited by the CPU capabilities of the Server in which the DataFire PRIme is installed. Toll costs for the single line are a known value, and determined by the tariffing rates applied to the caller. Often the first minute is the most expensive, and the rates drop for subsequent minutes of connect time.

Choosing aggregated channel sessions (the Link Aggregation option) adds complexity to the operation. The Link Aggregation feature automatically adds channels to a session or subtracts channels from a session based on the utilization of the channels already in place for the session.

Several factors work together to provide this automatic bandwidth control; you must carefully assign the values for these that will provide the most cost-effective strategy. For example, when the toll cost for a first minute is higher than subsequent minutes, you must be careful that your setup does not continually bring up and tear down channels in your session because then you will be continually incurring the higher "first minute" charge.

Another factor to consider is that the throughput capability added to

your data transfer by adding channels is not linear. That is, if you have one channel open and then add a second, you are not doubling your thoughput. Because of the overhead required to send packets over multiple channels, you are increasing your throughput by a value less than 100%. As you add channels, you add throughput, but you also add cost and overhead. At a certain point the added overhead of an additional channel cancels its advantage to the bandwidth and then you are just adding cost to the operation by adding channels.

Cost and the throughput required for an application are important factors to balance when making a decision about the bandwidth to use for a transfer.

Summary of Examples

Data Pipeline You can set up the DataFire PRIme to push data across a WAN connection using an expanding bandwidth to keep the throughput high.

For more information about this type of setup, see page 3-4.

Client to Server Calls For client dial-ups to the server, you can use the DataFire PRIme to provide access for multiple simultaneous sessions.

For more information about this type of setup, see page 3-11.

IP Routing To allow WAN access between LANS, you can use the DataFire PRIme as an IP Router (or gateway).

For more information about this type of setup, see page 3-14.

Example 1: Data Pipeline

With 23 (or 30) B+D channels available, providing a data pipeline between two servers can be an efficient means of quickly moving data.

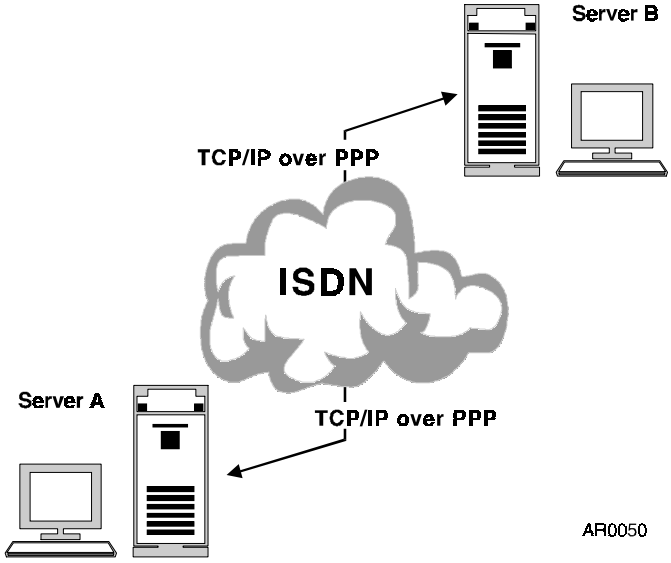

Figure 3-1. Data Pipeline Scenario

You can easily set up this link to automatically use maximum available bandwidth, for maximum performance, using Link Aggregation.

Setup Requirements

The setup requirements that follow describe how to set up the servers if both use a DataFire PRIme, but any PRI device using Multi-link PPP can interact with the DataFire PRIme and could be set up in a similar manner.

In this scenario, Server B calls Server A to obtain data. The following features are used:

- Link Aggregation
- BACP

Server A Setup: Inbound

When you use the Link Entry screen for an Inbound Link, you are providing the parameters that the *mpd* and *netd* daemons will use to answer the call. Each call that will be answered must have an Inbound Link associated with it.

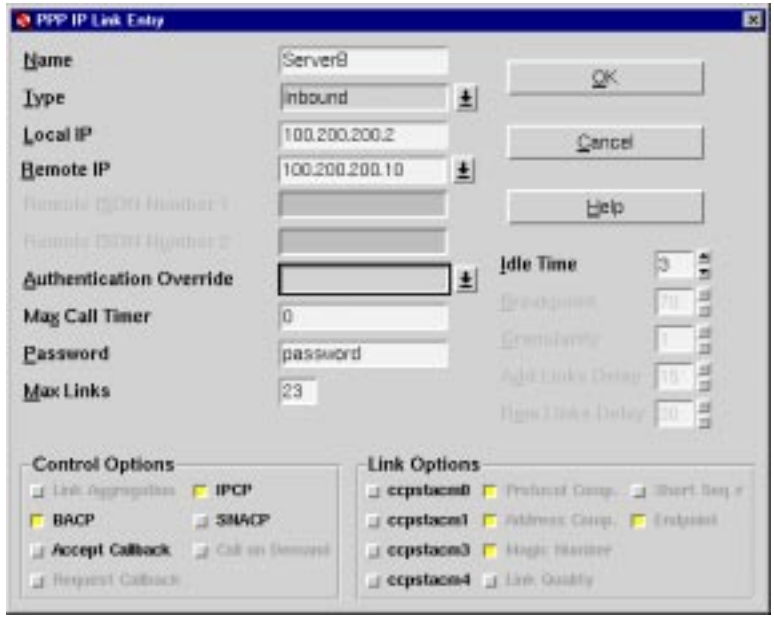

Figure 3-2. Link Entry Screen Setup for the Incoming Call

Name and Password: The contents of the Name and Password fields, are used to authenticate the incoming call. The Outbound link on Server B must use the same name and password.

Local IP: This IP address must be unique to this session.

Remote IP: For this example, the link will be opened with one channel, with the capability to use all available channels in this single session. A pool of IP addresses is not needed, so choosing one IP address makes sense.

Max Links: (Maximum number of channels that can be brought up during the session) Figure 3-2 shows that all 23 channels are available for this call. Since this is supposed to be a pipeline from one server to another, it makes sense to use as many channels as possible. Channels are added by the calling side. If there are already channels in use on either server, the bandwidth of the call is limited to the number of available channels. If this link expands to all channels, other links will be shut out for the duration of the call.

Idle Time: In this example, after three minutes with no activity, the adapter will hang-up the line. Setting a reasonable value in this field ensures that the ISDN call is not up for an unnecessarily extended period of time, in order to keep costs down.

BACP: This must be enabled on both ends of a connection for it to work. In this example, the Outbound call will also have BACP enabled. This will allow the calling side to provide notification when channels are added to or removed from the session.

Note: A discussion of the use of BACP with Callback is provided on page 3-8.

Server B Setup: Outbound

The parameters provided for the Outbound Link are used by the DataFire PRIme when it places the call.

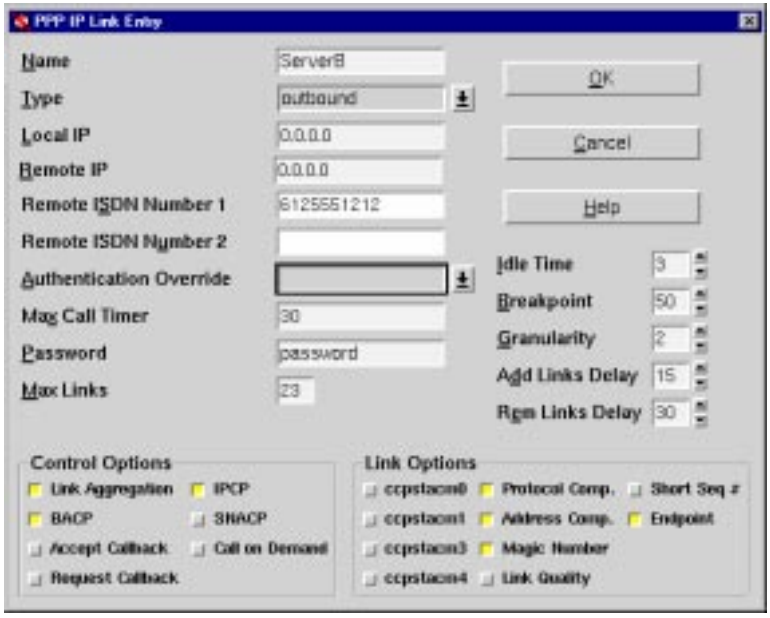

Figure 3-3. Setup for the Outbound Call

Name and Password: For the call to be answered and authenticated, both the name and password must match the name and password expected and set up for the Inbound Link.

Local IP: In this case, we used 0.0.0.0 so that an IP Address for Server B is provided by Server A. The *Remote IP* in the Link setup for Server A (see Figure 3-2) will be assigned to Server B when it calls.

Remote IP: An IP address of 0.0.0.0 allows Server A to provide its IP address to Server B. (The Local IP address used in Figure 3-2 could be used here instead.)

Remote ISDN Numbers: This is the phone number of the PRI line going to Server A. For calls to a PRI line there is only one phone number required.

Max Call Timer: In this example, the data transfer is supposed to take less than 30 minutes. Setting this value ensures that after 30 minutes of consecutive connection time, warning messages will be posted to the error log. Although both sides of the connection can use this feature, it is most useful for the calling side (that pays the cost of the call) to use as a means to keep track of the amount of time a connection is up. The system administrator of Server B can examine the error log file to determine if the connection is taking more time than expected.

Max Links: Since the connection in this example is meant to provide high speed data transfer, a value equivalent to all channels is used.

Idle Time: In this example, after three minutes without packet traffic, the call will be torn down.

Link Aggregation: With this feature enabled, channels will be added to the session in order to keep up a high rate of data transfer. Channels are automatically subtracted when utilization drops. Since this example describes a data "pipeline," throughput is the most important factor for the transfer. For that reason, the Breakpoint is set low to quickly bring up channels, and the Granularity is 2 so that channels are added two at a time until all channels are in use.

Refer to page 3-2 for more information about Link Aggregation.

BACP: With this feature enabled, the called side is notified before a channel is added or subtracted from a session.

Note: A discussion of the use of BACP with Callback is provided on page 3-8.

How it works

After the links are set up on both servers, the daemons (*mpd* and *netd*) that answer calls must be started on Server A. (See page 1-14) When data is to be transferred between servers, the system administrator for Server B initiates a call by executing the following command:

```
mlpconn -s A ServerB
```

(Alternatively, Server B can be configured to use on-demand dialing and static routes.)

The DataFire PRIme in Server B places the call and Server A answers. Names and passwords are verified, and a connection is made. Initially there is one B channel in use for the session. The application that required the link begins to transfer data.

When the utilization of the channel reaches 50% (Breakpoint = 50), Server B waits for 15 consecutive seconds of above 50% utilization (Add Links Delay = 15), and then notifies Server A that additional bandwidth will be added (BACP). Server B then adds two more channels (Granularity = 2). This continues until all available channels are in use (Max Link =23).

As data traffic begins to fall below 50% utilization, Server B waits for 30 consecutive seconds of below 50% utilization (Remove Links Delay = 30 seconds), notifies Server A that channels will be removed from the session, and then removes two channels. If the utilization of the remaining channels declines past 50%, more channels will be removed.

Once the application has stopped transferring data, and for 3 minutes (Idle Time = 3) there is *no* traffic over the channels that remain connected, Server B will tear down the session.

If the total connection time ever exceeds 30 minutes (Maximum Call Timer = 30), warnings will be posted to the error log on Server B.

Application Scenario

The Server to Server Pipeline example has several real-life applications. Generally, any business that must report a large quantity of information in a short time fits this application.

Specifically, the data pipeline could be used by a branch office of a bank that calls the central office every night to dump the day's transactions and update customer accounts. Since it is important that financial transactions occur in a timely fashion, it makes sense to pay for maximum channel usage in order to transfer data quickly.

Another application that could use a data pipeline is a large retail organization with remote outlets. The data transferred over the pipeline could include both daily inventory and receipts.

Adding BACP with Callback to the Example

In the example just presented, BACP, without Callback, is enabled for both sides, which only means that BACP is negotiated during the initial call, and then subsequently the calling side notifies the other system when a channel is to be added or removed.

There are times when you may also want to use the Callback facility offered by BACP. Since it allows you the flexibility to set up both Inbound and Outbound links that will negotiate for callback from the other side, it is a feature that is useful when security and cost considerations are a factor, i.e. if it is cheaper or improves security to ensure that all calls (that add channels to a session) come from just one side.

Using the same example (Server B calls Server A to initiate a session), BACP Callback can be added to the setup to ensure that subsequently, all channels are added by Server A calling Server B, as illustrated in Figure 3-4.

If the toll charge is less when calling from Server A to Server B, this setup will ensure that most of the calling charge is incurred in the least expensive direction, but the timing of each connection is still controlled by Server B.

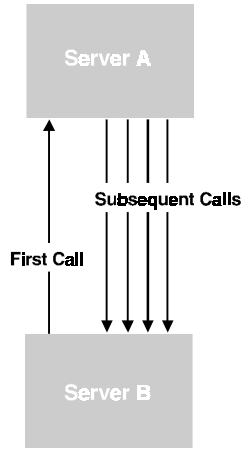

Figure 3-4. Using Callback

How to Enable BACP with Callback

The setup of both the Inbound and Outbound Link Entry screens must be changed to enable BACP with Callback.

Inbound Link BACP

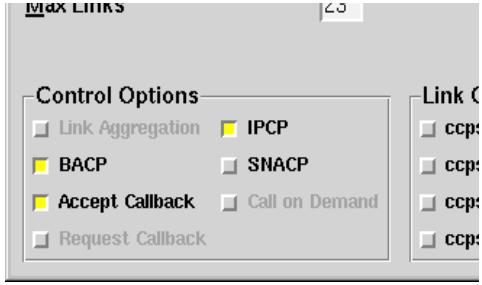

Figure 3-5. Inbound Accept Callback

Under Control Options for the Inbound Link, click on the Accept Callback option to enable it as shown in Figure 3-5.

This allows Server A to accept BACP negotiation from Server B requesting a callback from Server A when a channel is to be added to the session.

Outbound Link BACP

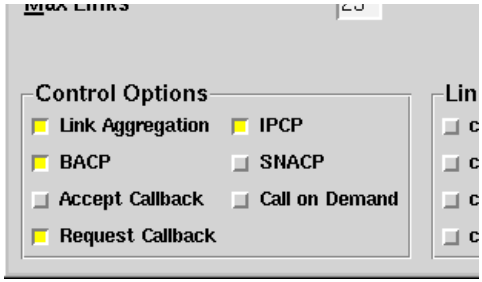

Figure 3-6. Outbound Request Callback

Under Control Options for the Outbound Link, click on the Request Callback option to enable it, as shown in Figure 3-6.

This instructs Server B to request a callback from Server A when a channel is to be added to the session.

Accepting a Callback on an Outbound Link

An additional Callback scenario exists for BACP whereby the DataFire PRIme makes a call, and the called device negotiates for added channels by requesting a callback from the DataFire PRIme (instead of waiting for the DataFire PRIme to add the channels).

This scenario is not possible between two DataFire PRIme adapters because the DataFire PRIme does not support Request Callback on Inbound Links. It is supported as a feature on the Outbound Link because there may be other devices that do support this type of callback and situations where cost or security concerns require it. To enable, click on BACP and Accept Callback when configuring an Outbound link.

Example 2: Clients to Server

With one PRI line controlled by the DataFire PRIme, multiple BRI clients calls can be answered at the same time.

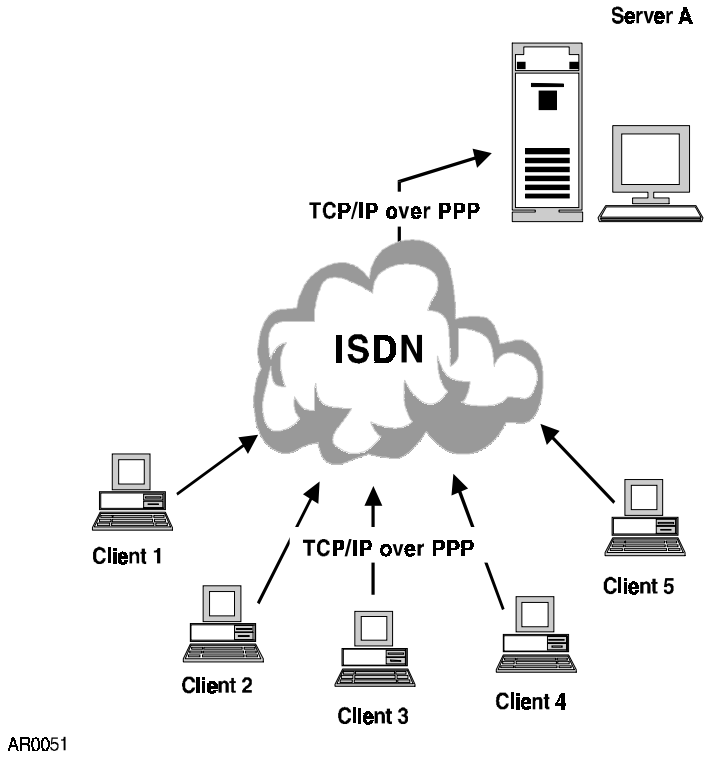

Figure 3-7. Client to Server Scenario

Setup Requirements

The setup requirements that follow describe how to set up Inbound Links on Server A for the clients that will call. Client setup depends on the equipment used in the client system.

In this scenario, client machines call Server A. The following feature is used:

- IP Pools for Remote IP assignment

Server A Setup for a Client

Each client that will call must have a separate "account" set up for it, using the Link Entry screen. For this example, that would be five separate links, one for each client.

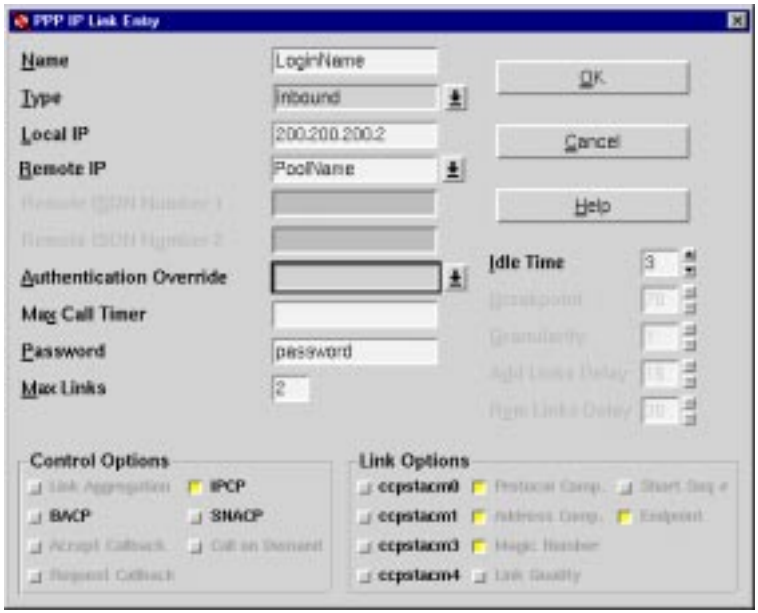

Figure 3-8. Setup for a Client Call

Name and Password: Each client must have a unique name, analogous to a Login Name, and a password.

Local IP: In this situation, this IP is left at the Global default.

Remote IP: Because it provides the most flexibility, clients should be set up to request an IP from the server. Once the call is accepted by Server A, an IP address will be assigned from the pool of IP addresses named in this field. (Note that the IP pool must be created before using its name in the Link Entry screen.)

Idle Time: In this example, after three minutes without packet traffic, the call will be torn down by Server A. This keeps channels free for other calls.

Client Setup

To have the remote IP assigned by Server A, clients must configure their network connection to obtain an IP address automatically or use 0.0.0.0 as their IP address.

How It Works

Once the *mpd* and *netd* daemons are running, all incoming client calls that have a link "account" will be answered and authenticated using Name and Password. The client will be assigned an IP address from the pool (Remote IP = PoolName). The client can use up to two B channels during the call (Max Links = 2). If three consecutive minutes of no traffic accumulate, the session will be brought down (Idle Time = 3).

Application Scenario

The obvious application for this example is an Internet Service Provider that offers ISDN service to clients, but there are other applications that this example fits equally well. Bank ATMs that must call their central office to access the database could use this setup and also cash registers at a retail outlet to verify credit cards or checks.

Example 3: IP Routing

By using a single PRI connection between two servers with LANs, multiple users on either LAN can effectively access either system.

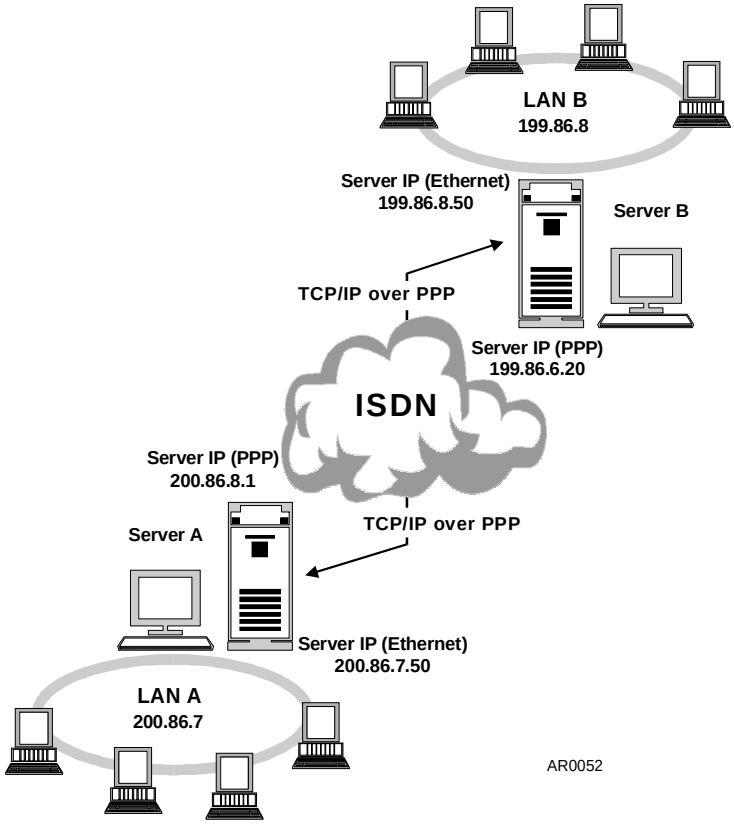

Figure 3-9. IP Routing Scenario

Setup Requirements

The setup requirements that follow describe how to set up the servers if both use a DataFire PRIme, but any PRI device using Multi-link PPP can interact with the DataFire PRIme and could be set up in a similar manner.

In this scenario, Servers A and B are used to route calls between two LANs. The setup makes calls transparent to the users on either LAN. The following features are used:

- Call On Demand
- Link Aggregation

Server Setup For this example, both servers will be able to call, or receive calls from, the other server. Therefore, both servers need an Inbound and an Outbound Link defined.

Server A Inbound

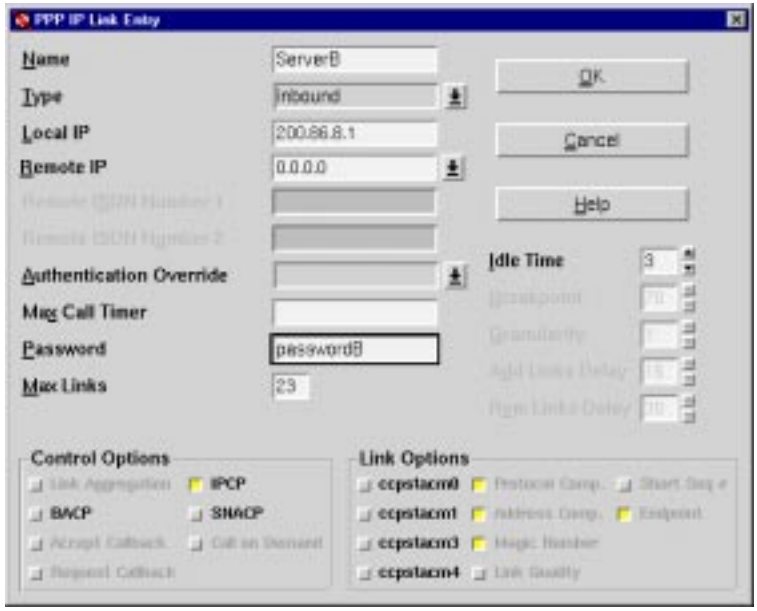

Figure 3-10. Server A Inbound Link Setup

Name and Password: The contents of the Name field and the password provided in the Password field are used together to authenticate the incoming call. The Outbound link on Server B must use the same name and password.

Local IP: The IP address assigned to the DataFire PRIme is effectively the gateway address for the users on LAN A.

Remote IP: Using 0.0.0.0 causes Server B to supply it's Local IP address as the Remote IP. In this example that would be 199.86.6.20.

Max Links: (Maximum number of channels that can be brought up during the session) Figure 3-10 shows that all 23 channels are available for this call. Since multiple users will be accessing the other server, it makes sense to allow multiple channels to be used.

Idle Time: In this example, after three minutes without packet traffic, the call will be torn down.

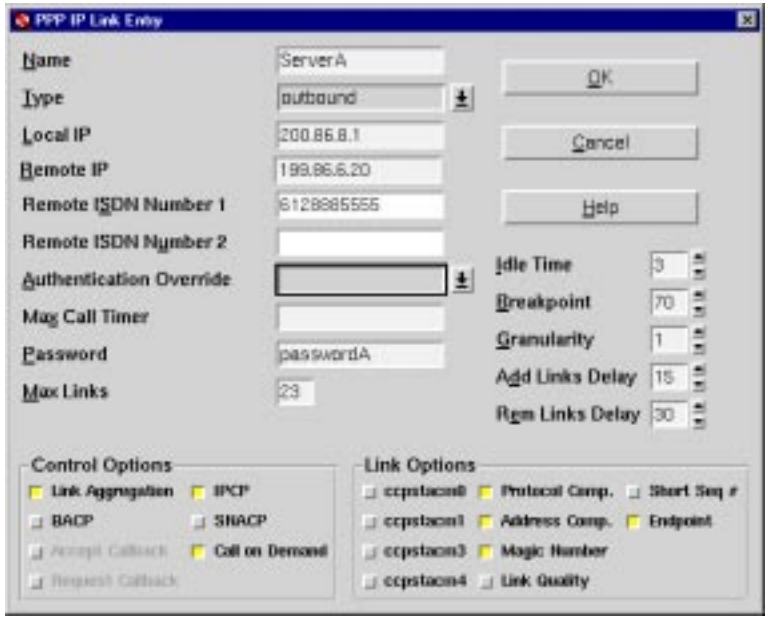

Figure 3-11. Server A Outbound Link Setup

Name and Password: The contents of the Name field and the password provided in the Password field are used together to authenticate the incoming call. The Outbound link on Server B must use the same name and password.

Local IP: The IP address assigned to the DataFire PRIme is effectively the gateway address for the users on LAN A.

Remote IP: To use Call On Demand, the IP of the remote server must be supplied in this field. The IP address of Server B is 199.86.6.20.

Max Links: (Maximum number of channels that can be brought up during the session) Figure 3-10 shows that all 23 channels are available for this call. Since multiple users will be accessing the other server, it makes sense to allow multiple channels to be used.

Idle Time and Call On Demand: In this example, after three minutes without packet traffic, the call will be torn down. Since *Call on Demand* is also enabled, the DataFire PRIme will identify when new data is ready to transfer and then re-establish the connection automatically.

Link Aggregation: With this feature enabled, channels will be added to the session automatically as utilization by user applications across

the WAN increases and automatically subtracted when utilization drops.

Cost and the throughput required are important factors to balance when making a decision about the bandwidth to make available for a session. In this example, user demand will have peaks that can be accommodated by adding channels. However, a trade-off between cost and throughput still exists.

See page 3-2 for more information.

Server B Inbound

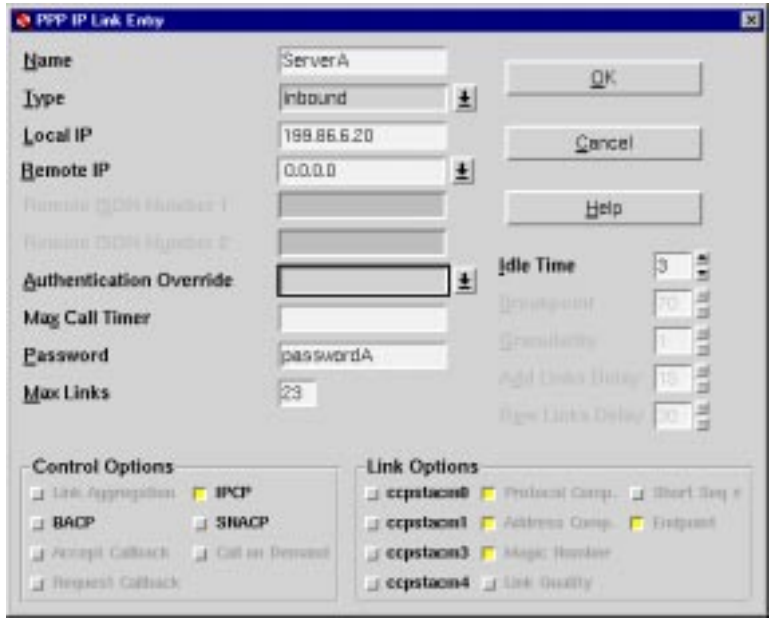

Figure 3-12. Server B Inbound Link Setup

The Inbound Link setup for Server B is the same as the Inbound Link setup for Server A except for the Name, Password, and Local IP address. The Name and Password must be the same as used for the Server A Outbound Link. The Local IP address is 199.86.6.20 whether it is an Inbound or Outbound Link.

Server B Outbound

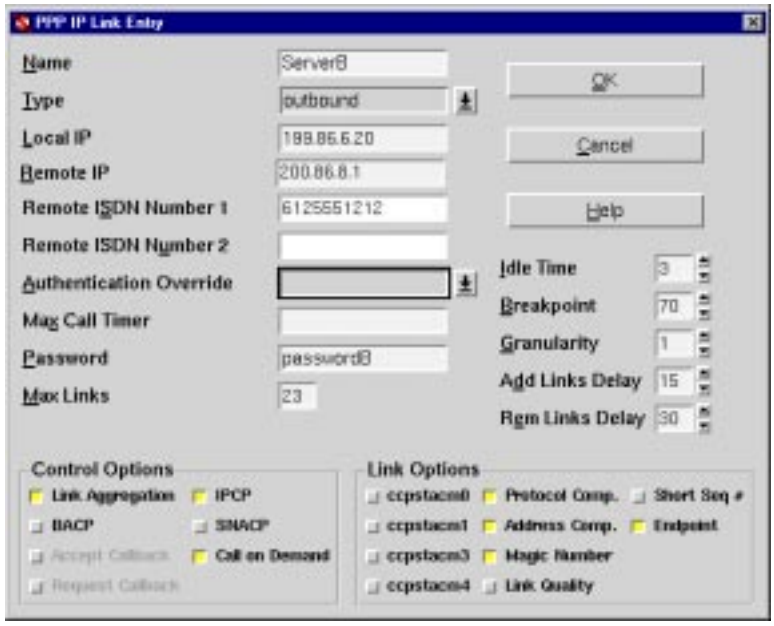

Figure 3-13. Server B Outbound Link Setup

The Outbound Link setup for Server B can be the same as the Outbound Link setup for Server A except for Name, Password, and Local IP address. The Name and Password must be the same as those used for the Server A Inbound Link. The Local IP address is 199.86.6.20 whether it is an Inbound or Outbound link.

Other Setup: ***Route Tables***

In order for IP packets to be routed between the LANs that are attached to the servers, each server must have an entry for the other LAN in its Route Table. If an automatic routing protocol (like RIP) is enabled on the servers, the Route Tables will be automatically updated. Otherwise, you must manually add the entries using the *route add* command.

At the command line on Server A, type:

```
route add -net 199.86.8.0 200.86.8.1 1
```

On Server B:

```
route add -net 200.86.7.0 199.86.6.20 1
```

Additionally, to configure your Solaris host you should remove the */etc/notrouter* file, if present, and reboot. See the Solaris man pages on *route*, *routing*, *routed* and *ip*.

Users

Once the proper route entries are made to the server Route Tables, the users on LAN A and LAN B can use the default gateways for their system: for LAN A that would be 200.86.7.50, and for LAN B that would be 199.86.8.50.

How It Works

Once the Inbound and Outbound links on both servers are configured and the *mpd* and *netd* daemons are running on both servers, the link can be brought up with on-demand traffic and static routes, or the system administrator for Server A may manually bring up the link by typing the following at the command prompt:

```
mlpconn -s A ServerB
```

Without an application running to use the connection, it will go idle within three minutes (Idle Time = 3).

The system administrator of Server B must type the following at the command prompt:

```
mlpconn -s A ServerA
```

Without an application running to use the connection, it will go idle within three minutes (Idle Time = 3).

Now an application on either LAN can open a call to the other server at any time. Once a connection is made, any traffic destined for the other server will keep the connection open, regardless of which server originally opened the call. Channels will be added or subtracted, or the connection dropped, depending on utilization.

For example, if a user application on LAN A is instructed to access a file on Server B, then Server A (as a gateway to Server B), will initiate a call (assuming a connection is not already in place). After the Name and Password are authenticated by Server B, and the connection is made, the file is available to the application. If, meanwhile, a user application on LAN B requires a file from Server A, it is available because the connection is already made. The initial connection is one B channel.

Since user applications from either LAN can now access data from either server using the existing session, more B channels to service the traffic may be added. Each time utilization of the B channels already in use reaches 70% (Breakpoint = 70) for 15 consecutive seconds (Add Link Delay = 15), one B channel will be added to the session (Granularity = 1). Subsequently, if the utilization drops below the Breakpoint for 30 consecutive seconds (Remove Link Delay = 30), one B channel will be dropped until the session is back to one channel.

After three minutes of no traffic over the connection (Idle Time = 3), the

connection will be torn down until another request for data causes the connection to be automatically brought up (Call on Demand).

The process works the same regardless of which Server places the initial call.

Using BACP with Callback

If there is a cost advantage to having one server place most calls to support a session, BACP with Callback can be used. See page 3-8 for more information.

Application Scenario

A corporation with remote branch offices could take advantage of the setup described by this example. When communication must effortlessly flow between offices, this solution is easy and effective. E-mail and database sharing are just two examples of the type of person-to-person communication that is becoming increasingly important to world-wide corporate enterprises.

chapter **4**

Trace and Statistics

In this chapter

Digi provides several tools for you to use when evaluating the operation of the DataFire PRIme— a trace utility (*isdntrace*) and a two statistic reporting utilities (*mlpstat* and *isdnstat*).

This chapter discusses the following topics:

Gathering Information

There are three tools you can use to obtain information about the system subnet activity: *mlpstat*, *isdntrace* and *isdnstat*.

These tools are invoked from the command line and return specific, but different, data about the ISDN routing you have set up.

Information about links

Use *mlpstat* to display data about each link that is currently up, inbound and outbound. You can identify the number of channels in use for a particular link and examine the number of packets transmitted and received.

Information about low-level protocols

Use *isdntrace* to view low-level protocol events on a particular subnet.

Information about ISDN traffic

Use *isdnstat* to examine the number of packets exchanged on a specific subnet and identify the types of errors that may have occurred.

Each of these tools is discussed in more detail, and example commands are provided, on the following pages. For an exhaustive discussion of all command options, see the man pages.

Procedure Follow these general steps to gather information about subnet operation:

1. Login as root.
2. Determine the subnet letter you will be working with and/or determine the link names for which you want to gather statistics. You can get this information using wancfg, or by examining the isdnconf files in the /etc directory.
3. Invoke the tool by typing it's name on the command line with the appropriate arguments.
4. Examine the output. You can use a shell script to provide continuous output to the console or redirect the output to a file to save it.

mlpstat

Displays statistics for the PPP links that are currently in use.

When to use

Use to monitor:

- Number of channels used by a link before adding or subtracting a channel (using mlpadd and mlpsub)
- BACP
- Link Aggregation by comparing the statistics over time to ensure that the number of channels changes when the number of Octets transmitted and received changes.
- Call on Demand activity by examining the Started at and Last change entries.

Command format

mlpstat -s <*subnet*> <*linkname*> -v

subnet

corresponds to a letter assigned in *wancfg*. Each adapter in the system has a designated subnet letter as is shown in the contents pane. You must include the -s argument on the command line.

linkname

is the name assigned to the link during setup, using *wancfg*. If you do not designate a linkname, statistics for all links that are up on the subnet will be displayed.

-v

verbose, use to display more complete statistics. Without this flag, only the *Type of call* and *Link Count* statistics are displayed.

Example

Example command:

```
# mlpstat -s A adminA -v
```

isdntrace

Displays the messages passing through the ISDN, MLP, and LAPD protocols.

When to use

Use to trace low-level events occurring on the subnet.

Command format

isdntrace -s <*subnet*> -p <*protocol*> -v -a

subnet

corresponds to a letter assigned in *wancfg*. Each adapter in the system has a designated subnet letter as is shown in the contents pane. You must include the -s argument on the command line.

protocol

is the protocol you want to trace: isdn, lapd, mlp

-v

verbose, use to display more complete trace data

-a

ascii, displays data in ASCII format

-?

displays exhaustive list of options

Example

/etc/isdntrace -s A -p isdn

Displays tracing for subnetwork A at the isdn protocol layer (ISDN).

/etc/isdntrace -s A -a

Displays tracing on subnetwork 'A' for the default protocol (ISDN), in ASCII.

/etc/isdntrace -s C -p lapd

Displays tracing on subnetwork 'C' for the LAPD protocol layer.

isdnstat

Displays statistics regarding the isdn protocol layers on a subnet.

When to use

Use to obtain packet statistics and error information.

Command format

isdnstat -s <*subnet*> -p <*protocol*> -v -a

-s subnet

corresponds to a letter assigned in *wancfg*. Each adapter in the system has a designated subnet letter as is shown in the contents pane.

-p protocol

is the protocol to display statistics for isdn or lapd

-v

verbose, use to display more complete statistics data.

-a

ascii, displays data in ASCII format

-?

displays exhaustive list of options

Examples

/usr/bin/isdnstat -s A -p lapd

/usr/bin/isdnstat -s C -p isdn

appendix ***A***

Configuration Worksheets

In this chapter

Use the worksheets in this chapter to record the information you will need during installation and configuration of the DataFire PRIme adapter and driver.

Worksheets provided in this chapter:

ISDN-PRI Parameters

Use the Worksheet below to note the parameters for each ISDN line in the system. Each ISDN-PRI line creates a subnet when configured.

Worksheet 4-1: ISDN-PRI Parameters

Parameters	**Subnet ___**	
Adapter Model	23 B + D (T1)	30 B + D (E1)
Switch Type *Mark the type of switch used at the Central Office*	❑ National ISDN_2 ❑ ATT_5ESS ❑ DMS_100	❑ ETSI
Incoming Bearer Capability *Mark the types of Bearer Capability the adapter should accept for incoming calls*	❑ Speech ❑ Unres Digital ❑ 3.1 khz ❑ Res Digital ❑ Unres Digital 56	❑ Speech ❑ Unres Digital ❑ 3.1 khz ❑ Res Digital
Long/Short Haul Line *Mark the correct Long Haul or Short Haul parameters* *(See page 1-8 for more information about this option)*	❑ Long Haul Pulse: ❑ -0.0 dB ❑ -7.5 dB ❑ -15.0 dB ❑ -22.5 dB Equalization: ❑ High ❑ Low ❑ Short Haul ❑ 0 - 133 feet ❑ 134 - 267 feet ❑ 268 - 400 feet ❑ 401 - 532 feet ❑ 533 - 655 feet	

Global PPP Parameters

Record the global PPP parameters for each subnet (ISDN-PRI line).

Worksheet 4-2: Global PPP Parameters

Parameter	Subnet __	Subnet __	Subnet __
Adapter IP Address	___.___.___.___	___.___.___.___	___.___.___.___
DNS (PRimary)	___.___.___.___	___.___.___.___	___.___.___.___
DNS (Secondary)	___.___.___.___	___.___.___.___	___.___.___.___
Local ISDN Number	___.___.___.___	___.___.___.___	___.___.___.___
CHAP System ID			
Log File Name			

IP Pools

Record the IP addresses or ranges of addresses that can be used as a pool for inbound calls that request an IP address.

Worksheet 4-3: Pools

Subnet ____

Pool Name	Ranges of (or individual) IP Addresses			
	___.___.___.___	___.___.___.___	___.___.___.___	___.___.___.___
	___.___.___.___	___.___.___.___	___.___.___.___	___.___.___.___
	___.___.___.___	___.___.___.___	___.___.___.___	___.___.___.___
	___.___.___.___	___.___.___.___	___.___.___.___	___.___.___.___
	___.___.___.___	___.___.___.___	___.___.___.___	___.___.___.___
	___.___.___.___	___.___.___.___	___.___.___.___	___.___.___.___
	___.___.___.___	___.___.___.___	___.___.___.___	___.___.___.___
	___.___.___.___	___.___.___.___	___.___.___.___	___.___.___.___
	___.___.___.___	___.___.___.___	___.___.___.___	___.___.___.___
	___.___.___.___	___.___.___.___	___.___.___.___	___.___.___.___

Outbound Links

This worksheet corresponds to the choices for outbound calls that you can make.

Worksheet 4-4: Outbound Links

Outbound Link Parameters	Subnet ____			
Outbound Link Name				
Local IP Address	___.___.___.___	___.___.___.___	___.___.___.___	___.___.___.___
Remote IP (or 0.0.0.0)	___.___.___.___	___.___.___.___	___.___.___.___	___.___.___.___
Remote ISDN Number 1				
Remote ISDN Number 2				
Override Authentication?				
Max Call Timer (minutes)				
Password				
Max Links (# channels)				
Idle Timer (minutes)				
Use Link Optimization?				
Breakpoint (%)				
Granularity (# channels)				
Add Links (seconds)				
Remove Links (seconds)				
Use Call On Demand?				
Use BACP?				
With Callback Request?				
With Callback Accept?				

Inbound Links

Use this worksheet to choose parameters for Inbound calls for each subnet (or ISDN line).

Worksheet 4-5: Inbound Links

Inbound Link Parameters	Subnet ____			
Inbound Link Name				
Local IP	___.___.___.___	___.___.___.___	___.___.___.___	___.___.___.___
Remote IP/Pool Name				
Override Authentication?				
Max Call Timer (minutes)				
Password				
Max Links (# channels)				
Idle Timer (minutes)				
Use BACP?				
With Callback Accept?				

appendix ***B***

Quick Reference

In this chapter Use this chapter to quickly find a command syntax or short-cut key sequence

This chapter discusses the following topics:

Using the Quick Reference

All of the items provided in the Quick Reference are explained in the previous pages of this manual. They are reproduced in the Quick Reference to make it easier for you to use them.

The Quick Reference can be removed from the manual or reproduced so that it is handy when you need it.

Quick Reference

Command Line Reference

Configuration Utility **wancfg**

Brings up the configuration utility. Use the following commands first if you are working from a workstation on the LAN instead of from the server:

For *ksh*: export DISPLAY=<IP address or name>:0.0

Example:

```
#export DISPLAY=rodger:0.0
```

For *csh*: DISPLAY=<IP address or name>:0.0

export

Example:

```
#DISPLAY=rodger:0.0
#export
```

Statistics Utilities **mlpstat** -s <*subnet*> <*linkname*> -v

Displays statistics for the PPP links that are currently in use.

Example command:

```
# mlpstat -s A adminA -v
```

isdnstat -s <*subnet*> -p <*protocol*> -v -a

Displays statistics regarding the isdn protocol layers on a subnet.

Example commands:

```
#/usr/bin/isdnstat -s A -p lapd
#/usr/bin/isdnstat -s C -p isdn
```

Trace Utility **isdntrace** -s <*subnet*> -p <*protocol*> -v -a

Displays the messages passing through the ISDN, MLP, and LAPD protocols.

Example commands:

```
#/etc/isdntrace -s A -p isdn
#/etc/isdntrace -s SUB1 -a
```

Connection commands **mlpconn -s** <*subnet*> <*connection_name*>

Use this command to initiate an outbound call.

Example:

```
mlpconn -s A boston
```

mlpadd -s <*subnet*> *connection_name*

Use this command to expand the number of B channels used during a connection by one.

Example:

```
mlpadd -s A boston
```

mplsub -s <*subnet*> *connection_name*

Use this command to subtract one B channel from an outbound connection that is currently up.

Example:

```
mlpsub -s A boston
```

mlpdisc -s <*subnet*> *connection_name*

Use this command to terminate an outbound link:

Example:

```
mlpdisc -s A boston
```

Short-cut Keys for wancfg

Navigating the Utility

You can use your mouse to click on items, or you can use "Hot keys" as explained below:

- You can access items in a window by holding down the <Alt> key and pressing the underlined letter in an item. Example: To pull down the File menu, press <Alt> and F simultaneously.
- Use the <Tab> key to move between fields.
- Use the space bar to toggle a check box on or off.

Special Control Key Functions

Press the <Ctrl> key along with the keys listed to get short-cut access to the functions:

<Ctrl> + U	Undo, or reset values to default
<Ctrl> + R	Remove a Digi adapter from the configuration
<Ctrl> + N	Add a Digi adapter to the configuration
<Ctrl> + K	Keep adapter configuration information when switching out an adapter
<Ctrl> + A	Advanced options for ISDN-PRI and PPP; click on Help for more information

Index