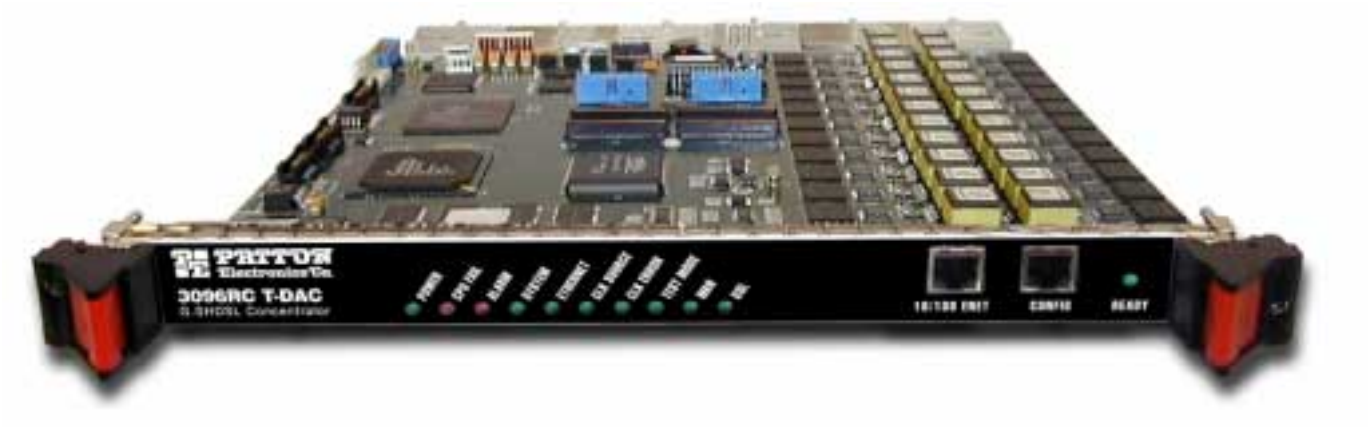
PATTON Electronics Co.

Model 3096RC

G.SHDSL TDM-Digital Access Concentrator (T-DAC)

Administrator's Reference Guide



Sales Office: **+1 (301) 975-1000**
Technical Support: **+1 (301) 975-1007**
E-mail: **support@patton.com**
WWW: **www.patton.com**

Document Number: **110112U Rev. A**
Part Number: **07MD3096RC-ARG**
Revised: **August 29, 2003**

Patton Electronics Company, Inc.
7622 Rickenbacker Drive
Gaithersburg, MD 20879 USA
Voice: **+1 (301) 975-1000**
Fax: **+1 (301) 869-9293**
Technical Support: **+1 (301) 975-1007**
Technical Support e-mail: **support@patton.com**
URL: **www.patton.com**

Contents

About this guide

This guide describes configuring a Patton Electronics Time Division Multiplexed (TDM) Digital Access Concentrator (T-DAC). This section describes the following:

- Who should use this guide (see “Audience”)
- How this document is organized (see “Structure”)
- Typographical conventions and terms used in this guide (see “Typographical conventions used in this document” on page 8)

Audience

This guide is intended for the following users:

- System administrators
- Operators
- Installers
- Maintenance technicians

Structure

This guide contains the following chapters:

- Chapter 1 (on page 11) on describes using the Administration Page window
- Chapter 2 (on page 15) describes using the Home window
- Chapter 3 (on page 21) describes using the Import/Export window
- Chapter 4 (on page 25) describes using the System Status window
- Chapter 5 (on page 33) describes using the System History window
- Chapter 6 (on page 41) describes using the Alarms window
- Chapter 7 (on page 49) describes using the DS0 Mapping window
- Chapter 8 (on page 67) describes using the Clocking window
- Chapter 9 (on page 75) describes using the mDSL Port Configuration window
- Chapter 10 (on page 105) describes using the Ethernet window
- Chapter 11 (on page 109) describes using the Filter IP window
- Chapter 12 (on page 117) describes using the Frame Relay window
- Chapter 14 (on page 141) describes using the ICMP window
- Chapter 15 (on page 145) describes using the IP window
- Chapter 16 (on page 161) describes using the TCP window
- Chapter 17 (on page 167) describes using the UDP window
- Chapter 18 (on page 171) describes using the RIP Version 2 window
- Chapter 19 (on page 179) describes using the SNMP window
- Chapter 20 (on page 185) describes using the System window
- Chapter 21 (on page 199) describes using the System Log window

- Chapter 22 (on page 211) describes using the T1/E1Link window
- Chapter 23 (on page 237) describes the contents of the About window
- Chapter 24 (on page 239) describes the contents of the License window

Typographical conventions used in this document

This section describes the typographical conventions and terms used in this guide.

General conventions

The procedures described in this manual use the following text conventions:

Table 1. Text conventions

Convention	Meaning
Futura bold type	Indicates the names of menu bar options.
Italicized Futura type	Indicates the names of options on pull-down menus.
Futura type	Indicates the names of fields or windows.
Garamond bold type	Indicates the names of command buttons that execute an action.
< >	Angle brackets indicate function and keyboard keys, such as <SHIFT>, <CTRL>, <C>, and so on.
Are you ready?	All system messages and prompts appear in the `Courier` font as the system would display them.
`% dir *.*`	Bold Courier font indicates where the operator must type a response or command

Mouse conventions

The following conventions are used when describing mouse actions:

Table 2. Mouse conventions

Convention	Meaning
Left mouse button	This button refers to the primary or leftmost mouse button (unless you have changed the default configuration).
Right mouse button	This button refers the secondary or rightmost mouse button (unless you have changed the default configuration)
Point	This word means to move the mouse in such a way that the tip of the pointing arrow on the screen ends up resting at the desired location.
Click	Means to quickly press and release the left or right mouse button (as instructed in the procedure). Make sure you do not move the mouse pointer while clicking a mouse button. Double-click means to press and release the same mouse button two times quickly
Drag	This word means to point the arrow and then hold down the left or right mouse button (as instructed in the procedure) as you move the mouse to a new location. When you have moved the mouse pointer to the desired location, you can release the mouse button.

Chapter 1 Introduction

Chapter contents

Introduction

You may manage the Model 3096RC Time Division Multiplexed (TDM) Digital Access Concentrator (T-DAC) by using its internal HTTP/HTML Web Management windows. However, to access the HTTP/HTML windows, you must first define:

- The T-DAC system's LAN IP method to obtain address
- LAN IP address
- LAN IP subnet mask for the T-DAC

If you have not defined the above parameters, refer to the procedures in the Getting Started Guide that came with your T-DAC

Logging into the HTTP/HTML Web Management windows

To log into the HTTP/HTML Web Management windows, you must enter the 4-octet Internet Protocol (IP) address (for example, *http://your.server.ip.address*) as the Universal Resource Locator (URL) into a World-Wide Web (WWW) browser. After you enter the IP address, the T-DAC will ask for your user name and password as shown in figure 1.

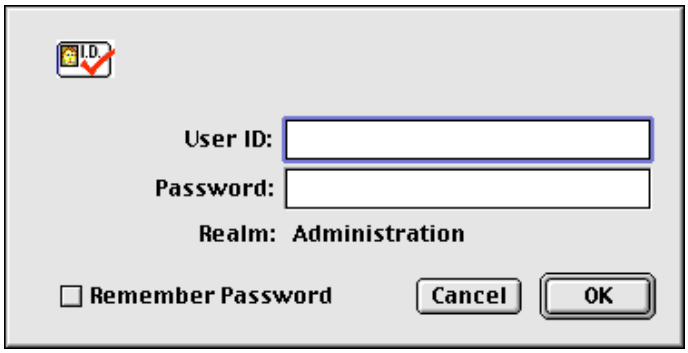


Figure 1. T-DAC login window

Your T-DAC will accept the following default administrative passwords:

- **superuser**—this password carries full permission to change and view any parameters in the T-DAC
- **monitor**—this password allows full viewing of any non-password oriented variables.

Note For security reasons, we recommend that you change these passwords immediately after initial configuration.

HTTP/HTML and SNMP Object Format

In this document, we shall describe the variables found on each of the internal HTTP/HTML windows. This description will include brief definitions of the Patton Enterprise MIB or SNMP MIB II object identifiers wherever applicable. The format of the variables will resemble figure 2.

Figure 2. HTTP/HTML and SNMP object format

Saving HTTP/HTML Object Changes

Sometimes you will need to save changes that you have made in the HTTP/HTML windows. Do the following to make changes to read/write variables:

1. Select the appropriate Modify screen.
2. Make changes to the desired parameter.
3. Click on the **Submit** button.
4. Return to the HOME screen.
5. Click on the **Record Current Configuration** button.

> **Note** Make sure you follow steps 1 through 5 when modifying the HTTP/HTML windows. Otherwise, your changes will be lost when the T-DAC is power-cycled.

Chapter 2 Home

Chapter contents

Introduction

The T-DAC Web Management HOME window is the first management window that you see after logging into the T-DAC (see figure 3).

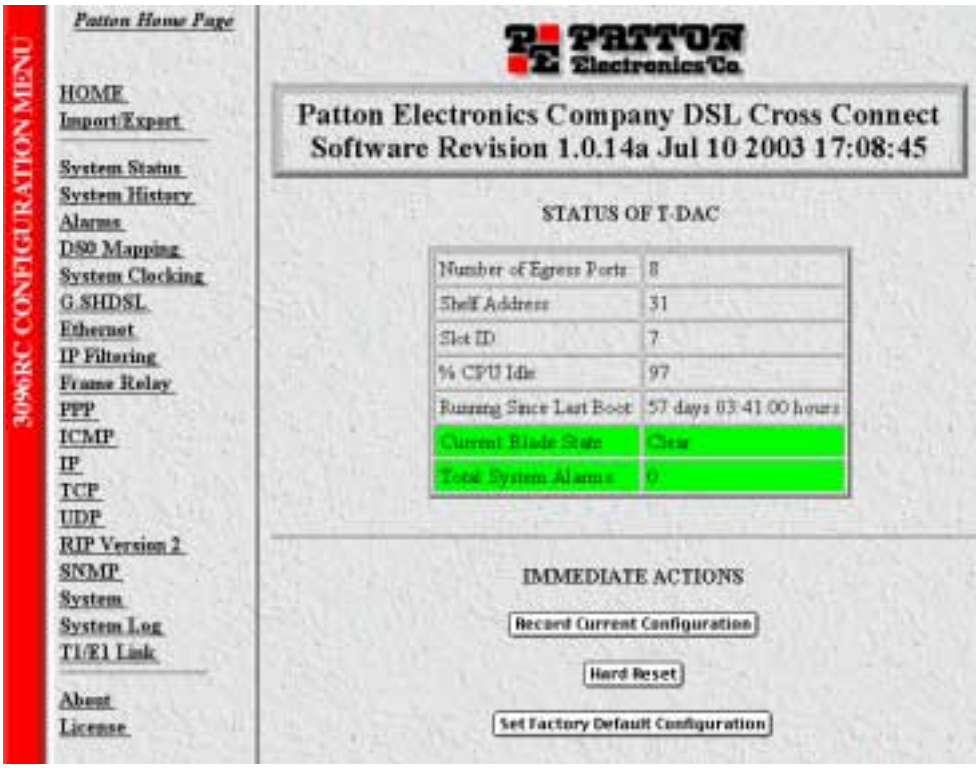


Figure 3. HOME window

The HOME window consists of sections that enable you to:

- View general product information about the T-DAC, such as the current software version (see section "Product information box" on page 18)
- View a summary of the system's operating status that includes the following information:
  - Number of egress ports on the rear blade
  - Shelf address
  - Slot ID
  - Percent of idle CPU time
  - Amount of time since the last time the system software was restarted (also referred to as *booting*)
  - Current T-DAC (front blade/rear blade) alarm status, which displays the highest-level alarm currently detected in the T-DAC—listed as *Major*, *Minor*, or *Clear* (for none)
  - Total alarms active in the T-DAC

  See section "Operating status variables" on page 18 for more information.

- Initiate the following *immediate actions*:
  - Save any changes you have made to the T-DAC's system configuration
  - Perform a hard reset (*cold restart*) of the system without power-cycling the T-DAC. Reset all the T-DAC's configurable parameters to their factory-default values.

  See section "Immediate Actions" on page 19 for more information.

The HOME window is divided into two *panes*: the Configuration Menu pane and the configuration/information pane (see figure 4). The Configuration Menu contains the links to the various T-DAC subsystem windows, while the configuration/information pane is where you can view status and other information, or make changes to the system configuration. Unlike the Configuration Menu pane, which looks the same no matter which subsystem window you may move to, the configuration/information pane contents will change as you move from one subsystem window to another.

Note Clicking on the HOME link in the Configuration Menu pane returns you to the HOME window from any other window.

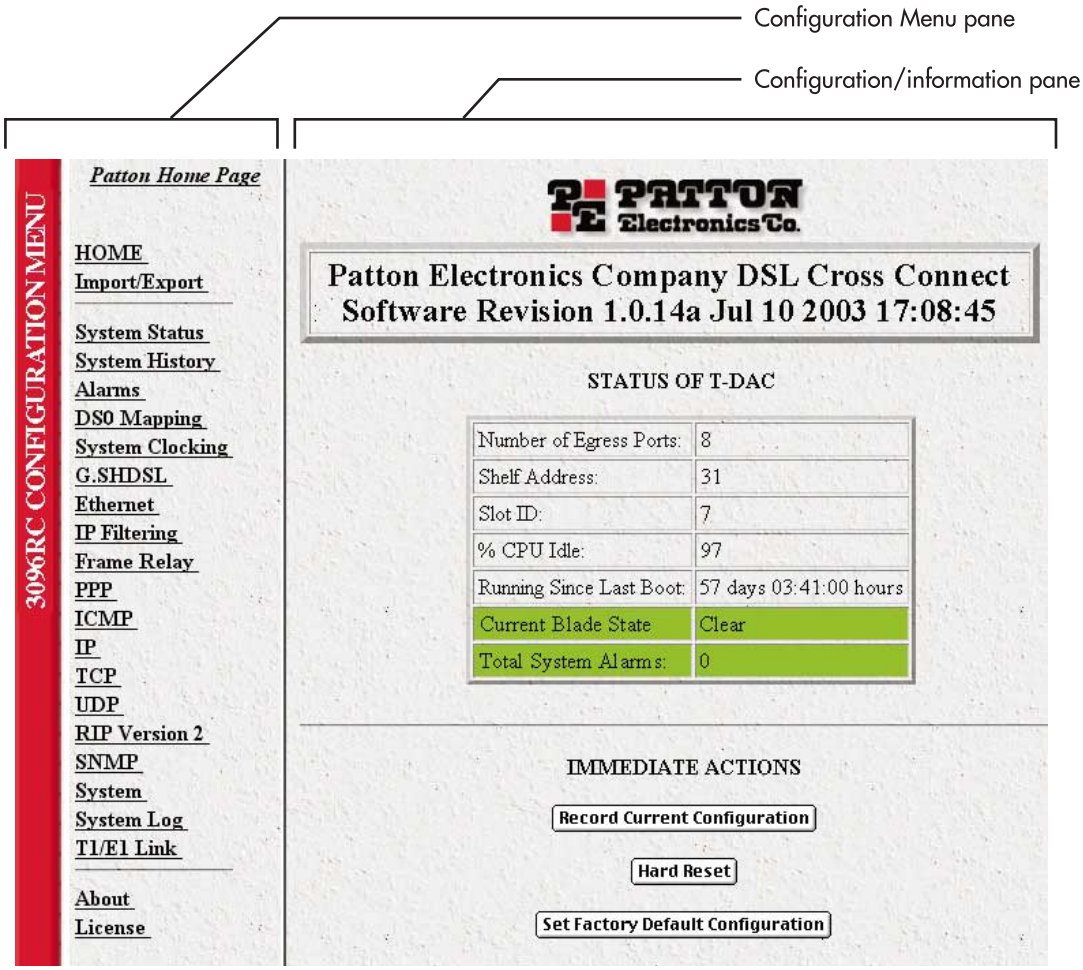


Figure 4. HOME window panes

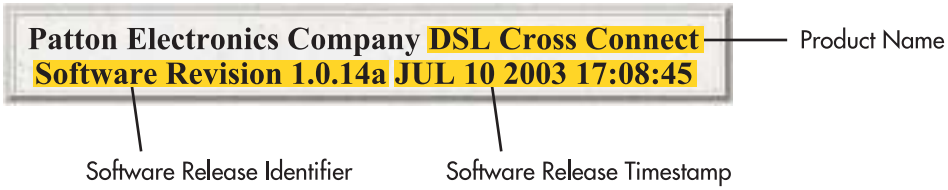


Figure 5. Product information section of Home window

Product information box

The product information box (see figure 5) displays the following:

- Product name: *DSL Cross Connect*
- Software release identifier: The current software version running on the T-DAC. The identifier is in the form *X.Y.Z*(*n*) where:
  - *X* denotes a major release involving an extensive system revision.
  - *Y* indicates a revision within Release *X* adding one or more new features.
  - *Z* denotes a revision within Release *X.Y* correcting problems that were found in the previous release.
  - *n* (optional) is a lowercase alpha character. The value *b* for *beta* may indicate software made available to certain parties for before the official formal release to the general public, often for early access trials or field testing.
- Software release timestamp: The date and time the software version was created.

Operating status variables

The system variables that describe the operating status of the T-DAC are shown in figure 6 and described in the following sections.

Number of Egress Ports:	8
Shelf Address:	31
Slot ID:	7
% CPU Idle:	97
Running Since Last Boot:	57 days 03:41:00 hours
Current Blade State	Clear
Total System Alarms:	0

Figure 6. STATUS menu

Number of Egress Ports (boxEgressCount)

Defines the number of T1/E1 WAN egress ports (4, 8, or 16) on the rear blade.

Shelf Address (cPCIShelfAddr)
Indicates the address of the ForeFront chassis in which the 3096RC resides. The address is set via DIP switches located ForeFront chassis midplane. Using various On/Off combinations up to 33 (0-32) binary shelf addresses can be defined. See ForeFront chassis User Guide for more information

Slot ID (cPCISlotID)
Indicates the ForeFront chassis slot number occupied by the 3096RC. On the ForeFront chassis models 6276 and 6476, slot numbering sequence starts from the bottom with slot number 1. Numbering sequence for the ForeFront model 6676 starts from the left of the chassis with slot number 3.

% CPU Idle (boxIdleTime)
Indicates the percent of system CPU capacity currently available to the Model 3096RC.

Running Since Last Boot (sysUpTime)
The time (in hundredths of a second) since the T-DAC was last power-cycled.

Current Blade State (alarmBoxState)
The highest level alarm currently active in the T-DAC system—listed as *Critical* (red), *Major* (orange), *Minor* (yellow), or *Clear* (green)—no alarms present.

Total System Alarms (alarmTotal)
Total number of alarms currently active in the system.

Immediate Actions
In superuser mode you can initiate several immediate actions (see figure 7) which will cause the T-DAC to operate according to the descriptions in the following sections.

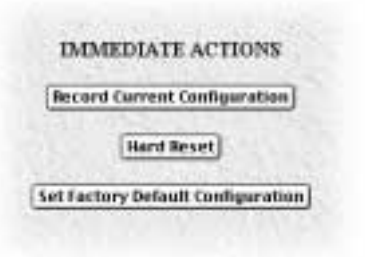


Figure 7. Immediate Actions buttons

Record Current Configuration (storeConfig(1))
Clicking the button labelled **Record Current Configuration** causes the T-DAC to save the current configuration in permanent Flash memory. In other words, configuration changes made in the subsystem web windows become permanent when you click **Record Current Configuration**.

1. Configuration changes in the T-DAC are made by clicking a button labelled **Submit Query** on any of the subsystem window. When you click **Submit Query**, the T-DAC stores the parameter values in volatile DRAM (dynamic RAM) only. Since the **Submit Query** changes take immediate effect, the administrator can test different configuration parameters without needing to change the Flash configuration each time.

2. Without clicking on **Record Current Configuration**, all configuration changes will be lost if the power is recycled. After doing the **Record Current Configuration** save, the current configuration of the T-DAC will not be lost when The T-DAC is powered down.

Note The most important step after completing the configuration is to save it in permanent memory by clicking on **Record Current Configuration**.

Hard Reset (hardReset(2))

This button causes the T-DAC to perform a cold restart. When you select **Hard Reset**, the T-DAC requests confirmation before executing the command, after which, the T-DAC will disconnect all current sessions, re-initialize the interfaces, and re-load configuration parameters from Flash memory.

Set Factory Default Configuration (forceDefaultConfig(3))

This button deletes the current configuration from Flash memory and loads the factory default parameters into Flash. The factory default settings will not take effect in the T-DAC until it has been re-booted, for example by doing a **Hard Reset**.

Note **Set Factory Default Configuration** will delete the T-DAC's Ethernet IP address, reset the password to the default administrative passwords (see section "Logging into the HTTP/HTML Web Management windows" on page 12), and any other site specific-settings made for your particular installation. In order to use the HTTP/HTML Management windows you will have to re-enter the T-DAC's Ethernet IP address and netmask using the T-DAC's front panel control port. Refer to the *Getting Started* guide for information on configuring the IP address.

Chapter 3 Import/Export

Chapter contents

Introduction

The Import/Export function enables you to make a backup (or *exported*) copy of your T-DAC's configuration parameters. By exporting the configurations, the saved files can quickly be loaded, or *imported*, into a replacement T-DAC—greatly speeding up the installation process should a T-DAC need replacing.

Note All actions for Import/Export require *superuser* access privileges.

To import or export a configuration, click on Import/Export under the Configuration Menu to display the Import/Export main window (see figure 8).

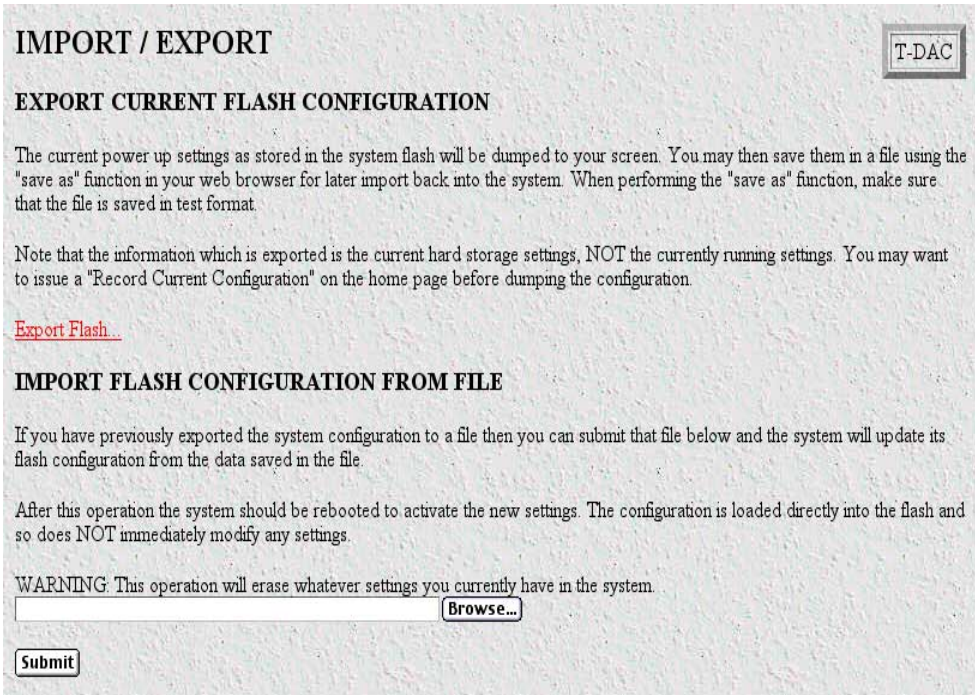


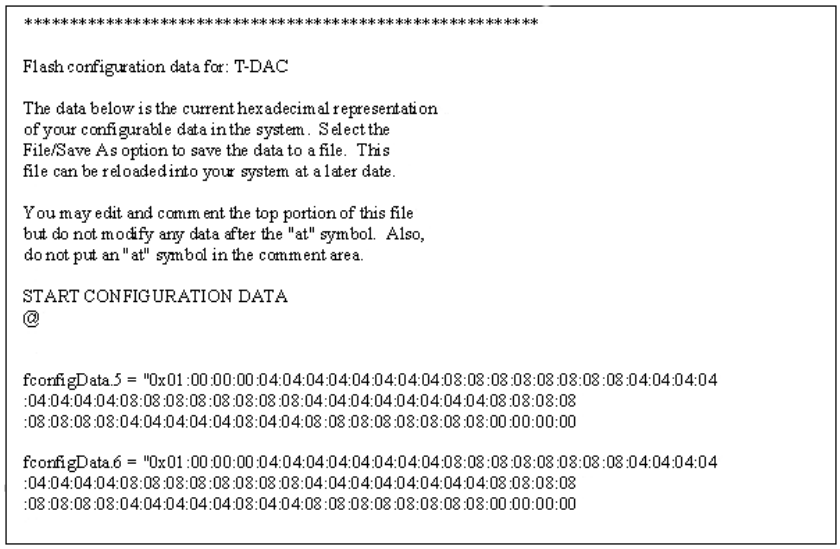
Figure 8. Import/Export main window

Export current Flash configuration

Note The exported configuration file is a text-format file. Do not try, however to edit the operating characteristics contained in the file.

Note The parameters that will be exported are the power-up settings as they are stored in Flash memory and *may not* be the current operating parameters. To ensure that you export the most current parameters, go to HOME, then click on the **Record Current Configuration** button under Immediate Actions.

To export the Flash configuration, click on the Export Flash link on the Import/Export main window. The T-DAC will display text configuration information resembling that shown in figure 9.



```
************************************************************

Flash configuration data for: T-DAC

The data below is the current hexadecimal representation
of your configurable data in the system.  Select the
File/Save As option to save the data to a file.  This
file can be reloaded into your system at a later date.

You may edit and comment the top portion of this file
but do not modify any data after the "at" symbol.  Also,
do not put an "at" symbol in the comment area.

START CONFIGURATION DATA
@


fconfigData.5 = "0x01:00:00:00:04:04:04:04:04:04:04:04:08:08:08:08:08:08:08:04:04:04:04
:04:04:04:04:08:08:08:08:08:08:08:08:04:04:04:04:04:04:04:04:08:08:08:08
:08:08:08:08:04:04:04:04:04:08:04:04:08:08:08:08:08:08:08:08:00:00:00:00

fconfigData.6 = "0x01:00:00:00:04:04:04:04:04:04:04:04:08:08:08:08:08:08:08:04:04:04:04
:04:04:04:04:08:08:08:08:08:08:08:08:04:04:04:04:04:04:04:04:08:08:08:08
:08:08:08:08:04:04:04:04:04:08:04:04:08:08:08:08:08:08:08:08:00:00:00:00
```

Figure 9. Typical T-DAC flash memory configuration data

To save the displayed data as a text file, select the **Save** option on your browser (see figure 10). For example, under Netscape, select **File** > **Save As**. A dialog box will display enabling you to save the contents of the export parameters to a text file. Select the location where you want the file stored, type a file name, and click **Save**.

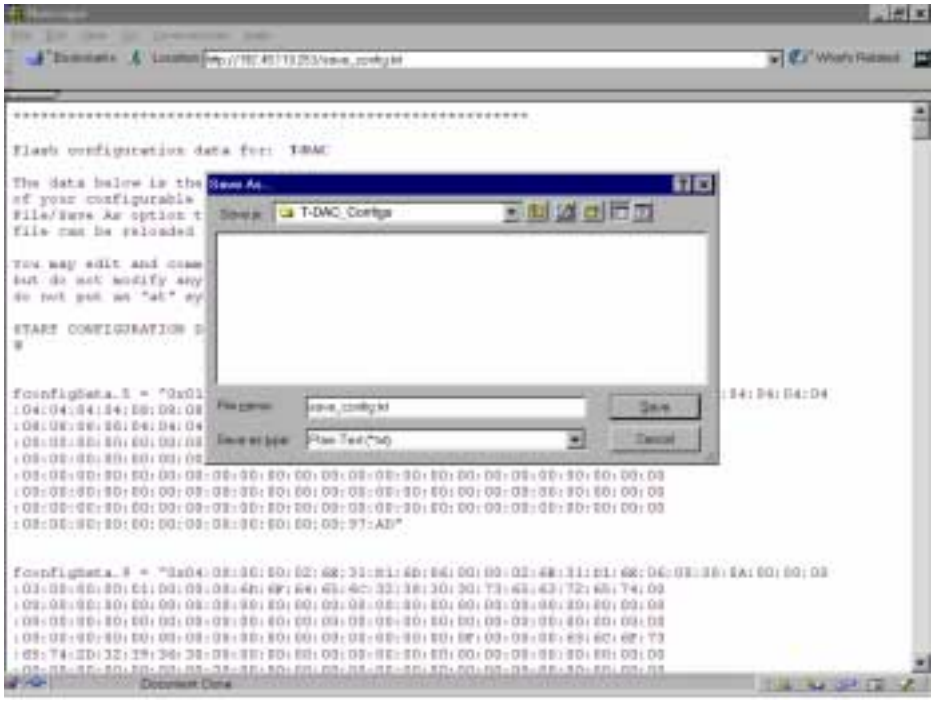


Figure 10. Saving the T-DAC flash memory configuration data as a text file

Import Flash Configuration From File

To import a configuration file into the T-DAC, type the complete path and filename for the configuration file you wish to load or click on the **Browse…** button to select the desired file, then click on the **Submit Query** button (see figure 8 on page 22).

Upon successfully importing the file, the T-DAC will display *Configuration Load Complete*, indicating that the new operating parameters have been loaded into Flash memory.

Click on HOME under the Configuration Menu, then click on the **Hard Reset** button under Immediate Actions.

Note *Do not* select **Record Current Configuration** after importing configuration parameters.

Chapter 4 System Status

Chapter contents

Introduction

The System Status window (see figure 11) displays a comprehensive status summary of the major Model 3096RC subsystems.

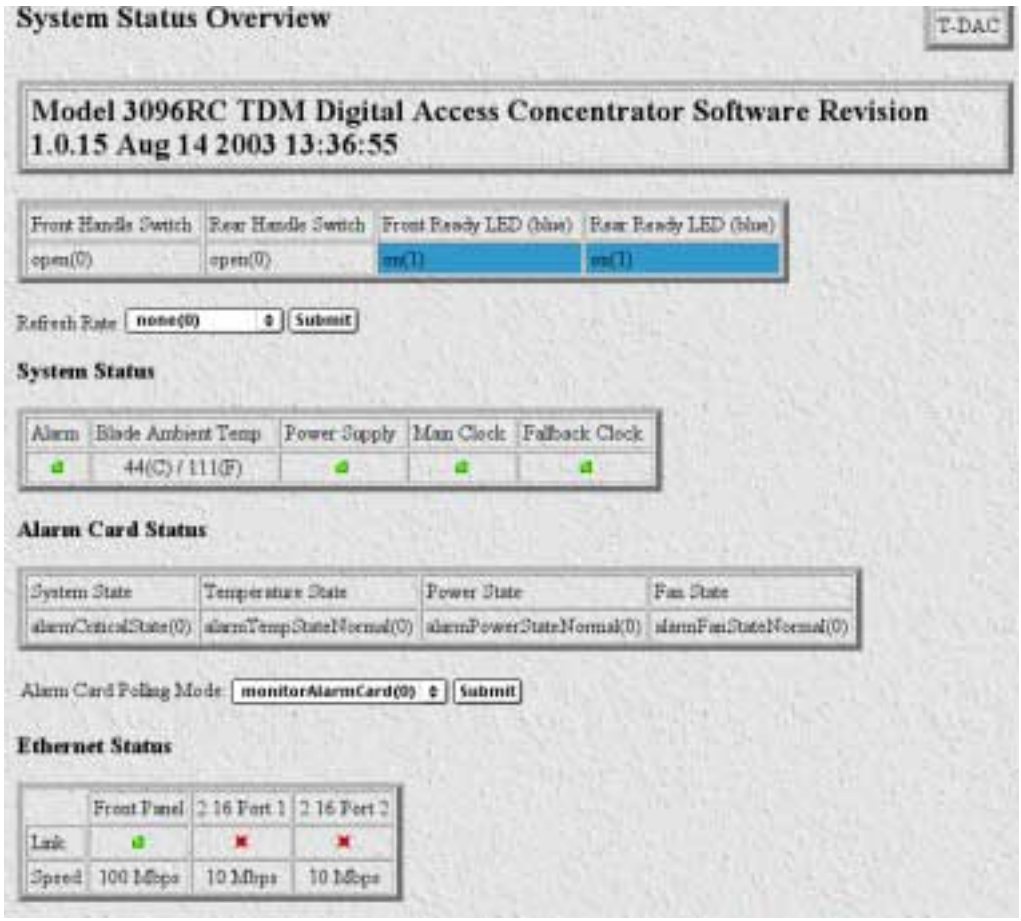


Figure 11. System Status window

The window consists of the following sections:

- **General product information**—Displays the product name, software release identifier, and software release timestamp.
- **Physical states table**—Displays current state of certain physical components of the T-DAC, including the front handle switch, rear handle switch, front READY LED (blue), and rear READY LED (blue).
- **Refresh rate parameter**—Determines how often the System Status window is refreshed.
- **System Status table**—Displays the state of alarms, the internal temperature of the 3096RC—displayed in Celsius (C)/Fahrenheit (F), the current operational status of the two power supplies and the 3096RC's system clock.
- **Alarm Card Status**—Displays the system, termperature, power, and fan status from the alarm card.
- **Ethernet Status**—Displays the link status and speed of the 3096RC's three Ethernet links.

- **T1/E1 Port Information table**—Displays the circuit name *(Circuit ID)*, and operational state *(Status)* of each WAN circuit. Clicking on the *Configure* link (WAN port number) located above each *WAN Circuit*, displays the T-DAC *WAN Circuit CONFIGURATION LINK* window for that WAN port.
- **G.SHDSL Port Information table** —Displays the name *(Circuit ID)* and operational state *(G.SHDSL Status)* of each G.SHDSL port. Clicking on the *Port* link located above each *Circuit ID*, displays the G.SHDSL port information window for that G.SHDSL port.

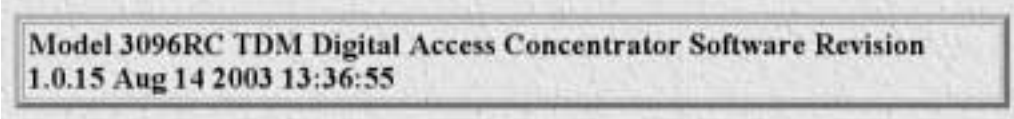


Figure 12. General product information box

General product information box

The general product information Box (see figure 12) provides the following information:

- Product name: *DSL Cross Connect*
- Software release identifier: The current software version running on the T-DAC. The identifier is in the form *X.Y.Z*(*n*) where:
  - *X* denotes a major release involving an extensive system revision.
  - *Y* indicates a revision within Release *X* adding one or more new features.
  - *Z* denotes a revision within Release *X.Y* correcting problems that were found in the previous release.
  - *n* (optional) is a lowercase alpha character. The value *b* for *beta* may indicate software made available to certain parties for before the official formal release to the general public, often for early access trials or field testing.
- Software release timestamp: The date and time the software version was created.

Figure 13. Physical states table

Physical states table

The physical states section of the System Status window (see figure 13) lists the possible conditions of the T-DAC components (see table 3).

Table 3. Physical states

Item	Setting	Description
Front handle switch	Open	The switch on at least one of the two front handles is open, indicating that the handle is unlocked. When both handles are unlocked, the blue READY LED status indicator on the T-DAC's front panel will light, indicating that the T-DAC front blade is ready for removal. The T-DAC can then be removed from the CPCI chassis.
	Closed	Both front handle switches are closed, indicating that the handles are locked and the T-DAC cannot be removed from the cPCI chassis.
Rear handle switch	Open	The switch on at least one of the two rear handles is open, indicating that the handle is unlocked. When both handles are unlocked, the blue READY LED status indicator on the T-DAC's rear blade will light, indicating that the rear blade is ready for removal. The rear blade can then be removed from the CPCI chassis.
Front READY LED (blue)	On	The blue READY LED status indicator on the T-DAC's front panel is lit, indicating the switches on both front handles are open and the handles are unlocked, so the T-DAC is ready to be removed from the CPCI chassis.
	Off	The blue READY LED status indicator on the T-DAC's front panel is not lit, indicating that the switches on at least one of the front handles are closed and the handle(s) are unlocked: the T-DAC is ***not*** ready for removal, and therefore ***cannot*** be removed from the CPCI chassis.
Rear READY LED (blue)	On	The blue READY LED status indicator on the rear blade is lit, indicating that the switches on both rear handles are open and the handles are unlocked, so the rear blade is ready to be removed from the CPCI chassis.
	Off	The blue READY LED status indicator on the rear blade is not lit, indicating that the switches on at least one of the rear handles are closed and the handle(s) are unlocked: the rear blade is ***not*** ready for removal, and therefore ***cannot*** be removed from the CPCI chassis.

Refresh rate parameter

This parameter (see figure 14) selects how often the System Status window is refreshed.

Figure 14. Refresh rate parameter

The user-selectable options are:

- **none(0)**
- **rate10sec(10)**—Refresh every 10 seconds
- **rate15sec(15)**—Refresh every 15 seconds
- **rate30sec(30)**—Refresh every 30 seconds
- **rate1min(60)**—Refresh every minute (60 seconds)
- **rate2min(120)**—Refresh every 2 minutes (120 seconds)
- **rate3min(180)**—Refresh every 3 minutes (180 seconds)
- **rate5min(300)**—Refresh every 5 minutes (300 seconds)

Click **Submit Query** after selecting the desired refresh rate.

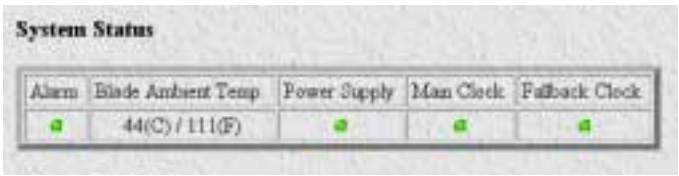


Figure 15. System status

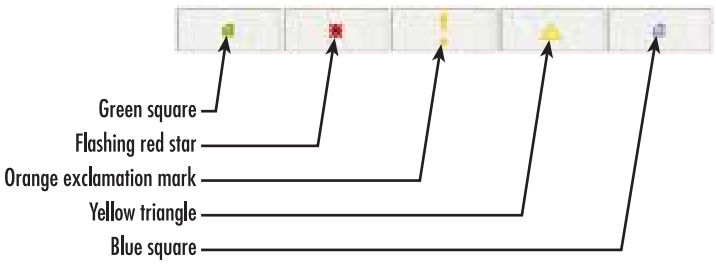


Figure 16. Alarm symbols

System status table

The system status table (see figure 15) displays the following parameters:

- **Alarm**—A flashing red star (see figure 16) indicates there is an alarm condition in the box. A green square denotes that no alarms are present and functioning properly.

Note If there is a flashing red indicator, go to the appropriate chapter listed in table 4 on page 30.

- **Blade Ambient Temp.**—Displays the internal temperature in Celsius (C)/Fahrenheit (F).
- **Power supply 1.** A flashing red star (see figure 16 on page 29) indicates there is an alarm condition in power supply 1. A green square denotes that power supply 1 is functioning properly.
- **Power supply 2.** A flashing red star (see figure 16 on page 29) indicates there is an alarm condition in power supply 2. A green square denotes that power supply 2 is functioning properly.
- **Main clock.** A flashing red star (see figure 16 on page 29) indicates there is an alarm condition in the main clock. A green square denotes that the main clock is functioning properly.
- **Fallback clock.** A flashing red star (see figure 16 on page 29) indicates there is an alarm condition in the fallback clock. A green square denotes that the fallback clock is functioning properly.

Table 4. System status/subsystem reference

Item	Recommended
Alarm	Chapter 6, "Alarms" on page 41
Blade Temp.	Chapter 6, "Alarms" on page 41
Power Supply S1	Chapter 6, "Alarms" on page 41
Power Supply S2	
Main Clock	Chapter 6, "Alarms" on page 41 and chapter 8, "System Clocking" on page 67
Fallback Clock	

Alarm Card status table

The Alarm Card status section (see figure 17) displays the system, termperature, power, and fan status from the alarm card.

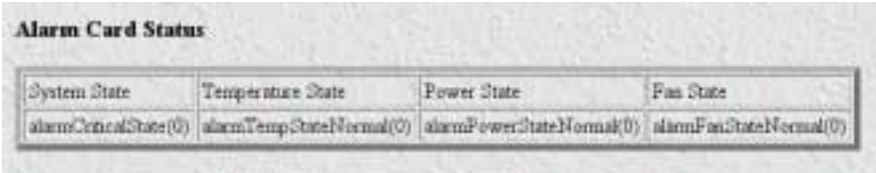


Figure 17. Alarm Card status

Ethernet status table

The Ethernet status section (see figure 18) displays the speed and alarm/no-alarm condition for each of the T-DAC's three Ethernet ports.

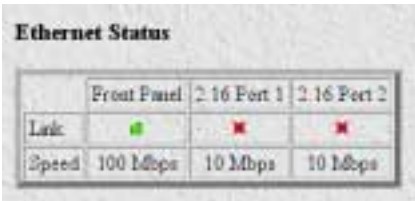


Figure 18. Ethernet status

The three ports are the front panel Ethernet port and the two internal ports (2.16 Port 1 and 2.16 Port 2) which can be routed through the rear blade to the cPCI chassis mid-plane.

- **Link**—A green square (see figure 16 on page 29) denotes that no alarms are present and parameter is functioning properly. A red flashing star indicates that an alarm condition exists.
- **Speed**—Displays *100 Mbps* or *10 Mbps*, depending on how the port is configured

Figure 19. T1/E1 port information

T1/E1 port information table

The T1/E1 port table (see figure 19) displays status information in three categories:

- **Configure**—WAN port numbers are displayed as hyperlinks. Clicking link displays a WAN Circuit Configuration Link window for configuring a WAN port.
- **Circuit ID**—The name defined for the WAN circuit.
- **Status**—Shows the operating status of the WAN circuit.

Note WAN port status color indicators show the state of each T1/E1 WAN port.The status indication symbols (see figure 16 on page 29) are defined as follows.

- Green square—Functioning properly and no alarms are present.
- Flashing red star—A critical (severity 4) alarm has been detected.
- Orange exclamation mark—A major (severity 5) alarm has been detected.
- Yellow triangle—A minor (severity 6) alarm has been detected.
- Blue square—The circuit is undergoing loopback diagnostics.
- Gray circle—Unused; not activated. The port is not configured for operation.

For full details on the WAN circuit parameters, refer to chapter 9, "DSL" on page 75.

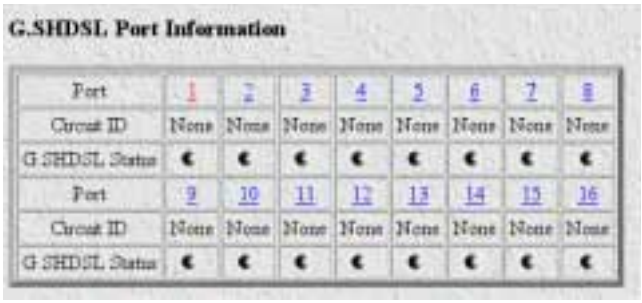


Figure 20. G.SHDSL port information

G.SHDSL port information table

The G.SHDSL port table (see figure 20) displays status information in three categories:

- **Port**—Clicking on the hyperlink for each port displays the G.SHDSL port information window.
- **Circuit ID**—The name of each G.SHDSL modem port.
- **G.SHDSL Status**—The indicator color shows the state of each G.SHDSL port.

Note G.SHDSL port status color indicators show the state of each G.SHDSL port.The status indication symbols (see figure 16 on page 29) are defined as follows.

- Green square—Functioning properly and no alarms are present.
- Flashing red star—A critical (severity 4) alarm has been detected.
- Orange exclamation mark—A major (severity 5) alarm has been detected.
- Yellow triangle—A minor (severity 6) alarm has been detected.
- Blue square—The circuit is undergoing loopback diagnostics.
- Gray circle—Unused; not activated. The port is not configured for operation.

For full details on the G.SHDSL circuit parameter, consult chapter 9, "DSL" on page 75.

Chapter 5 System History

Chapter contents

Introduction

The System History Overview window (see figure 21) provides access to information about the T-DAC's WAN and G.SHDSL port parameters and statistics.

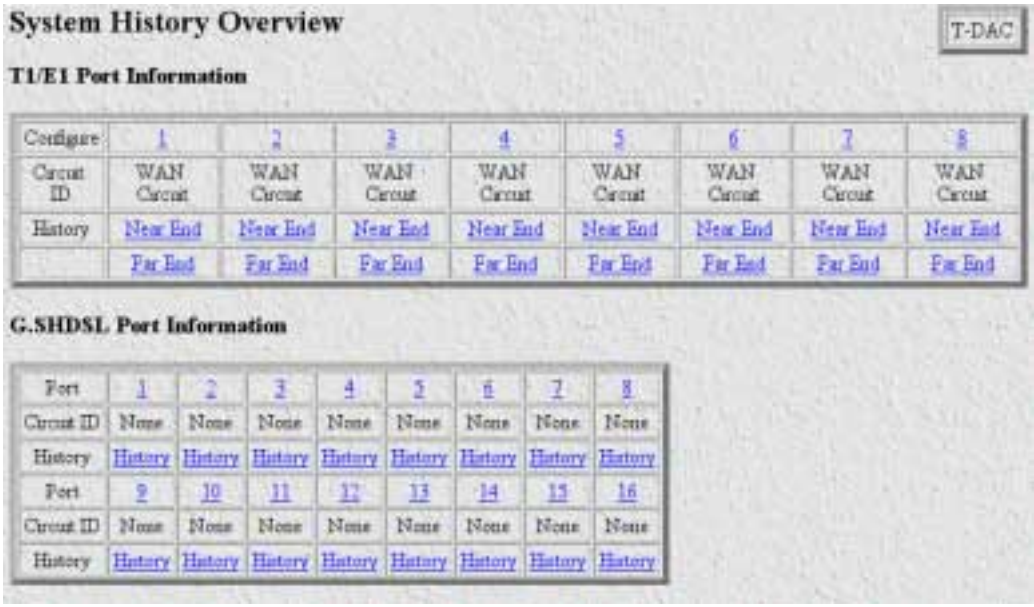


Figure 21. System History Overview window

The System History Overview window functions as a menu or portal to this information via two tables of hyperlinks to related sub-windows, as shown in figure 22.

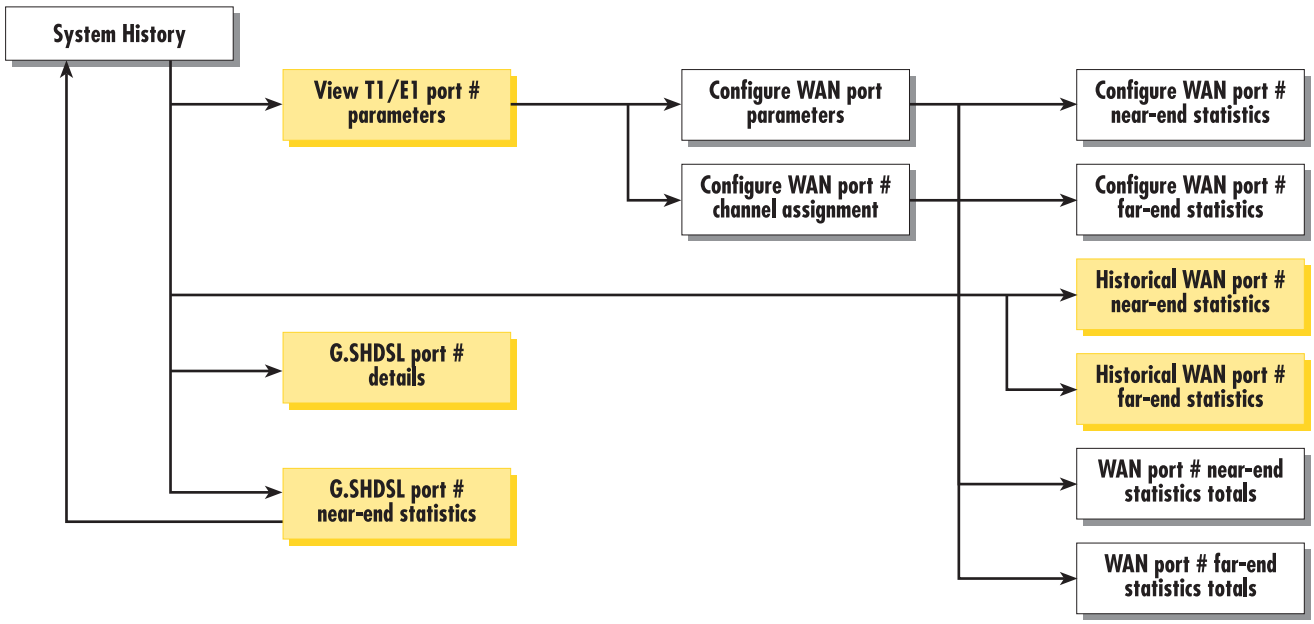


Figure 22. System History diagram

Click the System History hyperlink to display the System History Overview window.

The System History Overview window provides the following tables of hyperlinks:

- **T1/E1 Port Information**—For each T1/E1 port on the T-DAC, this table displays a port number hyperlink to the WAN Circuit Configuration window, the Circuit ID for the connected circuit, and hyperlinks to the statistical history windows for the near and far end of the T1/E1 link.
- **G.SHDSL Port Information**—For each G.SHDSL port on the T-DAC, this table displays a port number hyperlink to the G.SHDSL Port Details window, the Circuit ID for the connected G.SHDSL circuit, and a hyperlink to the History of Near End Performance window.

T1/E1 port information table

The T1/E1 port information table (see figure 21 on page 34) displays the following information:

- **Configure**—For each T-DAC WAN port, clicking port number hyperlink displays the WAN Circuit Configuration Link window where you can configure or view the configuration for the T1/E1 port.
- **Circuit ID**—Displays the configurable free-text name defined for the WAN circuit
- **History**—For each WAN port, these rows display near end and far end hyperlinks to the History of Near End Performance and History of Far End Performance windows. These windows display the performance statistics that the T-DAC has collected for each end of the link

For detailed information on the T1/E1 port parameters, refer to chapter 22, "T1/E1 Link" on page 211.

G.SHDSL port information table

The G.SHDSL table (see figure 21 on page 34) contains the following information:

- **Port**—For each T-DAC G.SHDSL port, clicking on this link displays the G.SHDSL Port Information window where you can configure or view the configuration for the G.SHDSL port.
- **Circuit ID**—Displays the configurable free-text name defined for the G.SHDSL circuit.
- **History**—For each G.SHDSL port, this row displays the history hyperlink to the History of Near End Performance window for the connected circuit.

For more information on the G.SHDSL port parameters, refer to chapter 9, "DSL" on page 75.

(WAN) Circuit ID # History of Near End Performance window

The (WAN) Circuit ID # History of Near End Performance window displays line statistics pertaining to the remote end of the T1/E1 links. The window displays statistics for the preceding 24 hour period in 15-minute intervals (see figure 23). Statistics for the current 15-minute interval are not shown on this window. They are displayed on the Current Near End Performance window.

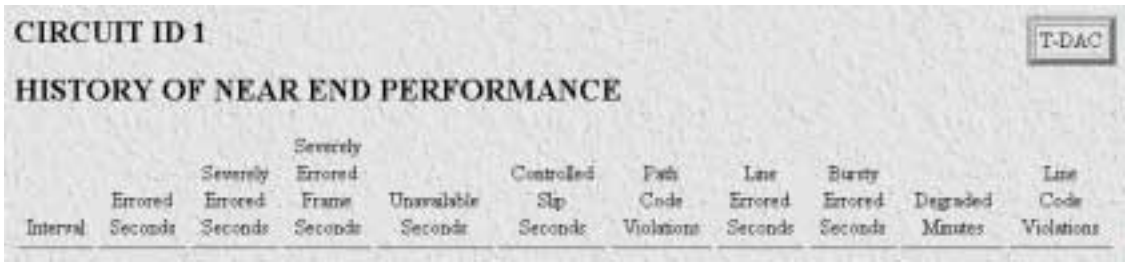


Figure 23. Circuit ID 1—History of Near-End Performance window

The (WAN) Circuit ID # History of Near End Performance window can be reached in three ways:

- From the System History management window
- From the T1/E1 Link Activity window
- From the WAN Circuit Configuration window

To open the (WAN) Circuit ID # History of Near End Performance web management window, for a given WAN port:

1. On the System History window, in the WAN Port Information table (see figure 21 on page 34), click the Near End hyperlink under the desired WAN port number.
2. On the T1/E1 Link Activity window, in the Link table for the desired WAN port number, in the Near End Line Statistics row, click the History hyperlink.
3. On the WAN Circuit Configuration window, in the table at the top of the window, in the Near End Line Statistics row, click the History hyperlink.

Interval (dsx1IntervalNumber)

A number between 1 and 96, where 1 is the most recently completed 15-minute interval and 96 is the oldest of the completed 15-minute intervals. When all 96 intervals are visible, then the 3096RC has been operating (powered-on) for at least 24 hours. If fewer than 96 intervals are displayed, then it has been less than 24 hours since the 3096RC was powered up.

Errored Seconds (dsx1intervaless)

The number of errored seconds encountered by a DS1 interface in one of the previous 96, 15-minute intervals.

Severely Errored Seconds (dsx1IntervalSESs)

The number of severely errored seconds encountered by a DS1 interface in one of the previous 96, 15-minute intervals.

Severely Errored Frame Seconds (dsx1IntervalSEFSs)
The number of severely errored framing seconds encountered by a DS1 interface in one of the previous 96, 15-minute intervals.

Unavailable Seconds (dsx1IntervalUASs)
The number of unavailable seconds encountered by a DS1 interface in one of the previous 96, 15-minute intervals.

Controlled Slip Seconds (dsx1IntervalCSSs)
The number of controlled slip seconds encountered by a DS1 interface in one of the previous 96, 15-minute intervals.

Path Code Violations (dsx1IntervalPCVs)
The number of path coding violations encountered by a DS1 interface in one of the previous 96, 15-minute intervals.

Line Errored Seconds (dsx1IntervalLESs)
The number of line errored seconds encountered by a DS1 interface in one of the previous 96, 15-minute intervals.

Bursty Errored Seconds (dsx1IntervalBESs)
The number of bursty errored seconds (BESs) encountered by a DS1 interface in one of the previous 96, 15-minute intervals.

Degraded Minutes (dsx1IntervalDMs)
The number of degraded minutes (DMs) encountered by a DS1 interface in one of the previous 96, 15-minute intervals.

Line Code Violations (dsx1IntervalLCVs)
The number of line code violations (LCVs) encountered by a DS1 interface during the current 15-minute interval.

(WAN) Circuit ID # History of Far End Performance window

The History of Far-End Performance window (see figure 24) displays line statistics pertaining to the remote end of the T1/E1 link. The page displays statistics for the preceding 24 hour period in 15-minute intervals. Statistics for the current 15-minute interval are not shown on this page. They are displayed on the Current Far End Performance window.

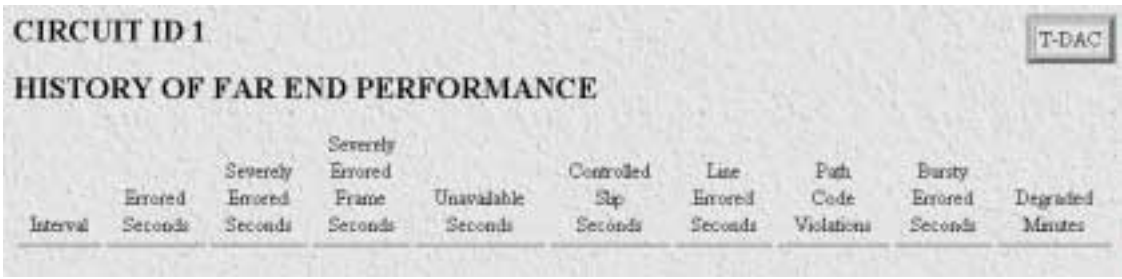


Figure 24. Circuit ID 1—History of Far-End Performance Window

The (WAN) Circuit ID # History of Far End Performance window may be reached in three ways:

- From the System History management window
- From the T1/E1 Link Activity window
- From the WAN Circuit Configuration window

To open the (WAN) Circuit ID # History of Far End Performance management window, for a given WAN port:

1. On the System History window, in the WAN Port Information table, click the Far End hyperlink under the desired WAN port number.
2. On the T1/E1 Link Activity window, in the Link table for the desired WAN port number, in the Far End Line Statistics row, click the History hyperlink.
3. On the WAN Circuit Configuration window, in the table at the top of the window, in the Far End Line Statistics row, click the History hyperlink.

Interval (dsx1FarEndIntervalNumber)

A number between 1 and 96, where 1 is the most recently completed 15-minute interval and 96 is the oldest completed 15-minutes interval (assuming that all 96 intervals are valid).

Errored Seconds (dsx1FarEndIntervalESs)

The number of far-end errored seconds encountered by a DS1 interface in one of the previous 96, 15-minute intervals.

Severely Errored Seconds (dsx1FarEndIntervalSESs)

The number of far-end severely errored seconds encountered by a DS1 interface in one of the previous 96, 15-minute intervals.

Severely Errored Frame Seconds (dsx1FarEndIntervalSEFSs)
The number of far-end severely errored framing seconds encountered by a DS1 interface in one of the previous 96, 15-minute intervals.

Unavailable Seconds (dsx1FarEndIntervalUASs)
The number of far-end unavailable seconds encountered by a DS1 interface in one of the previous 96, 15-minute intervals.

Controlled Slip Seconds (dsx1FarEndIntervalCSSs)
The number of far-end controlled slip seconds encountered by a DS1 interface in one of the previous 96, 15-minute intervals.

Line Errored Seconds (dsx1FarEndIntervalLESs)
The number of far-end line errored seconds encountered by a DS1 interface in one of the previous 96, 15-minute intervals.

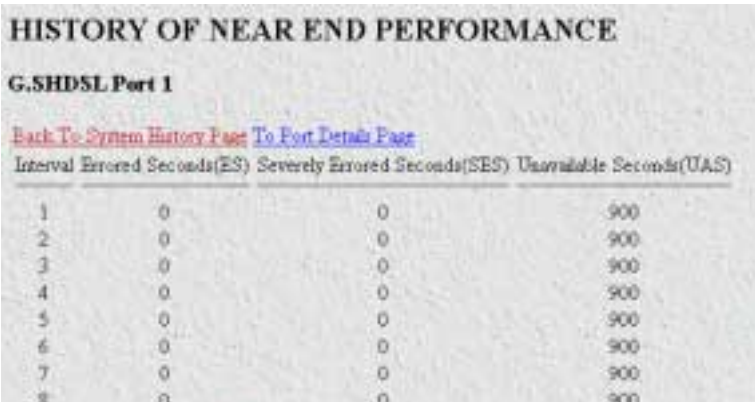
Path Code Violations (dsx1FarEndIntervalPCVs)
The number of far-end path coding violations encountered by a DS1 interface in one of the previous 96, 15-minute intervals.

Bursty Errored Seconds (dsx1FarEndIntervalBESs)
The number of far-end bursty errored seconds (BESs) encountered by a DS1 interface in one of the previous 96, 15-minute intervals.

Degraded Minutes (dsx1FarEndIntervalDMs)
The number of far-end degraded minutes (DMs) encountered by a DS1 interface in one of the previous 96, 15-minute intervals.

History of Near End Performance: G.SHDSL Port window

The History of Near End Performance: G.SHDSL Port window displays line statistics pertaining to the near end of a G.SHDSL link. The page displays statistics for the preceding 24 hour period in 15-minute intervals (see figure 25). The T-DAC cannot display statistics for the current 15-minute interval.


HISTORY OF NEAR END PERFORMANCE

G.SHDSL Port 1

Back To System History Page To Port Details Page

Interval	Errored Seconds(ES)	Severely Errored Seconds(SES)	Unavailable Seconds(UAS)
1	0	0	900
2	0	0	900
3	0	0	900
4	0	0	900
5	0	0	900
6	0	0	900
7	0	0	900

Figure 25. G.SHDSL History of Near End Performance window

The History of Near End Performance: G.SHDSL Port window may be reached in two ways:

- From the System History management window
- From the G.SHDSL Port Details window

To open the (WAN) Circuit ID # History of Near End Performance window, for a given WAN port, do the following:

- On the System History window, in the G.SHDSL History table, click the History hyperlink under the desired G.SHDSL port number.
- On the G.SHDSL Port Details window, click the History Details hyperlink.

The History of Near End Performance: G.SHDSL Port window displays the following information:

- G.SHDSL Port #—Identifies by T-DAC port number the G.SHDSL link for which statistics are shown.
- Back to System History Page hyperlink—Clicking on this link will return you to the System History management page.
- To Port Details Page hyperlink—Clicking on this link will return you to the G.SHDSL Port Details window for the specified G.SHDSL port number.

Interval (gshDSLIntervalNumber)

A number between 1 and 96, where 1 is the most recently completed 15-minute interval and 96 is the oldest completed 15-minute interval (assuming that all 96 intervals are valid).

Errored Seconds (historyESgshDSL)

The number of far-end errored seconds encountered by a G.SHDSL interface in one of the previous 96, 15-minute intervals.

Severely Errored Seconds (historySESgshDSL)

The number of far-end severely errored seconds encountered by a G.SHDSL interface in one of the previous 96, 15-minute intervals.

Unavailable Seconds (historyUASgshDSL)

The number of far-end unavailable seconds encountered by a G.SHDSL interface in one of the previous 96, 15-minute intervals.

Chapter 6 Alarms

Chapter contents

Introduction

The 3096RC provides alarm facilities that monitor the operating status of the T-DAC's power supply, G.SHDSL access ports, WAN ports, and ambient temperature. The T-DAC provides three alarm signaling methods to indicate that an alarm condition has been detected:

- Visual indication—via the T-DAC front panel ALARM status LED and rear blade ALARM status LED indicators
- Operator console indication—via the T-DAC management windows
- External alarms management host indication—delivered via SNMP traps or Syslog messages that the T-DAC can send to an external alarms management host

By default, all T-DAC alarms are set to display as major (orange) events, but you can use the Alarm Systems management windows to customize them, assigning a higher or lower level of severity to each item as desired. Your choices are *critical* (red), *major* (orange), *minor* (yellow), *informational* (blue), or *ignore* (no color).

Alarm System Overview window

The Alarm System Overview window (see figure 26) and related windows enable you to manage the 3096RC T-DAC's alarm system. Click on the Alarms hyperlink in the T-DAC's Configuration Menu to display the Alarm System Overview window.

Note From the Alarm System Overview window the system administrator can force the T-DAC to generate alarms for testing purposes as well as clear selected alarms.

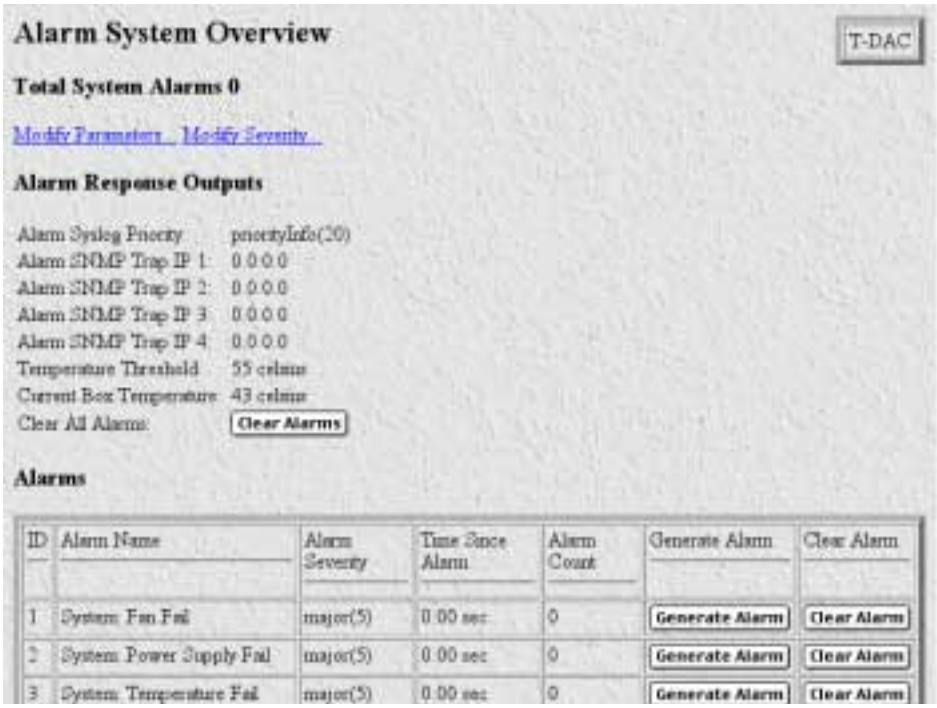


Figure 26. Alarm System Overview window

The G.SHDSL T-DAC uses three methods to indicate an alarm condition:

- Front panel LED and rear blade indications—The front panel ALARM LED and rear blade ALARM LED uses the following three states to indicate the presence and severity of an alarm:
  - **Off**—No alarm is active
  - **Solid**—Minor alarm
  - **Flashing**—Major alarm

Note The T-DAC's factory-default configuration is to consider all alarms to be major (orange) ones, so unless you customize the alarms severity levels (see section "Alarm Severity Configuration" on page 47), any alarm that occurs will cause the ALARM LED to flash, indicating a major alarm—the LED will never indicate a minor alarm.

Note If both power supplies are functioning normally, the POWER LED will display a solid light, but if one or more power supplies fail, the POWER LED will flash.

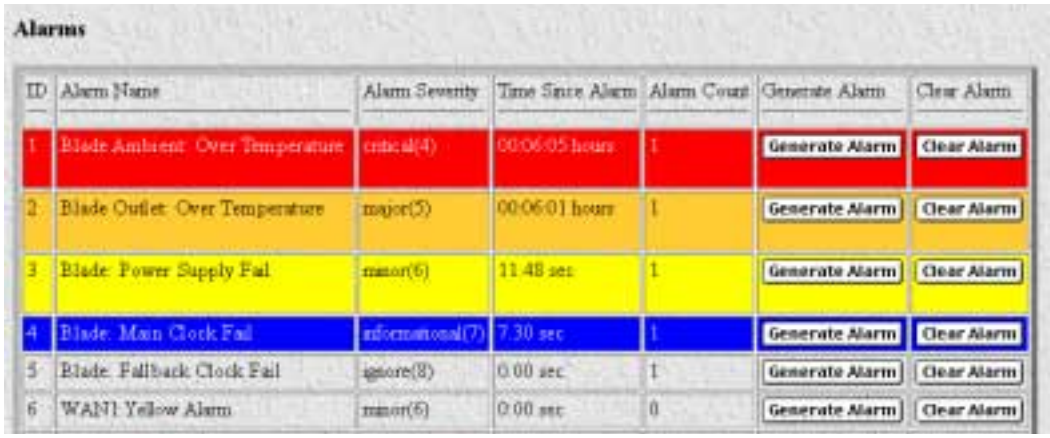


Figure 27. Sample alarm indications

- Management web page indication—The Alarms section (see figure 27) of the Alarm System Overview window (see figure 26 on page 42) uses color-coded highlighting to indicate which alarms are active and the severity levels of active alarms.
  - **RED**: indicates that one or more **CRITICAL** (severity 4) alarms are active. When active, *critical* alarm notifications also appear as red highlighting on the Home window (see figure 3 on page 16) and as a flashing red star (see figure 16 on page 29) on the System Status window (see figure 11 on page 26).
  - **ORANGE**: indicates that one or more **MAJOR** (severity 5) alarms are active. When active, *major* alarm notifications also appear as orange highlighting on the Home window (see figure 3 on page 16) and as an orange exclamation mark (see figure 16 on page 29) on the System Status window (see figure 11 on page 26).

- **YELLOW**: indicates that one or more **MINOR** (severity 6) alarms are active. When active, *minor* alarm notifications also appear as yellow highlighting on the Home window (see figure 3 on page 16) and as a yellow triangle (see figure 16 on page 29) on the System Status window (see figure 11 on page 26).
- **BLUE**: indicates that one or more **INFORMATIONAL** (severity 7) alarms are active. Being informational in nature, these alarms only appear on the Alarm System main window to indicate that an event has occurred, they do not generate alarm indications anywhere else.

- External host indication—For external notification, the T-DAC can be configured to send a Syslog event notification or an SNMP trap message (or both) to an external alarms management host. To configure the T-DAC to send SNMP traps or Syslog messages in response to alarm conditions, click on the Modify Parameters hyperlink (see figure 27 on page 43) to open the Alarm System Configurations—Alarm Response Outputs window (refer to section "Alarm System Configurations window" on page 45).

In addition to viewing current alarm status, you can force the T-DAC to generate an alarm as a test by clicking on the **Generate Alarm** button for the desired alarm. Click on the **Clear Alarm** button to clear the alarm when the test is concluded.

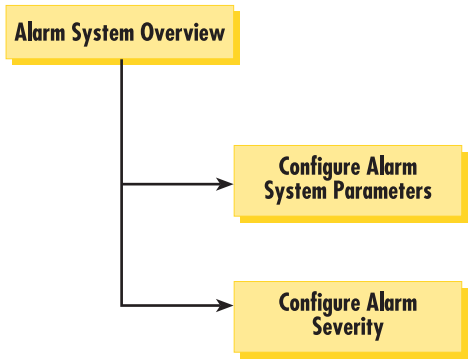


Figure 28. Alarms management diagram

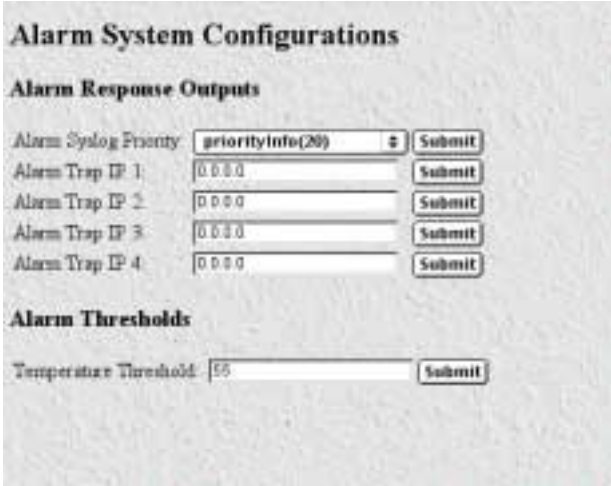


Figure 29. Alarm System Configurations window

Alarms management windows

As shown in figure 26 on page 42, the Alarms System Overview window provides links to the following alarm system management windows:

- Modify Parameters—links to the Alarm System Configurations window (see figure 29) for configuring the alarm response system with the IP addresses of one or more administrators who should be notified in case of an alarm (refer to section "Alarm System Configurations window")
- Modify Severity—links to the Alarm Severity Configuration window (see figure 30 on page 47) where you can configure the severity (importance) of each alarm. For each alarm, you can defined the value of Alarm Severity as *critical*, *major*, *minor*, *informational*, or *ignore*. Defining an alarm's severity as *ignore* disables that alarm. (refer to section "Alarm Severity Configuration" on page 47)

Alarm System Configurations window

When an alarm condition occurs, by default the T-DAC does the following to notify administrators of the alarm:

- Activates the front and rear panel Alarm LEDs
- Activates the alarm indications on the T-DAC web management windows (as color-coded highlighting on the Home window and as a color-coded symbol on the System Status window).

If it has been configured to do so, the T-DAC can also send Syslog and SNMP trap messages to an external alarm management host. This section describes how to configure the Syslog and/or SNMP trap alarm response outputs.

Click on Modify Parameters (see figure 26 on page 42) to open the Alarm System Configurations window (see figure 29). Choose the alarm response output that you wish to configure. After defining the value for a desired alarm response output parameter, click the **Submit Query** button to the right of the parameter you just modified.

Note You must click **Submit Query** for each parameter you modify in order to save your changes. Each submit query button on this page only affects the single parameter on the same line. Clicking a **Submit Query** button will not save changes made to parameter values on other lines.

The following sections describe the Alarm Response Output parameters.

Alarm Syslog Priority (syslogAlarmPriority)

Syslog is a protocol that enables the T-DAC to send event notification messages across IP networks to event message collectors (also known as *Syslog Servers* or *Syslog Daemons*). The Alarm Syslog Priority parameter defines what priority level an event must be at before the T-DAC sends a message to the Syslog daemon. The levels are:

- priorityDisable(1000)
- prioritySystem(80)
- priorityService(60)
- priorityOddity(40)
- priorityInfo(20)
- priorityDebug(10)
- priorityVerbose(5)

> **Note** Unless instructed to do otherwise by Patton Technical Support, you should leave the Alarm Syslog priority set for *prioritySystem(80)* (which will only generate a Syslog message for incidents greater than the System priority level) or *priorityDisable(1000)* (which deactivates Syslog message sending).

For more information on Syslog messages, refer to chapter "System Log" on page 199.

Alarm Trap IP 1 through 4 (alarmTrapIp0–alarmTrapIp3)

Simple Network Management Protocol (SNMP) trap daemons are a tool for managing TCP/IP networks, they are a simple method of alerting a management host of a problem with a device or application. The Alarm Trap IP parameter is the IP address of a host running the SNMP trap daemon that will be receiving messages sent from the T-DAC. Upon the occurrence of an alarm, the T-DAC sends an SNMP trap message to the host system (or a management station) defined by this parameter.

> **Note** The Alarm Trap IP requires that an IP address be entered. If you ***do not*** want the T-DAC to send SNMP trap messages, entering an address of *0.0.0.0* disables SNMP trap message sending.

Temperature Threshold (boxAlarmTemperature)

An alarm message is generated when the internal box temperature exceeds this value in degrees Celsius. You can change the threshold temperature, but we recommend using the factory default of 55° C.

Alarm Severity Configuration

This section describes configuring alarm severity levels. Clicking on Modify Severity (see figure 26 on page 42) displays the Alarm Severity Configuration window (see figure 30) listing of T-DAC alarms. From this window you can assign the severity for each alarm (*critical*, *major*, *minor*, *informational*, or *ignore*).

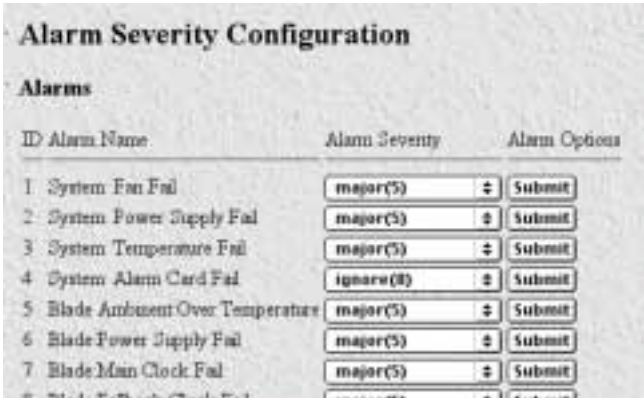


Figure 30. Alarm Severity Configuration window

The alarms can be independently configured to generate alarm messages. Each alarm item can be set for one of the following severity levels:

- **critical**(4)—When active, *critical* alarm notifications appear as red highlighting on the Home window (see figure 3 on page 16) and as a flashing red star (see figure 16 on page 29) on the System Status window (see figure 11 on page 26).
- **major**(5)—When active, *major* alarm notifications appear as orange highlighting on the Home window (see figure 3 on page 16) and as an orange exclamation mark (see figure 16 on page 29) on the System Status window (see figure 11 on page 26).
- **minor**(6)—When active, *minor* alarm notifications appear as yellow highlighting on the Home window (see figure 3 on page 16) and as a yellow triangle (see figure 16 on page 29) on the System Status window (see figure 11 on page 26).
- **informational**(7)—Being informational in nature, these alarms only appear as blue highlighting on the Alarm System main window to indicate that an event has occurred, they do not generate alarm indications anywhere else.
- **ignore**(0)—The T-DAC will not generate an alarm.

Note You can disable an alarm (as appropriate for your application) by defining its severity as *ignore*.

Note The T-DAC's factory-default configuration is to consider all alarms to be major (orange) ones, unless you customize the alarm's severity levels.

To configure the severity for a selected alarm, click on the drop-down menu for the that alarm, select the desired severity value, then click on **Submit Query** to implement the change.

Chapter 7 DS0 Mapping

Chapter contents

Introduction

To route traffic from one device connected to the T-DAC to another device (also connected to the T-DAC) you must define a *DS0 mapping* (also called an *internal connection* or *cross-connection*). An internal cross-connection carries traffic between the two external devices via the T-DAC. The external devices can be (but are not limited to) a T1/E1 NTU, a G.SHDSL customer premise equipment (CPE) modem, or another blade in the same CPCI chassis in which the T-DAC is installed.

The T-DAC's DS0 Mapping Overview window (see figure 31) provides the means for managing (mapping) internal connections.

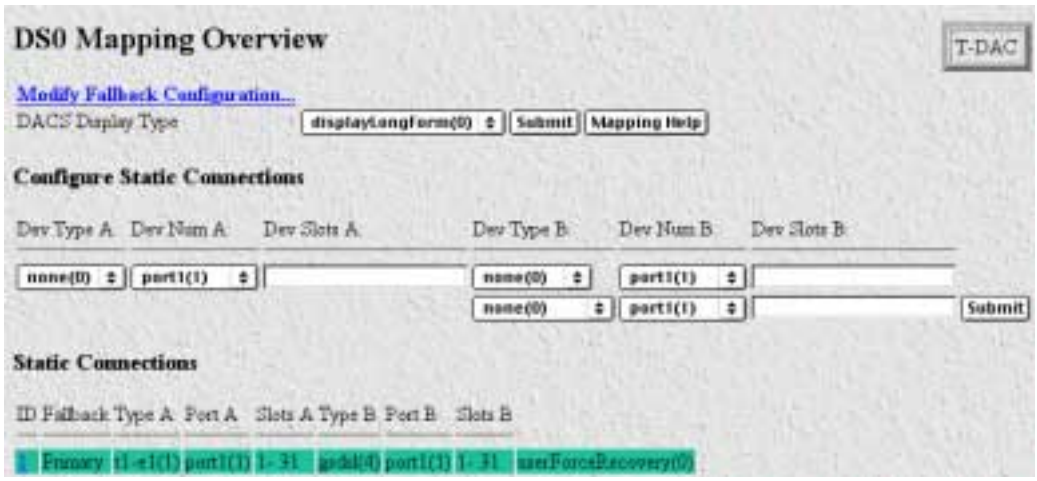


Figure 31. DS0 Mapping Overview window

External devices can connect to the T-DAC via a T1/E1 WAN port, a G.SHDSL port, or an H.110 port. (A device will connect to an H.110 port via the T-DAC's interface to the H.110 bus in the cPCI chassis mid-plane). Each DS0 mapping defines a one-to-one connection between a selected number of timeslots on one port and a corresponding number of timeslots on a different port. You can use the DS0 Mapping management web page to define these DS0 mappings (internal connections) and to view previously defined mappings.

The following types of internal connections can be defined:

- Between a G.SHDSL port and a T1/E1 WAN port
- Between a G.SHDSL port and another G.SHDSL port
- Between a G.SHDSL port and an H.110 bus port
- Between a T1/E1 WAN port and another T1/E1 WAN port
- Between a T1/E1 WAN port and the H.110 bus port

DS0 Mapping Overview main window

The DS0 Mapping Configuration window and related windows provide the means for you to manage the 3096RC T-DAC's DS0 mapping subsystem. To display the DS0 Mapping Configuration window (see figure 31), on the T-DAC Configuration Menu, click the DS0 Mapping link.

The DS0 Mapping window provides links to the DS0 Connection, DS0 Fallback, and DS0 Fallback ID windows as shown in the diagram below. These windows are described later in this chapter.

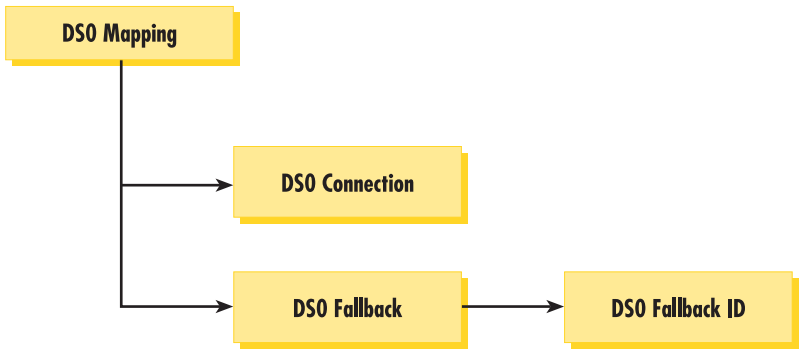


Figure 32. DS0 Mapping diagram

Clicking on the Modify Fallback Configuration link (see figure 31 on page 51) opens the DS0 Fallback Configuration window (see figure 33 on page 53), where you can define mappings between primary and fallback channels and view the T-DAC's table of previously defined fallback mappings.

The DS0 mapping window contains the following:

- Modify Fallback Configuration link that takes you to the DS0 Mapping subsystem where you can configure a fallback mechanism by which the T-DAC can switch the traffic from a failed primary channel to a back-up or *fallback* channel (see section "DS0 Fallback Configuration window" on page 52)
- DACS Display Type menu you can use to select the *Long Form* or the *Command Line Form* methods for configuring the cross-connection mapping (see section "DACS Display Type parameter")
- **Mapping Help** button that displays the online help window (see section "Mapping Help" on page 58)
- Configure Static Connections section where you can create the cross-connections (see section "Configuring static connections using the long form" on page 58 or section "Defining DS0 mappings using the command line interface (CLI)" on page 61)
- Static Connection section where you can view the previously defined DS0 mappings (cross-connections) in the T-DAC (see section "Defined Mappings Table (Static Connections)" on page 63)

DS0 Fallback Configuration window

The DS0 Mapping subsystem provides a fallback mechanism by which the T-DAC can switch traffic from a failed primary channel (*channel* is defined as a group of time slots on a given port) to a previously defined fallback channel. Once you have defined a fallback mapping, the T-DAC will monitor the primary channel for failure and, should the primary channel fail, the fallback channel will switch in (take over the traffic) for the primary channel. Once it has switched in, the fallback channel will carry all traffic the primary channel previously carried.

Clicking on the DACS Fallback System link (see figure 31 on page 51) opens the DS0 Fallback Configuration window (see figure 33), where you can define mappings between primary and fallback channels and view the T-DAC's table of previously defined fallback mappings.

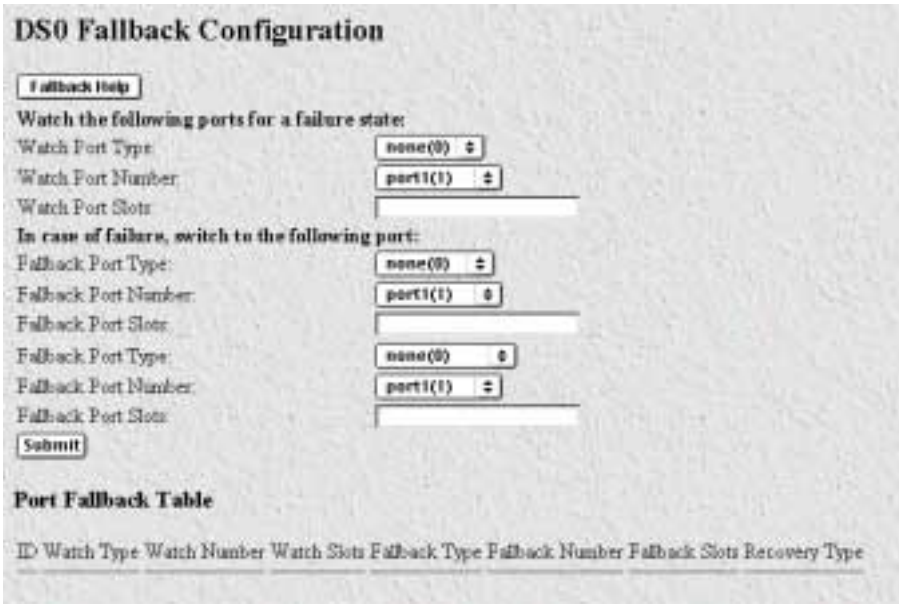


Figure 33. DACS Fallback Configuration window

Fallback Help Button

When you click the Fallback Help button, the T-DAC will display the Fallback Mapping Information page in a a new pop-up window (see figure 34). The Fallback Mapping Information page provides a procedural outline and a summarized description of the parameters for defining a fallback mapping.

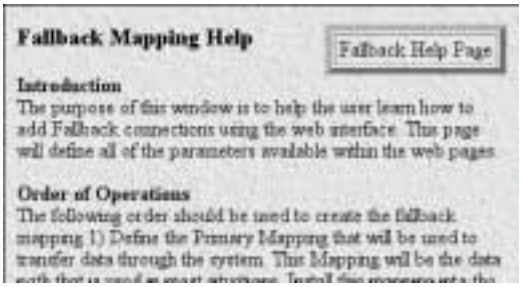


Figure 34. Fallback Mapping help window

Watch Port parameters

Watch Port parameters define the primary channel in a fallback mapping.

Watch Port Type [daxWatchTypegshDSL]

The port type for the primary channel port. Select one of the following values from the drop-down menu.

- none(0)

- t1-e1(1)
- gshDSL(4)

Watch Port Number [daxWatchPortgshDSL]

The Watch Port Number will correspond to one of the T-DAC's 16 G.SHDSL ports, or one of the 4, 8, 12, or 16 T1/E1 WAN ports. Within each port type, port numbers begin with 1 and end with the total number of ports of that type (e.g. 16 for G.SHDSL). As an example, to define a primary channel using the T-DAC third WAN port, you would select "Port 3" as the value for Watch Port Number.

Watch Port Slots [daxWatchSlot]

The Watch Port Slots parameters define which time slots will comprise the primary channel for the fallback mapping. Each time slot provides a 64 kbps data communications channel. Such a 64 kbps channel is also known as a DS0. The following time slots are available"

- G.SHDSL modem port: 72 time slots (DS0s), numbered 1 through 72 (72 64-kbps slots are needed to create a 4.6-Mbps link)
- T1 WAN port: 24 time slots (DS0s), numbered 1 through 24
- E1 WAN port: 31 time slots (DS0s), numbered 1 through 31
- H.110 streams can support up to 128 slots.

> **Note** You must define the same number of time slots for the primary and fallback channels. In other words, the number of time slots defined for Watch Port Slots must equal the number of time slots defined for Fallback Port Slots.

To define value for the time slots parameter, you will enter a text string specifying which time slot numbers will be used for the channel. You must enter the text string using a prescribed notation comprised of the following elements:

- **Numerals**—Use numerals (0, 1, 2, 3, 4, 5, 6, 7, 8, 9) to represent time slot numbers
- **Comma**—Use the comma (,) to separate non-contiguous timeslots. For example, the string 1,7,15 represents three timeslots numbered 1, 7 and 15.

> **Note** You may also use the comma to separate contiguous timeslots. However, since it is inefficient and may be confusing, doing so is not recommended.

- **Dash**—Use the dash (-) to represent a series of contiguous timeslots. For example, the string 1-31 represents all timeslots between 1 and 31 inclusive (i.e. time slot 1, time slot 31 and all time slots in between).

Slot Numbering Examples. For example, to define a channel comprising timeslots 1, 2, 5, 6, 7, and 15, either of the following entries would be valid.

- 1,2,5-7,15
- 1-2,5-7,15

Although the first string above is valid syntax, the second string is easier to read, and more clearly shows what is going on.

Fallback port parameters

Fallback port parameters define the alternate (backup) channel in a fallback mapping. Two sets of parameters appear on the page, three parameters for each of two fallback ports. When the fallback channel comprises a WAN or G.SHDSL port (i.e. ***not*** an H.110 connection), you must define the first fallback port only, (i.e. the first three parameters). When the fallback channel comprises an H.110 connection, you must define both fallback ports (i.e. all six parameters). The first port defines the transmit connection *to* the H.100 bus from the T-DAC, and the second port defines the receive connection *from* the H.110 bus to the T-DAC. The following parameters define the fallback channel:

Fallback Port Type [daxFallbackTypegshDSL]

This parameter defines the port type for the fallback channel. Select one of the following values from the drop-down menu:

- none(0)
- t1-e1(1)
- gshDSL(4)
- toH110(5)

> **Note** Selecting this value defines only the fallback transmit channel to the H.110 bus. You must also define the fallback receive channel from the H.110 bus by selecting fromH110(6) as the value of the second Fallback Port Type parameter.

Fallback Port Number [daxFallbackPortGsDS]

The Fallback Port Number will correspond to one of the T-DAC's 16 G.SHDSL ports, one of the 4, 8, 12, or 16 T1/E1 WAN ports, or one of the 32 H.110 ports. Within each port type, port numbers begin with 1 and end with the total number of ports of that type (e.g. 16 for G.SHDSL, 32 for H.110). As an example, to define a fallback transmit channel using the T-DAC third H.110 port, you would select "Port 3(3)" as the value for Fallback Port Number.

Fallback Port Slots [daxFallbackSlot]

The Fallback Port Slots parameters define which time slots will comprise the alternate (fallback) channel for the fallback mapping. Use the same notation as for Watch Port Slots, as described in the above section entitled, Watch Port Slots.

Fallback Port Type fromH110(0) [daxFallbackTypegshDSLH110]

This parameter defines the port type for fallback receive channel from the H.110 bus to the T-DAC. Select one of the following values from the drop-down menu.

- none(0)
- gshDSL(4)
- toH110(5)

Note Selecting this value defines only the receive channel from the H.110 bus. In order to define an H.110 fallback channel, you must first define the transmit channel to the H.100 bus by selecting toH110(5) as the value of the first Fallback Port Type parameter.

Fallback Port Number [daxFallbackPortgshDSLH11]
The Fallback Port Number will correspond to one of the T-DAC's 32 H.110 ports. For example to define a fallback receive channel using the T-DAC's fourth H.110 port, you would select "port 3(3)" as the value of Fallback Port Number.

Fallback Port Slots [daxFallbackSlotH110]
This parameter defines which time slots will comprise the fallback receive channel from the H.110 bus to the T-DAC for the fallback mapping. Use the same notation as for Watch Port Slots, as described in the above section entitled, Watch Port Slots.

Port Fallback Table

The Port Fallback Table (see figure on page 52) displays a list of all existing Fallback Mappings which a T-DAC operator has previously defined. Each row in the table displays a single fallback mapping, identified by an ID number.

Fallback Mapping ID
Clicking the fallback mapping ID hyperlink displays the DAX Fallback ID window, which you can use to delete the specified fallback mapping or change the value of the fallback Recovery Type parameter (see "DS0 Fallback ID (DAX Fallback ID) window")

The parameters comprising each fallback mapping are described in the paragraphs above, with one the exception—Recovery Type, which is described below.

Recovery Type [daxFallbackRecovery]
The Recovery Type parameter defines how the T-DAC will behave when the primary channel in a fallback mapping recovers (returns to normal operation) once the fallback channel has switched in. The default value is userForcedRecovery(0). You can change the value of Recovery Type on the DAX Fallback ID window.

DS0 Fallback ID (DAX Fallback ID) window

For the selected fallback mapping the DS0 Fallback ID window provides the capability to:

- Delete an existing DS0 fallback mapping (backup connection)
- Change the value of the fallback Recovery Type parameter.

The page also displays all parameters which define the selected fallback mapping.

Viewing the DS0 Fallback ID window

To view the DS0 Fallback ID window for a specific DS0 Fallback Mapping (backup connection):

1. On the DSO Fallback page, under Port Fallback Table, find the Connection ID number for the fallback mapping you wish to view.

2. Click the Connection ID number hyperlink to display the DS0 Fallback ID window for the selected connection ID.

Deleting a Fallback Mapping

To delete the Fallback Mapping displayed on the DS0 Fallback ID window:

1. In the drop-down menu for the Connection Status parameter, ensure that the value delete(1) is selected.
2. Click the **Submit Query** button to delete the connection (DS0 mapping).

Recovery Type [daxFallbackRecovery]

The Recovery Type parameter defines how the T-DAC will behave when the primary channel in a fallback mapping recovers (returns to normal operation) once the fallback channel has switched in. There are two options for the value of Recovery Type.

- **userForceRecovery(0)**—Default. When the primary channel port recovers and all failures are cleared, the T-DAC will continue to route traffic over the fallback channel until the T-DAC operator intervenes.

  To force traffic back to the primary channel:

  1. On the DS0 Mapping page, in the Static Connections table, find the connection for which you wish to force recovery.
  2. On the right-most side of the row, click the [Force Recovery] button

- **autoRecovery(1)**—When the primary channel port recovers and all failures are cleared, the T-DAC will automatically switch back to the primary channel defined for the connection and resume routing all traffic for the connection over the primary channel.

Force Recovery Button

When a fallback channel switches in for a primary channel, the T-DAC will display a force recovery button to the far right of the table, next to the entry for the failed connection. However, the button will only appear if the fallback connection is defined in Force Recovery mode. If the fallback connection is defined in Auto Recovery mode, the button will not appear.

DACS Display Type parameter

To define DS0 mappings (connections), you can use either the *Long Form* or the *Command Line Form*. To choose the method you prefer, use the DACS Display Type drop-down box to select one of the following parameter values:

- **displayLongForm(0)**—(Factory Default). Most people consider *Long Form* the easier method for defining DS0 mappings.The Long Form displays the DS0 Mapping page in the standard management window format with drop-down boxes and text box fields. Use this format to define the DS0 Mapping parameters by selecting values from drop-down boxes and typing values in the text box fields. (Refer to section "Configuring static connections using the long form" on page 58 for information on using the Long Form to configure static connections.)
- **displayCliForm(1)**—Advanced users of the *command line interface* (CLI) method may consider CLI a faster and more convenient method than the Long Form. To use CLI to define DS0 mappings, select displayCliForm(1) and click on the **Submit Query** button. The DS0 Mapping page will refresh, displaying a single text box (in place of the drop-down boxes and text box parameter fields) into which you may enter

CLI commands. (Refer to section "Defining DS0 mappings using the command line interface (CLI)" on page 61 for information on using the CLI to configure static connections.)

Mapping Help

Clicking on the **Mapping Help** button displays the *DS0 Mapping Help* window (see figure 32). The *DS0 Mapping Help* page provides a convenient online tutorial on how to use the T-DAC's web management pages to define DS0 mappings (cross-connections). The tutorial includes definitions for all configurable parameters on the *DS0 Mapping* web page. If you are using command line format to define DS0 connections, scroll down to the *Command Line Format* heading.

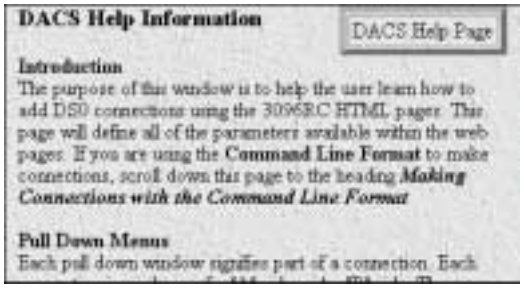


Figure 35. DACS Help Information window

Configuring static connections using the long form

To create a DS0 mapping (cross-connection) between external devices, you must define channels *A* and *B*.

External devices may include (but are not limited to) an NTU, a G.SHDSL CPE, or another blade installed in the same CPCI chassis as the T-DAC.

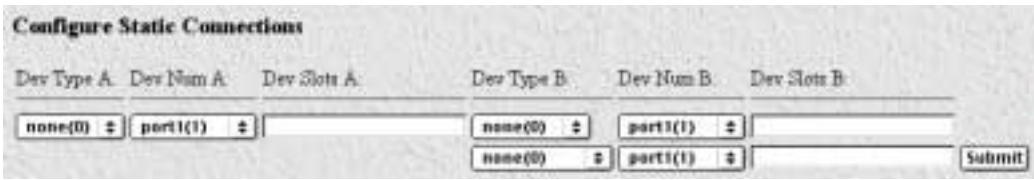


Figure 36. Configure Static Connections section of DS0 Mapping Configuration window

The drop-down menus in the Configure Static Connections section of the DS0 Mapping Configuration window (see figure 36) are organized into *A* and *B* channels. These channel names have been arbitrarily chosen and, as all data will be bi-directional, do not signify the direction that data will travel. In *displayLongForm*

mode, you will use drop-down menus and text boxes to define the DS0 mapping parameters. The following parameters define each channel the mapped connection (see figure 36).

- Device type *(Dev Type)*
- Device number *(Dev Num)* (see page 60)
- Device slots *(Dev Slots)* (see page 60)

Device Type A (daxDeviceTypeTogshDSL)

The Dev Type A menu defines the type of interface port the T-DAC will use for the *A* channel of this connection. The user has the option of selecting a T1/E1 device or a G.SHDSL device

Note Both channels of the connection can be T1/E1 or both sides can be G.SHDSL or just the B channel could be configured (in the event you needed to create an H.110 loopback).

The options are:

- none(0)
- t1-e1(1)—T1/E1 WAN ports for connection to a T1/E1 WAN line
- gshDSL(4)—G.SHDSL ports for connection to a G.SHDSL modem

Device Type B (daxDeviceTypeFromgshDSL) (daxDeviceTypeRxgshDSL)

The Dev Type B menu defines the type of interface port the T-DAC will use for the *B* channel of this connection. The user has the option of selecting a T1/E1 device, a G.SHDSL device, or the H.110 midplane (the H.110 selection can only be done from the B channel selection because it requires a *To* and *From* direction identifier.

Note On the DS0 Mapping window, under Device B, there are two rows of parameter fields for defining H.110 connections. When defining a WAN or G.SHDSL connection, ***do not*** define the parameters in the second row (i.e. leave the menu set to *none(0)*). When defining an H.110 connection, you must define values for all parameters in both rows.

Each connection to the H.110 bus consists of a pair of logical ports. The T-DAC transmits data to the H.110 bus using one logical port, and receives data from the H.110 bus on a different logical port. Under Device B, the DS0 Mapping page provides two rows of parameter fields for defining H.110 connections. When defining an H.110 connection, you must define values for all parameters in both rows. The parameters in the first row under Device B define the transmit port (to the H.110 bus) and parameters in the second row under Device B define the receive port (from the H.110 bus).

In the first row, the following options are available for Dev Type B:

- **none(0)**
- **t1-e1(1)**—T1/E1 WAN ports for connection to a T1/E1 WAN line
- **gshDSL(4)**—G.SHDSL ports for connection to a G.SHDSL modem
- **toH110(5)**—H.110 port for transmitting data to the H.110 bus via the CPCI chassis backplane.

In the second row, the following options are available for Dev Type B:

- **none(0)**
- **fromH110(6)**—H.110 port for receiving data from the H.110 bus via the CPCI chassis backplane.

Device Number A (daxDeviceNumberTogshDSL) and Device Number B (daxDeviceNumberFromgshDSL) (daxDeviceNumberRxgshDSL)

The parameters labeled Dev Num A and Dev Num B define the ports the T-DAC will use for channel A and channel B. The Device Number will correspond to one of the T-DAC's 16 G.SHDSL ports; 4, 8, 12, or 16 T1/E1 WAN ports; or 32 H.110 ports. Within each port type, port numbers begin with 1 and end with the total number of ports of that type (e.g. 16 for G.SHDSL and 32 for H.110). For example, to define a connection for channel A using the T-DAC's third G.SHDSL modem port, you would select *Port 3* as the value for Device Number A.

Device Slots A and B (daxDeviceSlotTo) (daxDeviceSlotFrom)

The Device Slots A and Device Slots B parameters define which 64-kbps time slots (also referred to as the *DS0 data communications channels*) will be used for channel A and channel B. The following time slots are available:

> **Note** There are a maximum of 32 ports available for the H.110 bus, but there could be as few as 4 ports available for the T1/E1 ports. If the port number selected is not within the range supported an error will be generated.

- G.SHDSL modem port: 72 time slots (DS0s), numbered 1 through 72 (72 64-kbps slots are needed to create a 4.6-Mbps link)
- T1 WAN port: 24 time slots (DS0s), numbered 1 through 24
- E1 WAN port: 31 time slots (DS0s), numbered 1 through 31
- H.110 streams can support up to 128 slots.

> **Note** You must define the same number of time slots for each side of the connection. In other words, the number of time slots defined for Slots A must be the same as the number of time slots defined for Slots B.

To configure the time slots parameter, enter a text string specifying which time slot numbers will be used for the channel. You must enter a text string that comprises the following elements:

- Numerals—Use numerals (0, 1, 2, 3, 4, 5, 6, 7, 8, 9) to represent time slot numbers
- Comma—Use the comma (,) to separate non-contiguous timeslots. For example, the string 1,7,15 represents three timeslots numbered 1, 7 and 15.

> **Note** You can also use the comma to separate contiguous time slots. However, since it is inefficient and may be confusing, doing so is not recommended.

- Dash (-)—Use the dash (-) to represent a series of contiguous timeslots. For example, the string 1-31 represents all timeslots between 1 and 31 inclusive (that is, time slot 1, time slot 31 and all time slots in between).

Slot Numbering Examples

For example, to define a channel comprising timeslots 1, 2, 5, 6, 7, and 15, either of the following entries would be valid:

- 1,2,5,6,7,15
- 1,2,5-7,15

Although the first string above is valid syntax, the second string is easier to read, and more clearly shows what is going on. The following strings are also valid syntax:

- 1-2,5,6,7,15
- 1-2,5,6-7,15
- 1-2,5-6,7,15

While the entries above would work, they are harder to grasp quickly than the first two examples. Beyond the cluttered appearance of these last three strings, they tend to obscure the part of reality they represent: the contiguous block of timeslots from 5-7.

After entering the parameters required to define the DS0 mapping, go to section "Saving a DS0 mapping definition" on page 63 for information on saving your cross-connection map to the T-DAC's random access memory (RAM) in order to activate the connection.

Defining DS0 mappings using the command line interface (CLI)

To define a new connection using CLI, you must enter text strings in the following format:

DeviceA:PortA:SlotsA/DeviceB:PortB:SlotsB

DeviceA and *DeviceB* define the type of interface the T-DAC will use for each channel of the connection. The following options are available:

- 1) t1-e1
- 2) gshDSL
- 3) toH110
- 4) from H110

PortA and *PortB* define which one of its 16 G.SHDSL ports; 4, 8, 12, or 16 WAN ports; or 32 H.110 ports the T-DAC will use for each channel of the connection. The value must be a number from 1 to 16 inclusive.

The Device Slots A and Device Slots B parameters define which 64-kbps time slots (also referred to as the *DS0 data communications channels*) will be used for channel A and channel B. The following time slots are available:

Note There are a maximum of 32 ports available for the H.110 bus, but there could be as few as 4 ports available for the T1/E1 ports. If the port number selected is not within the range supported an error will be generated.

- G.SHDSL modem port: 72 time slots (DS0s), numbered 1 through 72 (72 64-kbps slots are needed to create a 4.6-Mbps link)
- T1 WAN port: 24 time slots (DS0s), numbered 1 through 24
- E1 WAN port: 31 time slots (DS0s), numbered 1 through 31
- H.110 streams can support up to 128 slots.

> **Note** You must define the same number of time slots for each side of the connection. In other words, the number of time slots defined for Slots A must be the same as the number of time slots defined for Slots B.

To configure the time slots parameter, enter a text string specifying which time slot numbers will be used for the channel. You must enter a text string that comprises the following elements:

- Numerals—Use numerals (0, 1, 2, 3, 4, 5, 6, 7, 8, 9) to represent time slot numbers
- Comma—Use the comma (,) to separate non-contiguous timeslots. For example, the string 1,7,15 represents three timeslots numbered 1, 7 and 15.

> **Note** You can also use the comma to separate contiguous time slots. However, since it is inefficient and may be confusing, doing so is not recommended.

- Dash (-)—Use the dash (-) to represent a series of contiguous timeslots. For example, the string 1-31 represents all timeslots between 1 and 31 inclusive (that is, time slot 1, time slot 31 and all time slots in between).

Slot Numbering Examples

For example, to define a channel comprising timeslots 1, 2, 5, 6, 7, and 15, either of the following entries would be valid:

- 1,2,5,6,7,15
- 1,2,5-7,15

Although the first string above is valid syntax, the second string is easier to read, and more clearly shows what is going on. The following strings are also valid syntax:

- 1-2,5,6,7,15
- 1-2,5,6-7,15
- 1-2,5-6,7,15

While the entries above would work, they are harder to grasp quickly than the first two examples. Beyond the cluttered appearance of these last three strings, they tend to obscure the part of reality they represent: the contiguous block of timeslots from 5-7.

CLI Example #1

To define a DS0 mapping between a T1 line, (WAN) Port 1, timeslots 1–24, and a G.SHDSL modem, Port 3 (modem #3), timeslots 1, 2, type the following text:

t1-e1:1:1-24/G.SHDSL:3:1-24

CLI Example #2

To define a mapping between a T1 line, (WAN) Port 2, timeslots 4–6, and another T1 line, (WAN) Port 3, timeslots 8–10, type the following text:

t1-e1:2:4-6/t1-e1:3:8-10

CLI Example #3

To define a mapping between G.SHDSL modem port 6, timeslots 1–16, and G.SHDSL modem port 20, timeslots 1–16, type the following text:

G.SHDSL:6:1-16/G.SHDSL:20:1-16

After entering the parameters required to define the DS0 mapping, go to section "Saving a DS0 mapping definition".

Saving a DS0 mapping definition

Now that you have entered the parameters required to define the DS0 mapping you must save your cross-connection map to the T-DAC's random access memory (RAM) in order to activate the connection. To save the DS0 mapping, click the **Submit Query** button to save the static connection.

Defined Mappings Table (Static Connections)

The defined mapping (Static Connections) section of the DS0 Mapping Configuration window (see figure 37) displays all previously defined DS0 mappings (cross-connections) in the T-DAC. The parameter details are described in the following paragraphs.

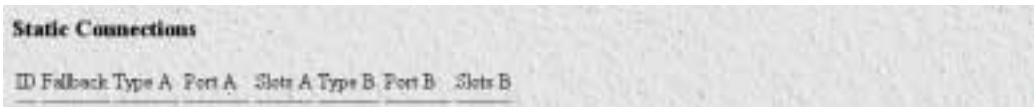


Figure 37. Configure Static Connections section of DS0 Mapping Configuration window

ID (daxConnectionID)

The connection ID is a number (a positive non-zero integer) that uniquely identifies each DS0 mapping. Connection IDs start with the number one (1), and are incremented sequentially. As DS0 mappings (connections) are defined, the T-DAC assigns connection IDs automatically. When the user enters DS0 mapping parameters and clicks the <submit query> button, the T-DAC automatically assigns the next available ID number in sequence to that connection.

Fallback

For DS0 mappings for which no fallback connection is defined, this column will be blank. For DS0 mappings with a defined fallback connection, the value in the Fallback column indicates whether the DS0 mapping displayed in that row is the primary or a backup connection. The first row will display the primary connection and the second row will display the defined backup connection. If the backup connection maps to the H.110 bus, a third row will display the parameters associated with the receive channel (the logical port on which the T-DAC receives data from the H.110 bus). For a backup connection displayed in the second row and third row (in the case of an H.110 connections), the parameter names with their MIB variables are given below.

- Type A *daxNewMapTypeTo*
- Port A *daxNewMapNumberTo*
- Slots A *daxFallbackSlotTo*
- Type B *daxNewMapTypeFrom*
  daxNewMapTypeH110
- Port B *daxNewMapNumberFrom*
  daxNewMapNumberH110
- Slots B daxFallbackSlotFrom
  daxNewMapSlotH110

Type A
Displays the type of interface port the T-DAC uses for the *A* channel of this connection.

Port A
Displays the ports the T-DAC uses for channel A.

Slots A
Displays which 64-kbps time slots (also referred to as the *DS0 data communications channels*) are used for channel A.

Type B
Displays the type of interface port the T-DAC uses for the *B* channel of this connection.

Port B
Displays the ports the T-DAC uses for channel B.

Slots B
Displays which 64-kbps time slots (also referred to as the *DS0 data communications channels*) are used for channel B.

DS0 Connection ID (DAX Connection ID) window

The DS0 Connection ID window provides the capability to delete an existing DS0 mapping (connection). The page also displays all the mapping parameters which define the connection.

Viewing the DS0 Connection ID window
To view the DS0 Connection ID window for a certain DS0 mapping (connection):

1. On the DSO Mapping page, under Static Connections, find the Connection ID number for the DS0 mapping you wish to view.
2. Click the Connection ID number hyperlink to display the DS0 Connection ID window for the selected connection ID.

Deleting a DS0 Mapping

To delete the DS0 Mapping displayed on the DS0 Connection ID window:

1. In the drop-down menu for the Connection Status parameter, ensure that the value delete(1) is selected.
2. Click the submit Query button to delete the connection (DS0 mapping).

Note When you delete a DS0 mapping (connection), the T-DAC also deletes any and all fallback mappings defined for the connection automatically. Fallback mappings, however, are *not* shown on this page. You can determine whether a fallback mapping is defined for a connection by examining the Port Fallback Table on the DS0 Fallback window or the Static Connections table on the DS0 Mapping page.

Chapter 8 System Clocking

Chapter contents

Introduction

During operation the 3096RC T-DAC sychronizes data transmission on all DS0 channels with a digital clock pulse, called the *reference clock*. The system clocking parameters define the T-DAC's source for that pulse (i.e. where the T-DAC will look for the reference clock).

The clocking subsystem includes a fallback mechanism by which the T-DAC monitors a primary clock source, and switches to a fallback source if the primary becomes unavailable. By default, the clocking fallback mechanism is disabled at the factory before the T-DAC is shipped. To activate the T-DAC's fallback system you must enable it.

The parameters *Clocking Mode*, *Primary Clocking Reference*, *Fallback Clocking Reference*, and *Enable/Disable Fallback System* control the T-DAC's clocking subsystem.

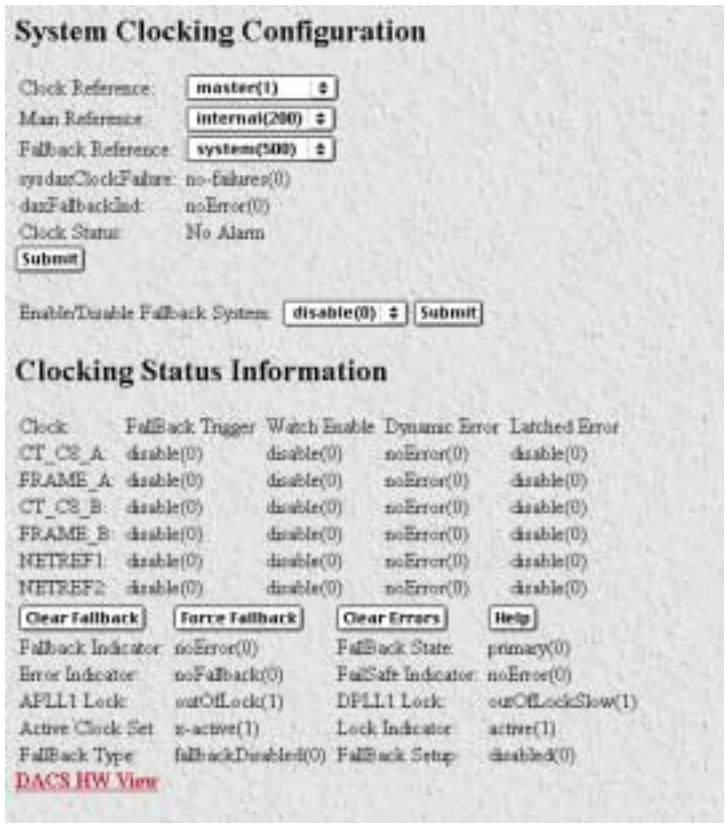


Figure 38. System Clocking Configuration window

System Clocking Configuration window

The System Clocking Configuration window enables you to define the system clocking parameters and view certain clocking status information. To display the System Clocking Configuration window (see figure 38), click the System Clocking link on the Configuration Menu pane.

The System Clocking Configuration window includes the following items:

- System Clocking Configuration table—Displays the configurable system clocking parameters and non-configurable (display-only) parameters (see section "System Clocking Configuration table" on page 69).

- Clocking Status Information table—Displays a set of display-only parameters intended for use by software engineers during field debugging. Therefore, most T-DAC end-users will not use this information. (See section "System Clocking Configuration table".)
- DACS HW View link—Clicking on this link takes you to the Hardware View window as shown in figure 39 (see section "DACS HW View link" on page 74).

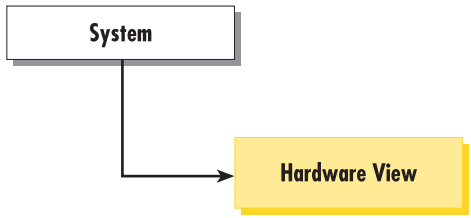


Figure 39. System Clocking windows map

System Clocking Configuration table

The following sections describe the system clocking parameters.

Note When you are finished configuring the system clocking parameters, make sure you save the changes (see section "Saving your work" on page 72).

Clock Reference (sysGSClockMode)

The Clock Reference parameter defines the clocking mode for the 3096RC. The clocking mode you assign to the T-DAC defines whether or not it provides the main reference clock to the entire chassis in which the T-DAC resides. Clocking mode options are as follows:

- Master—In master mode (also referred to as *primary mode*) the T-DAC obtains the main reference clock and provides it to other equipment installed in the chassis with the T-DAC. Because there can only be one master clock source in the chassis, if the T-DAC is the only blade in the chassis, you ***must*** define the clocking mode as master, but if another blade in the chassis has already been defined as the master, ***do not*** define the T-DAC's clocking mode as master.
- Secondary—In secondary mode, the T-DAC provides a backup (referred to as *secondary* or *fallback*) reference clock. It will obtain the main reference clock and provide it to other equipment in the chassis only if the device designated to provide the master clock reference fails. For reliability, we recommend having a secondary clocking blade defined for the chassis.
- Slave—In slave mode the T-DAC does not provide any clock reference. Frequently, the 3096RC will be defined as a slave while another blade (such as the Patton Model 6511) is configured as the master.

To configure the T-DAC's clocking mode, select one of the following values from the Clock Reference drop-down menu:

- master(1)—The T-DAC will obtain the main reference clock and provide it to the other equipment installed in the chassis with the T-DAC
- secondary(2)—If the device designated to provide the chassis master clock reference fails, the T-DAC—as the secondary source of the master clock—will obtain the main reference clock and provide it to the other equipment installed in the chassis with the T-DAC
- slave(3)—The T-DAC will ***not*** provide clocking reference for any other blade in the chassis

Main Reference (sysgshDSLClockMainRef) and Fallback Reference (sysgshDSLClockFallbackRef)

The Main Reference and Fallback Reference parameters define a primary and secondary (fallback) reference for the T-DAC system clock source (and for all blades in the chassis when the T-DAC's clocking mode is defined as master). The T-DAC will use the fallback reference if and only if the primary reference becomes unavailable. By default, the clocking fallback mechanism is disabled at the factory before the T-DAC is shipped. To activate the T-DAC's fallback system you must enable it (see Enable/Disable Fallback System).

When defining the primary and secondary clocking sources, you can select any one of the T-DAC's 4, 8, 12, or 16 WAN ports, the T-DAC internal clock pulse oscillator, or a system clock provided by another blade in the same chassis. The 3096RC will use the main reference as its system clocking source unless the main reference fails or is disconnected. When the primary reference becomes unavailable 3096RC will switch to the fallback reference as its system clocking source.

Both parameters will be defined from the same set of possible values. For the fallback reference to serve its purpose, however, you must define it by selecting a value different from the main reference. You must also enable the T-DAC's fallback mechanism (see Enable/Disable Fallback System). For the T-DAC's primary and secondary clocking references, you can choose:

- One of the T-DAC 4, 8, 12, or 16 WAN ports
- An internal oscillator residing within the T-DAC
- A system clock provided by another blade in the chassis

To define the Main Reference and the Fallback Reference, select one of the following values from the drop-down menu:

- wan-1(1)—use WAN port #1 for the clock source
- wan-2(2)—use WAN port #2 for the clock source
- wan-3(3)—use WAN port #3 for the clock source
- wan-4(4)—use WAN port #4 for the clock source
- wan-5(5)—use WAN port #5 for the clock source
- wan-6(6)—use WAN port #6 for the clock source
- wan-7(7)—use WAN port #7 for the clock source
- wan-8(8)—use WAN port #8 for the clock source
- wan-9(9)—use WAN port #9 for the clock source

- wan-10(10)—use WAN port #10 for the clock source
- wan-11(11)—use WAN port #11 for the clock source
- wan-12(12)—use WAN port #12 for the clock source
- wan-13(13)—use WAN port #13 for the clock source
- wan-14(14)—use WAN port #14 for the clock source
- wan-15(15)—use WAN port #15 for the clock source
- wan-16(16)—use WAN port #16 for the clock source
- internal(200)—use the internal free-running oscillator for the clock source.
- external(300)—use the system clock reference provided by another blade in the chassis for the clock source.

Clocking Status [sysdaxClockFailure]

The Clocking Status parameter indicates which, if any, clocking source has failed. The T-DAC considers a clocking source failed when:

- The T-DAC can no longer detect a pulse
- The T-DAC detects an incorrect number of clock pulses per frame.

The value of Clocking Status may be one of the following:

- no-failures(0)—The T-DAC has detected no failure in the clocking subsystem
- main-ref-fail(1)—The T-DAC's primary clocking reference has failed
- fallback-ref-fail(2)—The T-DAC's fallback clocking reference has failed
- master-system-clock-fail(4)—The clock signal provided by the blade in the cPCI chassis with its clocking mode defined as Master has failed.
- secondary-system-clock-fail(8)—The clock signal provided by the blade in the cPCI chassis with its clocking mode defined as Secondary has failed.

Fallback Indication [daxFallbackInd]

The Fallback Indication parameter indicates whether the T-DAC has switched to its defined secondary reference as its clocking source. The value of Fallback Indication may be one of the following:

- noError(0),
- fallbackActive(1)

Clock Status

The Clock Status field indicates alarm conditions relating to the T-DAC's clocking subsystem. If there are no alarms, the Clock Status field will indicate No Alarm (see figure on page 56). If an alarm condition exists, an Alarms Present message will be displayed along with one or more of the following failure descriptions as warranted by the situation:

- Main Local Reference Fail—The T-DAC primary clocking reference has failed
- Fallback Local Reference Fail—The T-DAC's fallback clocking reference has failed

- Master System Fail—The clock signal provided by the blade in the cPCI chassis with its clocking mode defined as Master has failed.
- Secondary System Fail—The clock signal provided by the blade in the cPCI chassis with its clocking mode defined as Secondary has failed.
- Fallback Indication—The T-DAC has switched it's clocking source to the fallback reference.

Enable/Disable Fallback System

This parameter defines the T-DAC's clocking fallback mechanism as enabled or disabled. By default, the clocking fallback mechanism is disabled at the factory before the T-DAC is shipped. To activate the T-DAC's fallback system you must enable it. When disabled, the T-DAC will not use the fallback reference clocking source, even if the primary reference becomes unavailable. To define the Enable/Disable Fallback System parameter, select one of the following values form the drop-down box.

- disable(0)
- enable(1)

Once you have defined the desired value for the Enable/Disable Fallback System parameter, you must click the adjacent **Submit Query** button to save your selection into volatile DRAM.

Saving your work

Once you have defined your desired values for the system clocking parameters, you must click the **Submit Query** button to save your settings into volatile DRAM.

Immediate actions buttons

The immediate actions buttons with their respective functions are described below:

- Clear Fallback—Clicking the Clear Fallback button clears the system clocking fallback state by setting the value of FallBack State to primary(0). The T-DAC will stop using the fallback reference and return to using the defined primary reference as its clocking source
- Force Fallback—Clicking the Force Fallback button forces the T-DAC into the fallback clocking state by setting the value of FallBack State to fallback(1). The T-DAC will switch to the defined Fallback Reference as its clocking source.
- Clear Errors—Clicking the Clear Errors button clears the T-DAC's error condition for all clock signals. For all clock signals, the T-DAC will reset the Dynamic Error variables to a value of noError(0).
- Help—Clicking the Help button displays the DACS Clocking Help window (see figure 40).

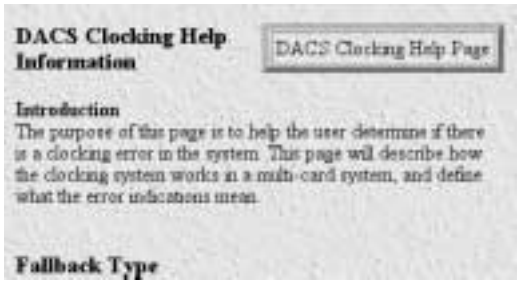


Figure 40. System Clocking help window

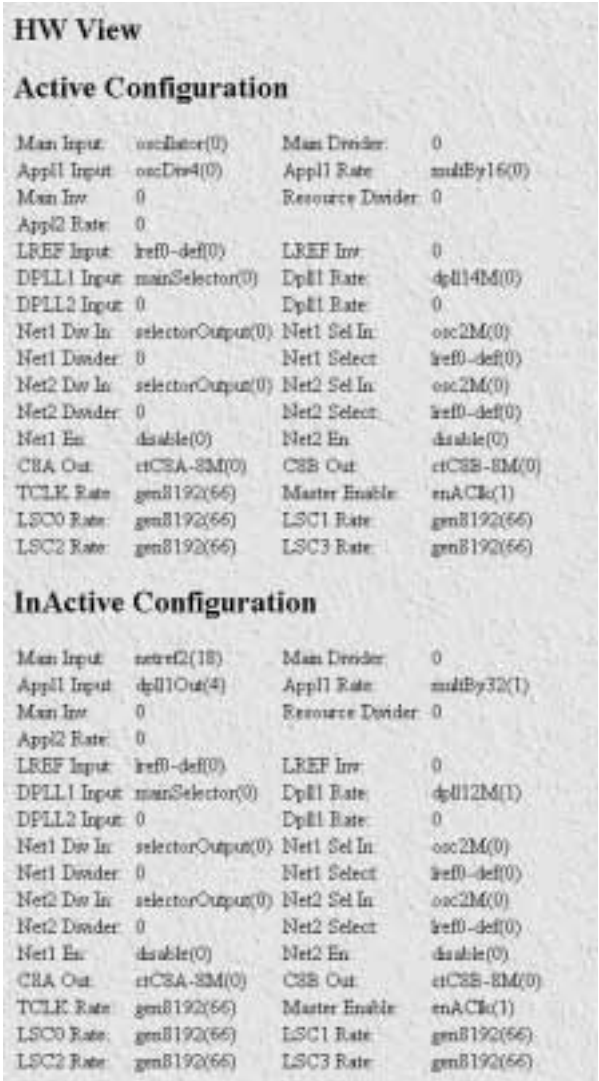
Additional Parameters

The following parameters displayed below the immediate actions buttons, are intended only for use by Patton Technical Support and are not described in this document.

- Fallback Indicator
- Error Indicator
- APLL1 Lock
- Active Clock
- FallBack Type

DACS HW View link

Clicking the DACS HW View link displays the DACS Hardware View window. The DACS Hardware View sub-page provides information about how your T-DAC hardware is configured. The following section describe the HW View window contents.



HW View

Active Configuration

Main Input:	oscillator(0)	Main Divider:	0
Appl1 Input:	oscDiv4(0)	Appl1 Rate:	multBy16(0)
Main Inv:	0	Resource Divider:	0
Appl2 Rate:	0		
LREF Input:	lref0-def(0)	LREF Inv:	0
DPLL1 Input:	mainSelector(0)	Dpll1 Rate:	dpll14M(0)
DPLL2 Input:	0	Dpll1 Rate:	0
Net1 Div In:	selectorOutput(0)	Net1 Sel In:	osc2M(0)
Net1 Divider:	0	Net1 Select:	lref0-def(0)
Net2 Div In:	selectorOutput(0)	Net2 Sel In:	osc2M(0)
Net2 Divider:	0	Net2 Select:	lref0-def(0)
Net1 En:	disable(0)	Net2 En:	disable(0)
CSA Out:	ctCSA-8M(0)	CSB Out:	ctCSB-8M(0)
TCLK Rate:	gen8192(66)	Master Enable:	enAClk(1)
LSC0 Rate:	gen8192(66)	LSC1 Rate:	gen8192(66)
LSC2 Rate:	gen8192(66)	LSC3 Rate:	gen8192(66)

InActive Configuration

Main Input:	netref2(18)	Main Divider:	0
Appl1 Input:	dpll1Out(4)	Appl1 Rate:	multBy32(1)
Main Inv:	0	Resource Divider:	0
Appl2 Rate:	0		
LREF Input:	lref0-def(0)	LREF Inv:	0
DPLL1 Input:	mainSelector(0)	Dpll1 Rate:	dpll12M(1)
DPLL2 Input:	0	Dpll1 Rate:	0
Net1 Div In:	selectorOutput(0)	Net1 Sel In:	osc2M(0)
Net1 Divider:	0	Net1 Select:	lref0-def(0)
Net2 Div In:	selectorOutput(0)	Net2 Sel In:	osc2M(0)
Net2 Divider:	0	Net2 Select:	lref0-def(0)
Net1 En:	disable(0)	Net2 En:	disable(0)
CSA Out:	ctCSA-8M(0)	CSB Out:	ctCSB-8M(0)
TCLK Rate:	gen8192(66)	Master Enable:	enAClk(1)
LSC0 Rate:	gen8192(66)	LSC1 Rate:	gen8192(66)
LSC2 Rate:	gen8192(66)	LSC3 Rate:	gen8192(66)

Figure 41. DACS Hardware View window

Active Configuration Table

The Active Configuration table shows the values currently stored in active volatile DRAM. These values represent the live operational status. The active configuration will be lost when the T-DAC is powered down.

Inactive Configuration Table

The Inactive Configuration table shows the values of the hardware configuration variables stored in NVRAM. When the T-DAC is powered up these values will be written to DRAM and become the new active configuration.

Chapter 9 DSL

Chapter contents

Introduction

The T-DAC's G.SHDSL port subsystem comprises 16 G.SHDSL ports for connection to external G.SHDSL CPE modems at nx64 data rates up to 4.608 Mbps. Each G.SHDSL port consists of an internal G.SHDSL modem whose signals are presented on a two-wire pair within the 50-pin RJ-21X connector on the T-DAC's rear blade. Managing the T-DAC's G.SHDSL ports involves defining the configurable G.SHDSL port parameters, monitoring the G.SHDSL port status and statistics. The T-DAC also provides the capability for you to define and download configurable parameters to a connected Patton remote CPE, such as the model 3086 or 3201.

To display the G.SHDSL Port Configuration window, on the Configuration Menu pane, click the G.SHDSL link (see figure 42).

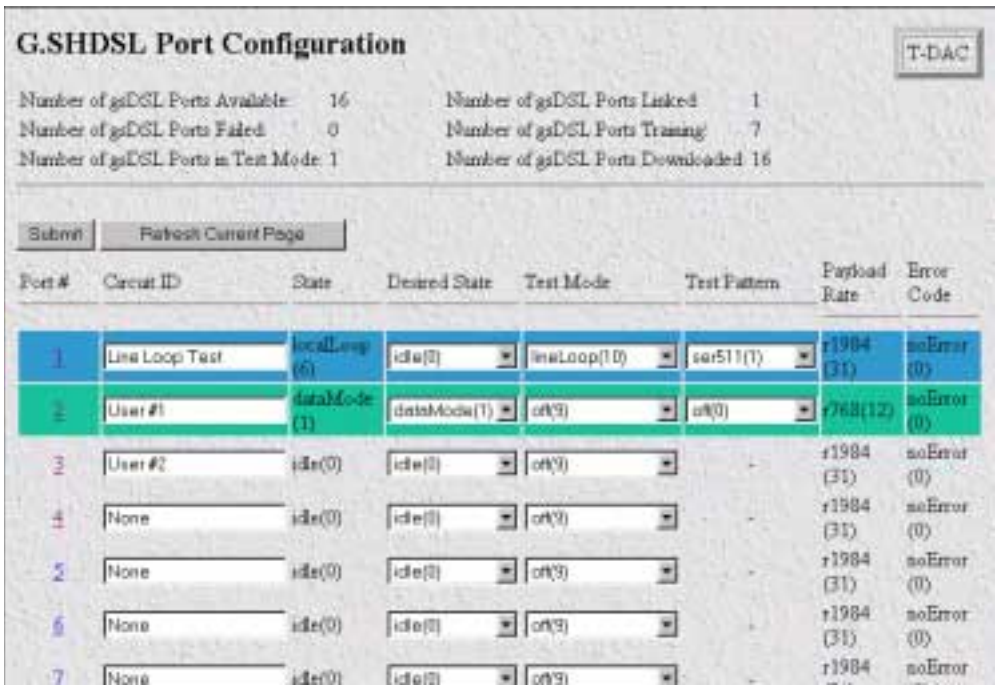


Figure 42. G.SHDSL Port Configuration window

G.SHDSL Port Configuration main window

The G.SHDSL Port Configuration main window (see figure 42) provides the means for you to manage the G.SHDSL port subsytem on the 3096RC T-DAC. These page displays current status, statistics, and configurable parameters for the G.SHDSL ports. It provides the means to define the configurable parameters for each G.SHDSL port and provide information about the G.SHDSL links to remote CPE G.SHDSL. The status and statistics information is shown in display-only fields. Configurable parameter values may be shown in display-only format or in user-definable formats such as drop-down boxes or user-entry text fields, depending on port operating status, and the specific page on which the parameter appears.

The G.SHDSL Port Configuration window provides links to the windows shown in the figure 43.

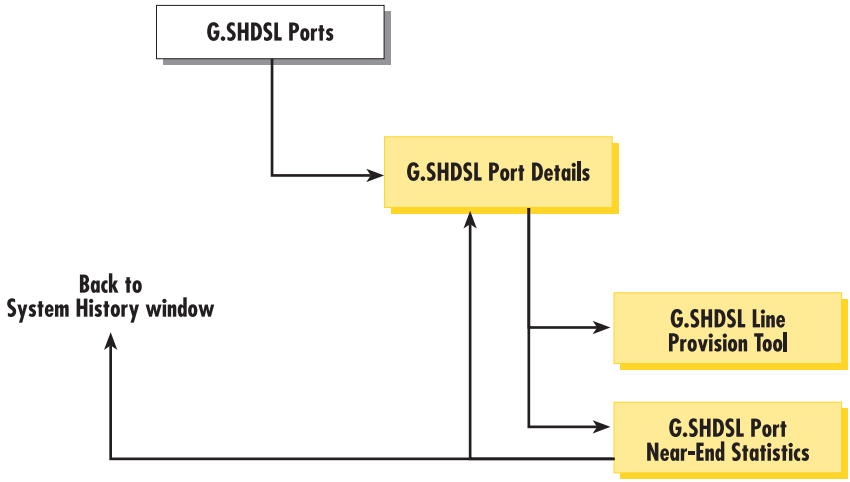


Figure 43. G.SHDSL management windows map

The G.SHDSL Ports web management page shows the high-level status summary for all 16 G.SHDSL ports, plus a more detailed summary status for each individual port. The page provides this information in two tables:

- G.SHDSL Port Summary Status
- G.SHDSL Port Status (see page 80)

The contents of the two tables is described in subsequent paragraphs.

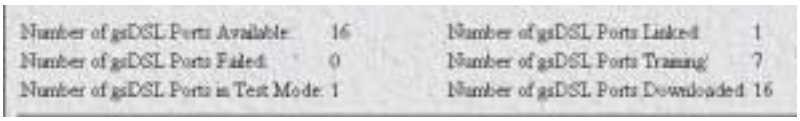


Figure 44. G.SHDSL Port Summary Status section of G.SHDSL Port Configuration window

G.SHDSL Port Summary Status

The G.SHDSL Port Summary Status section of the G.SHDSL Port Configuration window (see figure 44) displays the following parameters:

- Number of gshDSL Ports Available (numgshDSLPorts)—Total number of G.SHDSL ports currently available for use. The sum of the values in Number of G.SHDSL Available and Number of G.SHDSL Failed will be 16. The T-DAC determines this parameter value during power up when the G.SHDSL modems are tested for availability or failure.
- Number of gshDSL Ports Failed (numgshDSLPortsFailed)—Total number of G.SHDSL ports with hardware failures. The sum of the values in Number of G.SHDSL Available and Number of G.SHDSL Failed will be 16. The T-DAC determines this parameter value during power up when the G.SHDSL modems are tested for availability or failure.
- Number of gshDSL Ports in Test Mode (numgshDSLPortsInTestMode)—Total number of G.SHDSL ports for which the T-DAC operator has defined the Test Mode parameter defined as one of the following:

- Local Loop
- Remote Serial Loops
- Remote Ethernet Loops
- Line Loop

- Number of gshDSL Ports Linked (numgshDSLPortsLinked)—Total number of G.SHDSL ports which have established a logical data link connection with a remote G.SHDSL CPE modem. The two devices have synchronized and are able to pass data.
- Number of gshDSL Ports Training (numgshDSLTraining)—Total number of G.SHDSL ports which are in the process of attempting to establish a logical data link connection with a remote G.SHDSL CPE modem.
- Number of gshDSL Ports Downloaded (numgshDSLPortsDownloaded)—Total number of G.SHDSL ports which have loaded their operating software from NVRAM into the port's digital signal processor (DSP) chip.

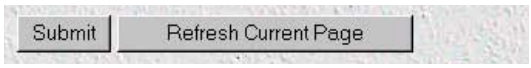


Figure 45. G.SHDSL Port Configuration window operator action buttons

Operator Action Buttons

The operator action buttons (see figure 45) do the following:

- **Submit Button**—When defining values for configurable parameters on the page, you will use this button to save your work. When you click the submit button, the T-DAC writes the currently displayed parameter values to volatile DRAM. You will also see a second Submit button at the bottom of the page, which provides exactly the same function.
- **Refresh Current Page Button**—Refreshes the display. When you click the Refresh Current Page Button, the T-DAC retrieves parameter values currently stored in DRAM and displays them on the page. Any values entered or selected since you last clicked [submit] will be overwritten with values retrieved from DRAM. After defining new values for configurable parameters on this page, use this button to update the display to reflect any resulting changes in G.SHDSL port status.

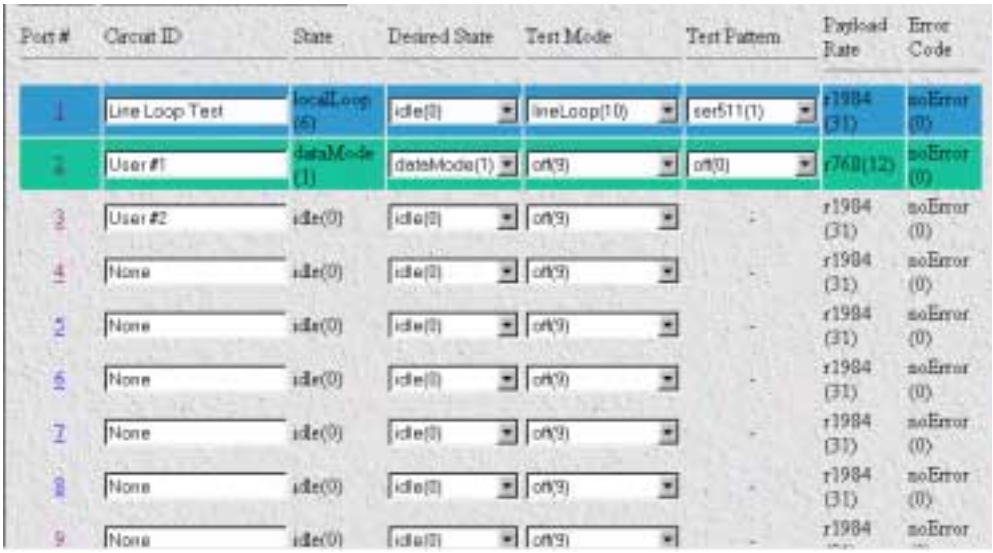


Figure 46. G.SHDSL Port Status section of G.SHDSL Port Configuration window

G.SHDSL Port Status

The G.SHDSL Port Status section of the G.SHDSL Port Configuration window (see figure 46) shows the overall status for each of the 16 internal G.SHDSL ports, and provides the means for you to define the following G.SHDSL port parameters:

- Circuit ID
- Desired State
- Test Mode
- Test Pattern

The following sections describe the contents of the G.SHDSL Port Status table.

Port Number [gshDSLPortNum]

The first column in the Port Status table identifies each of the 16 G.SHDSL ports by an index number. The ports are numbered 1 through 16. Each port number in the table also functions as a hyperlink. Clicking on the Port Number link opens the G.SHDSL Port Details sub-page, where you can view detailed port status and statistics, and define additional configurable G.SHDSL port parameters. The G.SHDSL Port Details window is described later in this chapter (see section "G.SHDSL Port Details window" on page 87).

Circuit ID [gshDSLCircuitID]

Configurable. The Circuit ID parameter provides a way for you to define a free-text name (character string) that identifies each circuit (link) connected to the T-DAC. Although the table display is limited to 20 characters at a time, the T-DAC supports Circuit IDs of up to 40 characters long. The recommended way to use this field is to design a structured mnemonic naming convention scheme for your application. For example, A DSL service provider might identify each of the T-DAC's G.SHDSL circuits using a subscriber ID (e.g. billybob@rednet.net), for the subscriber to which the circuit connects. Other examples might be to use a combination of user location and sequence number (e.g. dallas666), or to use subscriber account numbers.

State [gshDSLState]

The State parameter indicates the current real-time operating state of the port. Possible values are:

- **idle(0)**—The Desired State for the port is currently defined to be idle(0). This state typically indicates the port is currently NOT connected to a remote CPE modem.
- **dataMode(1)**—The T-DAC's G.SHDSL modem port has synchronized timing and established the link with the remotely connected CPE modem. The link is ready and able to transfer data.
- **training(2)**—The T-DAC's G.SHDSL modem port is attempting to synchronize and establish the link with the remotely connected CPE modem.
- **deactivating(3)**—The T-DAC's G.SHDSL modem port is disconnecting and de-synchronizing its link with the remotely connected CPE modem. deactivating(3) is the temporary intermediate state between dataMode(1) and idle(0). When the T-DAC operator changes the port's desired state from dataMode(2) to idle(0), the port state will quickly transition through deactivating(3) before changing to idle(0).
- **downloading(4)**—The port's digital signal processor (DSP) chip is currently loading it's operating software from NVRAM into the chip's memory.
- **error(5)**—The T-DAC has detected an error condition for the G.SHDSL modem port. The error condition may be caused by one of the following:
  - The port failed to download its operating software from NVRAM.
  - The port's operating software image is corrupted.

  Note See section "Clearing an error condition" for information on resetting a port to clear an error.
- **localLoop(6)**—The port is operating in local loopback mode (see section "Test Mode [sDSLTMSelection]" on page 82)
- **remSerLoop(8)**—The port is operating in remote serial loopback mode (see section "Test Mode [sDSLTM-Selection]" on page 82)
- **remEthLoop(11)**—The port is operating in remote ethernet loopback mode (see section "Test Mode [sDSLTMSelection]" on page 82)
- **lineLoop(10)**—The port is operating in line loopback mode (see section "Test Mode [sDSLTMSelection]" on page 82)

Clearing an error condition. To clear the error condition, do the following:

1. Click the port number link to open the G.SHDSL Port Details window.
2. At the bottom of the G.SHDSL Port Details window, click the button labeled **Hard Reset This Port**.

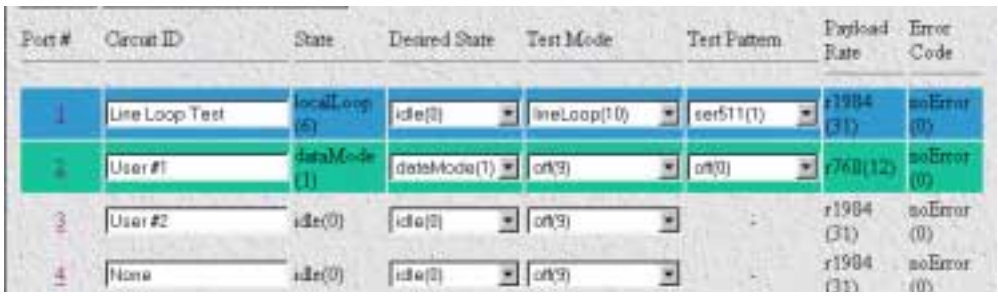


Figure 47. Color-coded port status example

Color-coded Port Status Indicators

The G.SHDSL Port Status table displays colored rows (see figure 47) to indicate port status for each port. The color-coded indications are described below:

- Green—The port is currently in dataMode(1) state. A G.SHDSL link is established with the remote CPE. The link is ready and able to transfer data.
- Blue—The port is operating in one of the following test modes
  - localLoop(6)
  - remSerLoop(8)
  - remEthLoop(11)
  - lineLoop(10)
- Yellow—One of the following is occurring:
  - The port is currently in training(2) state and the 4-minute link establishment timer has not expired
  - The port is in deactivating(3) state
  - The port is in downloading(4) state
- Orange—The port is in training(2) state and could not establish the G.SHDSL link (move to dataMode(2) state) within 4 minutes.
- Red—The port is currently in error(5) state (see section "State [gshDSLState]" on page 81)

Desired State [gshDSLDesireState]

Configurable. Indicates the T-DAC operator's current intentions for the port.

- **idle(0)**—Default value. The T-DAC operator intends the port for future use. Use this value when the port is not currently connected to a remote CPE modem.
- **dataMode(1)**—The T-DAC operator intends the port to be connected to a remote CPE modem for current active use

Test Mode [sDSLTMSelection]

Configurable when the value of port State is one of the following:

- **dataMode(1)**
- **localLoop(6)**

- **remSerLoop(8)**
- **remEthLoop(11)**

Otherwise, display-only with a value of *off(9)*.

Until the G.SHDSL link is established, the Test Mode value off(9) will appear in display-only form. Once the link is established and port state changes to datamode(1), the Test Mode drop-down menu will appear.

- **localLoop(6)**—The T-DAC's G.SHDSL port will operate in local loopback mode. Data transmitted through the T-DAC to the G.SHDSL port is looped back to the transmitting port as shown in figure 48.

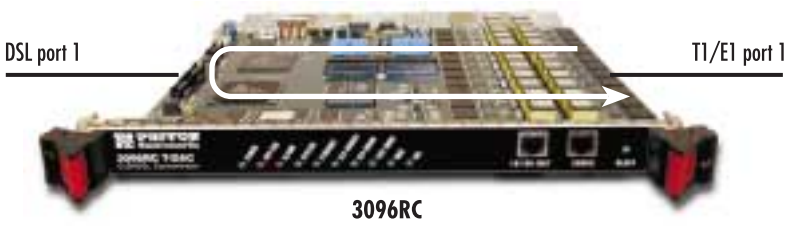


Figure 48. Local loopback

For example, suppose G.SHDSL port 1 is mapped to T1/E1 port 1, and the T-DAC operator has defined Test Mode for G.SHDSL port 1 as localLoop(6). As T1/E1 port 1 receives the T-DAC will send the data to G.SHDSL port 1 as normal. But instead of transmitting the data on G.SHDSL port 1, the T-DAC will loop the data back to T1/E1 port 1 for transmission on the T1/E1 link.

- **remSerLoop(8)**—For a Patton CPE G.SHDSL modem that provides a serial port (such as the model 3086), and that is remotely connected to this G.SHDSL port, remSerLoop(8) changes the operating mode of the serial port. The T-DAC will cause the serial port on the remote CPE to operate in loopback mode as show in figure 49.

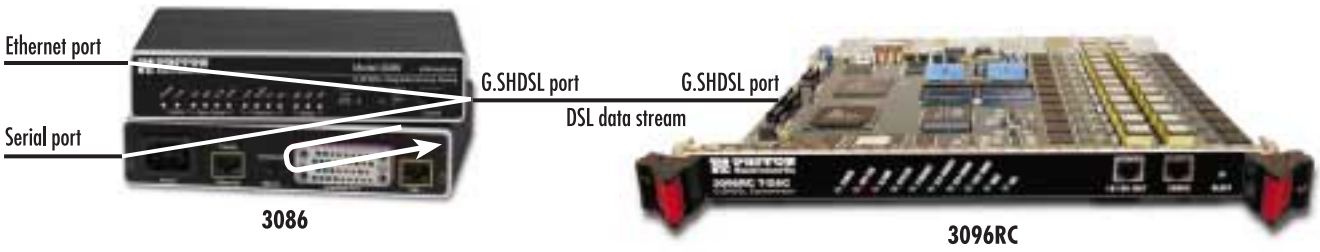


Figure 49. Remote serial loopback

When the T-DAC transmits data from the G.SHDSL port over the G.SHDSL link to the remote CPE's serial port, the serial port will loop the data back to the CPE's G.SHDSL port for transmission back to the T-DAC.

Note remSerLoop(8) has no effect on the Remote CPE's Ethernet port. Any data destined for the Ethernet port of a remote CPE will ***not*** be looped back.

- **remEthLoop(11)**—For Patton CPE G.SHDSL modems that provide an ethernet port, (such as models 3201 and 3086), and are remotely connected to this G.SHDSL port, remEthLoop(11) changes the operating mode of the Ethernet port. The T-DAC will cause the Ethernet port on the remote CPE to operate in loopback mode as show in figure 50.

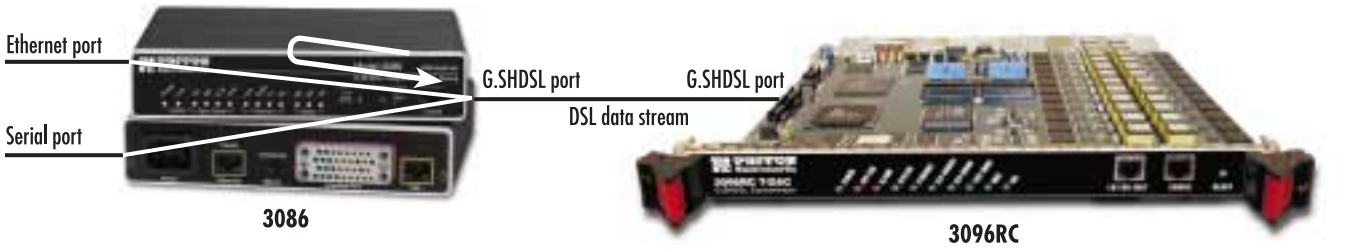


Figure 50. Remote Ethernet loopback

When the T-DAC transmits data from the G.SHDSL port over the G.SHDSL link to the remote CPE's Ethernet port, the Ethernet port will loop the data back to the CPE's G.SHDSL port for transmission back to the T-DAC.

> **Note** In the case where the remote CPE is a Patton model 3086, remEthLoop(8) has no effect on the Remote CPE's Serial port. remEthLoop(8) will NOT cause any data transmitted to the serial port of a remote CPE to be looped back.

- **lineLoop(10)**—The T-DAC's G.SHDSL port will operate in line loopback mode as shown in figure 51. For the CPE remotely connected to this port, you can use lineLoop(10) mode to test the G.SHDSL link from the CPE to the T-DAC and back to the CPE.

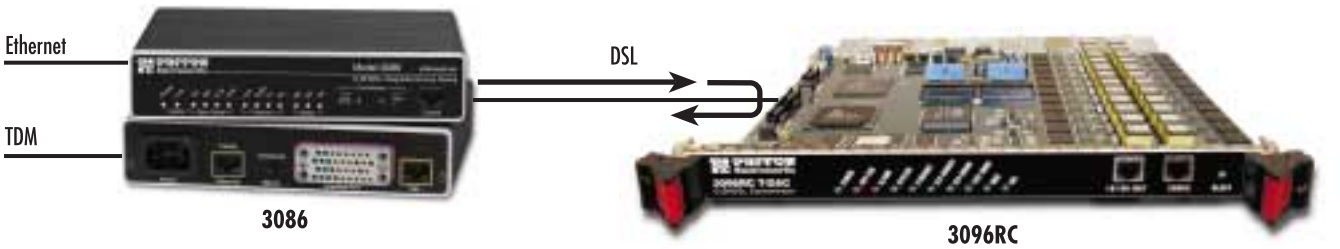


Figure 51. Line loopback

When a CPE transmits data to a T-DAC's G.SHDSL port with Test Mode defined as lineLoop(10), the G.SHDSLport will loop the data back to the CPE.

- **off(9)**—The default value for Test Mode. Appears as a display-only value.

Test Pattern [gshDSLPattSelect]

Configurable, but only when the value of State is one of the following:

- dataMode(1)
- localLoop(6)

- remSerLoop(8)
- remEthLoop(11)

Otherwise, display-only with a value of *off(9)*.

Until the G.SHDSL link is established, the G.SHDSL Port Status table will display a dash (-) in the Test Pattern column using display-only format. Once the G.SHDSL link is established and the port state changes to datamode(1), the Test Pattern drop-down menu will appear.

The Test Pattern parameter defines which test pattern the T-DAC will generate and transmit. The T-DAC's will transmit the selected test pattern to the destination port defined by the value of Test Mode (see section "Test Mode [sDSLTMSelection]" on page 82). To define the Test Pattern, select one of the following values from the drop-down menu, then click the **Submit Button**:

- off(0)
- ser511(1)
- ser511E(2)
- ser2047(3)
- ser2047E(4)
- ser63(5)
- ser63E(6)
- eth511(7)
- eth511E(8)
- eth2047(9)
- eth2047E(10)
- eth63(11)
- eth63E(12)

Once you click the **Submit Button**, the Test Pattern column will display the newly defined value in display-only format, together with a check box labelled Off. To disable the test or to change the test pattern, click the Off check box and click the **Submit Button**.

Payload Rate [gshDSLPayloadRate]

Display-only on the G.SHDSL Port Status page. Configurable on the G.SHDSL Port Details window.

Shows the currently defined payload rate (i.e. data rate as opposed to line rate) for the G.SHDSL link. The following values of Payload Rates may be defined for T-DAC G.SHDSL ports:

- r192(3)
- r256(4)
- r320(5)
- r384(6)
- r448(7)
- r512(8)
- r576(9)
- r640(10)
- r704(11)
- r768(12)
- r832(13)
- r896(14)
- r960(15)
- r1024(16)
- r1088(17)
- r1152(18)
- r1216(19)
- r1280(20)
- r1344(21)
- r1408(22)
- r1472(23)
- r1536(24)
- r1600(25)
- r1664(26)
- r1728(27)
- r1792(28)
- r1856(29)
- r1920(30)
- r1984(31)
- r2048(32)
- r2112(33)
- r2176(34)
- r2240(35)
- r2304(36)
- r2368(37)
- r2432(38)
- r2496(39)
- r2560(40)
- r2624(41)
- r2688(42)
- r2752(43)
- r2816(44)
- r2880(45)
- r2944(46)
- r3008(47)
- r3072(48)
- r3136(49)
- r3200(50)
- r3264(51)
- r3328(52)
- r3392(53)
- r3456(54)
- r3520(55)
- r3584(56)
- r3648(57)
- r3712(58)
- r3776(59)
- r3840(60)
- r3904(61)
- r3968(62)
- r4032(63)
- r4096(64)
- r4160(65)
- r4224(66)
- r4288(67)
- r4352(68)
- r4416(69)
- r4480(70)
- r4544(71)
- r4608(72)

Error Code [gshDSLErrorCode]

Display-only.

- noError(0)
- errorOne(1)
- errorTwo(2)
- errorThree(3)
- errorFour(4)
- errorFive(5)
- errorSix(6)
- errorSeven(7)

Saving Your Work

Once you have defined your desired values for the configurable parameters shown in the G.SHDSL Port Status table, you must click one of the two **Submit Query** buttons to save your settings into volatile DRAM. Click-

ing either of the submit query buttons will save the configurable parameter values displayed for all 16 G.SHDSL ports. Once you click the button, the T-DAC will implement the changes immediately.

Note To save your changes persistently, (i.e. when the T-DAC is powered down) you must visit the T-DAC HOME page, and click the **Save Current Configuration** button. When you click the **Save Current Configuration** button, the T-DAC will copy the configuration currently stored in volatile DRAM into non-volatile Flash memory for persistent storage.

G.SHDSL Port Details window

The G.SHDSL Port Details window (see figure 52) provides detailed management information and functions for a single selected T-DAC G.SHDSL port. The G.SHDSL Port Details window displays detailed port status, statistics, as well as the configurable parameters that define data rate and annex type for the link. The window also provides the capability to define certain configurable parameters for the G.SHDSL port of a remotely connected Patton CPE device.

Figure 52. G.SHDSL Port Details window

To display the G.SHDSL Port Details page, do the following:

1. On the Configuration Menu pane, click the DSL link to display the G.SHDSL Port Configuration window.
2. On the G.SHDSL Port Configuration page, in the Port Summary Status table, identify the port number for the port you wish to manage.
3. Click the Port # number link (see figure 53).

Figure 53. Port # links

The G.SHDSL Port Details window is organized into the following groups:

- Operator action buttons at the top of the page
- G.SHDSL Port Status and Statistics tables below the operator action buttons
- G.SHDSL Port Parameters tables on the lower part of the page.

The G.SHDSL Port Details window is related to other web management windows via links as show in figure 54.

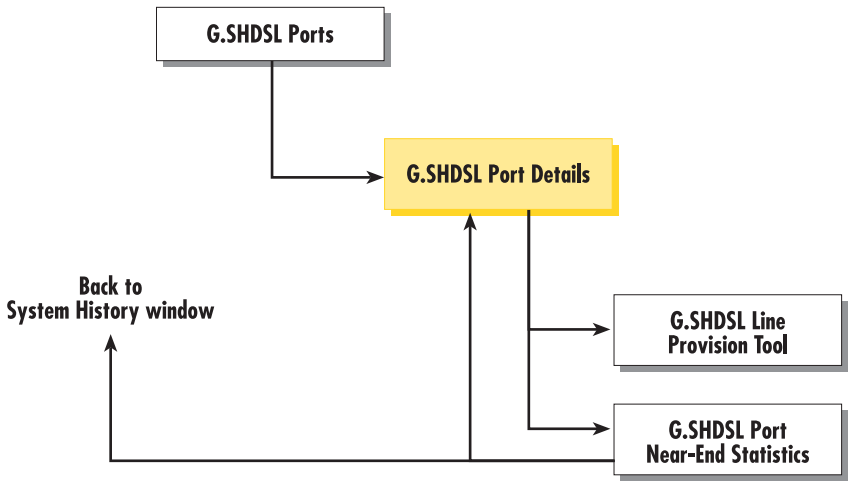


Figure 54. G.SHDSL Web Management windows map

The following paragraphs describe the contents of the G.SHDSL Port Details window.

Figure 55. Operator action buttons section of the G.SHDSL Port Details window

Operator action buttons

The G.SHDSL Port Details window provides the following operator action buttons (see figure 55):

- **Back**—Displays the previous page. When you click the **Back** button the T-DAC moves you back one level in the web management windows map (see figure 54 on page 88) to the G.SHDSL Port Configuration window.
- **Refresh Current Page**—Refreshes the display. When you click the **Refresh Current Page** button, the T-DAC retrieves parameter values currently stored in DRAM and displays them on the page. Any configurable parameter values entered or selected since you last clicked [submit] will be overwritten with values retrieved from DRAM. When monitoring operating status or statistics, or when defining new values for configurable parameters, use this button to update the display. You can watch any changes take place as they are reflected on the G.SHDSL port status display.
- **Clear Errors**—Clears all errors on this port. Resets the port statistical error counters to zero (0). A burst of errors typically occurs during port activation. Five (5) seconds after the port enters dataMode(1) the T-DAC will reset the statistical error counters to zero (0) in order to clear these expected startup errors. The port error counts accumulate from that point forward. Each time you click the **Clear Errors** button the T-DAC will clear all errors for this port, resetting the counters to zero.

  Clicking on the **Clear Errors** button resets the following counters:

  - CRC Errors [gshDSLCRCErrors]
  - Test Pattern Errors [gshDSLPattErrorCnt]
  - Link Drops (FLAPs) [gshDSLFlapCnt]
  - Loss of Delineation [gshDSLLOCDelineation]
  - Rx Fifo Errors [gshDSLRxFifoErr]
  - Tx Fifo Errors [gshDSLTxFifoErr]
  - Rx Fifo Overflow [gshDSLRxFifoOverflowErr]
  - Tx Fifo Overflow [gshDSLTxFifoOverflowErr]
  - Tx Stuff Errors [gshDSLTxStuffError]
  - Errored Sec [gshDSLErroredSec]
  - Severely Errored Sec [gshDSLSeverlyErroredSec]
- **Previous Port**—Displays the G.SHDSL Port Details page for the next lower numbered G.SHDSL port. For example, if you are viewing the G.SHDSL Port 3 Details page, when you click the **Previous Port** button the T-DAC will display the G.SHDSL Port 2 Details page. If you are viewing Port 1, the page will be refreshed.
- **Next Port**—Displays the G.SHDSL Port Details page for the next higher numbered G.SHDSL port. For example, if you are viewing the G.SHDSL Port 3 Details page, when you click the **Next Port** button the T-DAC will display the G.SHDSL Port 4 Details page. If you are viewing Port 16, the page will be refreshed.

Figure 56. G.SHDSL Port status and statistics sections of the G.SHDSL Port Details window

G.SHDSL Port status and statistics tables

The G.SHDSL Port Details page displays port status and statistics information organized as follows (see figure 56):

Port Status tables:

- General Info
- Activation State Info (see page 91)

Port Statistics tables:

- Fifo Info (see page 92)
- Data Path Info (see page 92)
- History Details (see page 93)

The following sections describe the contents of each table.

General Info table

The General Info table displays the current values of the following G.SHDSL port parameters:

- **Link** [**gshDSLLinkUp**]—Indicates the current state of the G.SHDSL link. One of the following values will be displayed:
  - up(1)
  - down(0)
- **Hardware** [**gshDSLHardwareFail**]—Indicates the current overall state of the G.SHDSL port hardware, i.e. the presence or absence of a hardware error condition. One of the following values will be displayed:
  - failed(1)
  - operational(0)
- **Line Quality** [**gshDSLLineQualityGood**]—Provides a highly generalized indication of the signal to noise ratio on the G.SHDSL line. One of the following values will be displayed:
  - good(16)
  - poor(0)

- **Sync State** [**gshDSLSyncState**]—Indicates the current state of synchronization on the line connecting this G.SHDSL port and the remote CPE modem. One of the following values will be displayed:
  - outOfSync(0)
  - acquiringSync(64)
  - inSync(128)
  - losingSync(192)
- **Download Done** [**gshDSLDownloadDone**]—Indicates whether the port's DSP has loaded its operational software from NVRAM. One of the following values will be displayed:
  - yes(1)
  - no(0)

Activation State Info table

The operating software for each G.SHDSL port includes a module called the Activation State Manager (ASM). The Activation State Info table provides information about the current software state for the port. The current values of the following G.SHDSL port parameters are shown in display-only format:

- **ASM State** [**gshDSLAtivationState**]—Indicates the current state of the Activation State Manager (ASM). One of the following values will be displayed:
  - asm-Idle(0)
  - asm-Normal(64)
  - asm-Deactivated(128)
  - asm-Training(192)
- **ASM Loss of Signal** [**gshDSLLossOfSignal**]—Indicates whether or not the port currently detects the presence of the G.SHDSL signal. One of the following values will be displayed:
  - loss(1)
  - foundSignal(0)
- **PCM Clock** [**gshDSLActivationFailurInfo**]—Indicates the current state of the pulse code modulation (PCM) clock. One of the following values will be displayed:
  - valid(0)—PCM clock is activated
  - invalid(1)
- **Loss Of Sync Word—**Indicates the current operating state of the ASM [gshDSLLossOfSyncWord] G.SHDSL framing software for this port. The ASM framer uses the synch word field in the G.SHDSL frame to control the timing on the link. One of the following values will be displayed:
  - loss(4)—G.SHDSL timing is out of synchronization
  - foundWord(0)—G.SHDSL timing is synchronized

- DPLL Locked [gshDSLDPLLLocked]—Indicates whether the DSL port's internal clock generator is phase-locked with its external reference clock. One of the following values will be displayed:
  - locked(1)
  - notLocked(0)

Fifo Info table

Each G.SHDSL port's data transceiver uses a first-in first-out (FIFO) queuing mechanism. The Fifo Info table provides statistics pertaining to FIFO queue operation. Current values of the following counters are shown:

- **Rx Fifo Errors [gshDSLRxFifoErr]**—Indicates the number queuing errors in the FIFO receive queue since the since the counter was last reset.
- **Tx Fifo Errors [gshDSLTxFifoErr]**—Indicates the number queuing errors in the FIFO transmit queue since the since the counter was last reset.
- **Rx Fifo Overflow [gshDSLRxFifoOverflowErr]**—Indicates the number of times a queue overflow occurred in the FIFO receive queue since the since the counter was last reset.
- **Tx Fifo Overflow [gshDSLTxFifoOverflowErr]**—Indicates the number of times a queue overflow occurred in the FIFO transmit queue since the since the counter was last reset.
- **Tx Stuff Errors [gshDSLTxStuffError]**—Indicates the number of transmit stuffing errors since the since the counter was last reset.

> **Note** A burst of errors typically occurs during port activation. Five seconds after the port enters dataMode(1) the T-DAC will reset the statistical error counters to zero in order to clear these expected startup errors. The port error counts accumulate from that point forward. Each time you click the **Clear Errors** button the T-DAC will clear all errors for this port, resetting the counters to zero.

Data Path Info table

The Data Path Info table displays the current values of the following G.SHDSL port statistics variables:

- **CRC Errors [gshDSLCRCErrors]**—Indicates the number of Cyclical Redundancy Check (CRC) errors on this port since the counter was last reset.
- **Test Pattern Errors [gshDSLPattErrorCnt]**—Indicates the number of test pattern errors detected on this port. Valid only when the port is defined to be in one of the test modes.
- **Link Drops (FLAPs) [gshDSLFlapCnt]**—Indicates the number of times the link has flapped (gone down and come back up again) since the counter was last reset.
- **Loss of Delineation [gshDSLLOCDelineation]**—Indicates the number of times since the counter was last reset that the G.SHDSL framer has lost track of the delineation (frame boundary) between G.SHDSL frames.
- **Noise Margin (dB) [DSLNoiseMargin]**—Indicates the most recently calculated noise margin in dB for the port. The T-DAC re-calculates this value every 2 seconds. To update the value click the click the refresh current page button.

History Details table

Note The title for the History Details table also functions as a hyperlink. Click the History Details link to display the G.SHDSL Port History of Near-End Performance window which provides a record of errors counted on this port during the last 24 hours in 15-minute intervals (see section "G.SHDSL Port History of Near-End Performance window" on page 101 for more information).

The History Details table displays the current values of the following G.SHDSL port statistics variables:

- **Port Up-Time (d:h:m:s)**

  [gshDSLTotalDay] [gshDSLTotalHour] [gshDSLTotalMin] [gshDSLTotalSec]

  Total length of time in days:hours:minutes:seconds since the downloaded state changed to yes(1) this port. This value is reset when the T-DAC powers down. (When the T-DAC first powers up the value of downloaded is no(0).)

- **Link Up-Time (d:h:m:s)**

  [gshDSLAvailableDay] [gshDSLAvailableHour] [gshDSLAvailableMin] [gshDSLAvailableSec]

  Total Length of time in days:hours:minutes:seconds since the link state for this port last changed to up(1). This value is reset when the link goes down.

- **Unavailable Time (d:h:m:s)**

  [gshDSLUnAvailableDay] [gshDSLUnAvailableHour] [gshDSLUnAvailableMin] [gshDSLUnAvailableSec]

  Total cumulative time in days:hours:minutes:seconds (since the last power cycle) that the link state for this port has been down(0).

- **Errored Sec**

  [gshDSLErroredSec]

  The total cumulative number of seconds in which there were one or more FIFO errors on this port since the counter was last reset.

- **Severely Errored Sec**

  [gshDSLSeverlyErroredSec]

  The total cumulative number of seconds in which there were one or more CRC errors on this port since the counter was last reset.

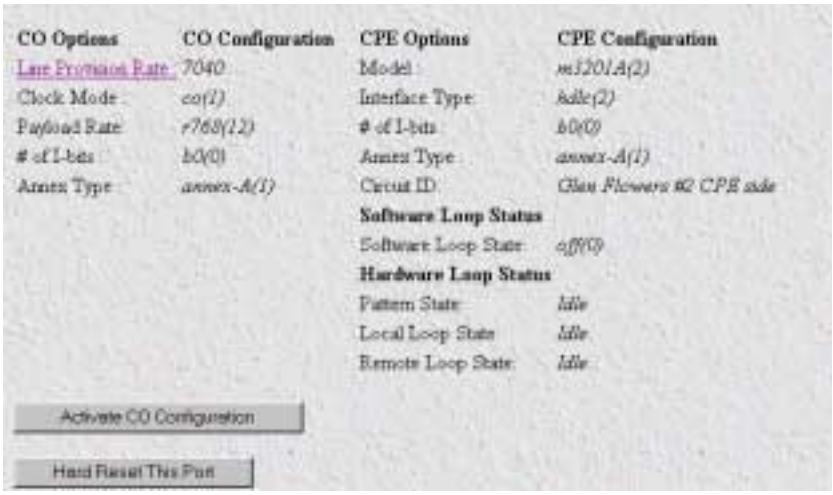


Figure 57. G.SHDSL port configuration section of the G.SHDSL Port Details window

Port configuration tables

The G.SHDSL Port Details window displays port configuration information in two port configuration tables, located near the bottom of the window (see figure 57):

- CO Configuration—Displays certain G.SHDSL port parameters for the indicated G.SHDSL port on the T-DAC (see "CO Configuration table" on page 95).
- CPE Configuration—Displays certain G.SHDSL port configuration parameters for the G.SHDSL CPE device remotely connected to the specified G.SHDSL port on the T-DAC (see "CPE Configuration table" on page 97).

> **Note** The CPE Configuration table will only appear when the T-DAC G.SHDSL port has established a link to the remotely connected CPE device.

The two tables display port parameters and operator-configurable port parameters in one of two modes:

- Display-only mode—You can view all the parameter values, but can not define any parameter values (see figure 57).

> **Note** Clicking on the **Change Config** button (see figure 57) changes mode from display-only to change mode. Clicking on the **Cancel** button returns to display-only mode.

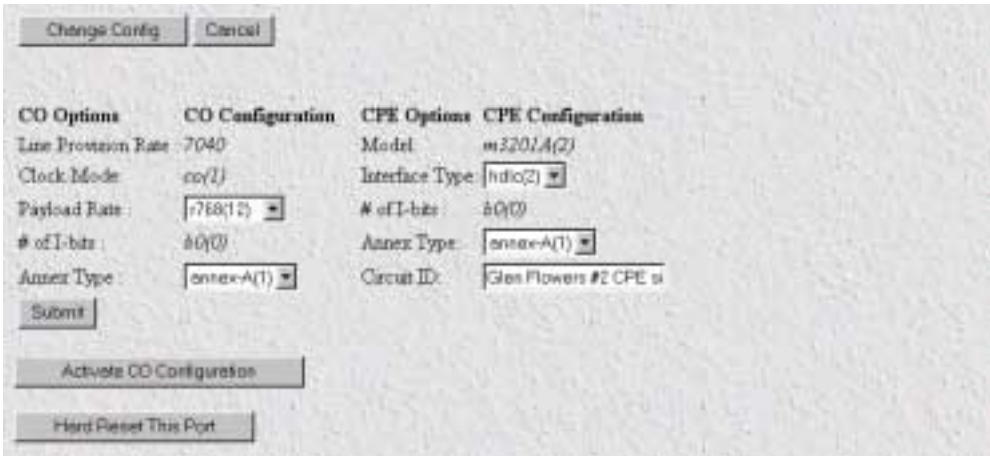


Figure 58. G.SHDSL port configuration section in Change mode

- Change mode—You can view all the parameter values and modify the values for some of the parameters (see figure 58). In Change mode, the T-DAC displays a **Cancel** button along with the **Change Config** button. Click **Cancel** to display the tables in display-only mode. In Change mode, clicking on the **Change Config** button refreshes the display. When you click the **Change Config**, the T-DAC retrieves parameter values currently stored in DRAM and displays them on the page. Any configurable parameter values entered or selected since you last clicked [submit] will be overwritten with values retrieved from DRAM. When monitoring operating status or statistics, or when defining new values for configurable parameters, use this button to update the display. You can watch any changes take place as they are reflected on the G.SHDSL port status display.

Change Config button

Click the **Change Config** button to display the Port Configuration tables in Change mode. In Change mode, clicking on the **Change Config** button refreshes the display. When you click the **Change Config**, the T-DAC retrieves parameter values currently stored in DRAM and displays them on the page. Any configurable parameter values entered or selected since you last clicked [submit] will be overwritten with values retrieved from DRAM. When monitoring operating status or statistics, or when defining new values for configurable parameters, use this button to update the display. You can watch any changes take place as they are reflected on the G.SHDSL port status display.

Cancel Button

The **Cancel** button only appears when the G.SHDSL Port Details page is displayed in change mode. In change mode, the T-DAC displays the **Cancel** button next to the **Change Config** button, above the Port Configuration tables. To return to display-only mode, click the **Cancel** button. When you click the **Cancel** button, the T-DAC will re-display the Port Configuration tables in display-only mode.

CO Configuration table

The CO Configuration table (see figure 57 on page 94) shows the following parameters:

- **Line Provision Rate** [**gshDSLLineProbeRate**]—Display-only. Indicates the recommended line rate calculated by the T-DAC's Line Probe (an on-board line rate provisioning tool). For more information about the Line Probe, see the section entitled "G.SHDSL Line Provision page"

Note The Line Provision Rate parameter label also functions as a hyperlink. Click the Line Provision Rate hyperlink to open the G.SHDSL Line Provision window (see "G.SHDSL Line Provision window" on page 103).

- **Clock Mode** [**gshDSLClockMode**]—Indicates whether the clocking for this G.SHDSL link is provided and controlled by the T-DAC or the remotely connected CPE device.
- **Payload Rate** [**gshDSLPayloadRate**]—Defines the payload rate (i.e. data rate as opposed to line rate) for this G.SHDSL link. The following values of Payload Rates may be defined for T-DAC G.SHDSL ports:

- r192(3)	- r256(4)	- r320(5)	- r384(6)	- r448(7)	- r512(8)
- r576(9)	- r640(10)	- r704(11)	- r768(12)	- r832(13)	- r896(14)
- r960(15)	- r1024(16)	- r1088(17)	- r1152(18)	- r1216(19)	- r1280(20)
- r1344(21)	- r1408(22)	- r1472(23)	- r1536(24)	- r1600(25)	- r1664(26)
- r1728(27)	- r1792(28)	- r1856(29)	- r1920(30)	- r1984(31)	- r2048(32)
- r2112(33)	- r2176(34)	- r2240(35)	- r2304(36)	- r2368(37)	- r2432(38)
- r2496(39)	- r2560(40)	- r2624(41)	- r2688(42)	- r2752(43)	- r2816(44)
- r2880(45)	- r2944(46)	- r3008(47)	- r3072(48)	- r3136(49)	- r3200(50)
- r3264(51)	- r3328(52)	- r3392(53)	- r3456(54)	- r3520(55)	- r3584(56)
- r3648(57)	- r3712(58)	- r3776(59)	- r3840(60)	- r3904(61)	- r3968(62)
- r4032(63)	- r4096(64)	- r4160(65)	- r4224(66)	- r4288(67)	- r4352(68)
- r4416(69)	- r4480(70)	- r4544(71)	- r4608(72)	-	-

- **# of I-Bits** [**gshDSLIbitSel**]—Defines the number of I bits transmitted in each G.SHDSL frame. The following values may be defined:
  - b0(0)
  - b1(1)
  - b2(2)
  - b3(3)
  - b4(4)
  - b5(5)
  - b6(6)
  - b7(7)

- Annex Type [gshDSLAnnexSel]—Defines the Annex type to be used on the link connected to this port. The following values may be defined:
  - annex-A(1)—Typically used in North America
  - annex-B(2)—Typically used outside North America
- **Enable EOC [gshDSLEOCEnabled]**—Defines whether the T-DAC can modify the remote CPE configuration by downloading configurable port parameters to the remotely connected CPE device over the G.SHDSL link. The following values may be defined:
  - Yes(1)—Enable remote CPE configuration
  - No(0)—Disable remote CPE configuration

CPE Configuration table

The CPE Configuration Table appears on the right side of the page. The table shows certain G.SHDSL Parameters for the CPE device remotely connected to the selected G.SHDSL port on the T-DAC. The T-DAC will automatically retrieve the parameter values from the CPE every three minutes and update this table. The table comprises two columns. The column labeled CPE Options shows the parameter names. The column labeled CPE Configuration shows the corresponding current value for each parameter. The table displays the following parameters:

- **Model [gsRMModelCode]**—Indicates the Patton model number of the remotely connected CPE device. One of the following values will be displayed:
  - notKnown(200)
  - m3201A(2)
  - m3201(3)
  - m3241(7)
  - m2157(6)
  - m2156(5)
  - m3086-C(4)
  - m3086-D(10)
  - m3086-K(8)
  - m3086-F(9)

Interface Type [gsRMInterfaceType]—Defines the frame layer protocol the CPE device will use when encapsulating the data received on the G.SHDSL link for forwarding on another link. One of the following values may be defined:

- hdlc(2)
- atm(1)

# of I-bits [gsRMIbitRate]—Indicates the number of I bits transmitted in each G.SHDSL frame. One of the following values will be displayed:

- b0(0)
- b1(1)
- b2(2)
- b3(3)
- b4(4)
- b5(5)
- b6(6)
- b7(7)

- **Annex Type [gsRMAnnex]**—Defines the Annex type to be used on the link connected to this port. The following values may be defined:
  - annex-A(1)—Typically used in North America
  - annex-B(2)—Typically used outside North America
- **Circuit ID [gsRMCircuitID]**—Initially copied from the T-DAC port configuration. The Circuit ID parameter provides a way for you to define a free-text name (character string) that identifies each circuit (link) connected to the T-DAC. Although the table display is limited to 20 characters at a time, the T-DAC supports Circuit IDs of up to 40 characters long. The recommended way to use this field is to design a structured mnemonic naming convention scheme for your application. For example, A DSL service provider might identify each of the T-DAC's G.SHDSL circuits using a subscriber ID (for example: *billybob@rednet.net*), for the subscriber to which the circuit connects. Other examples might be to use a combination of user location and sequence number (*dallas666* for example), or to use subscriber account numbers.

Additional CPE parameters

When the Port configuration tables are in display mode, the following CPE Loop Status parameters will appear in the CPE Parameters table. The CPE Loop Status parameters described below will not appear when the Port Configuration tables are in change mode.

- **Software Loop State [gsRMIntfLoopState]**—Indicates the current loopback state for the CPE device remotely connected to this G.SHDSL port on the T-DAC One of the following values will be displayed:
  - off(0)—No loopback
  - LineLoop(10)—The CPE's G.SHDSL port is operating in line loopback mode as shown in figure 59.

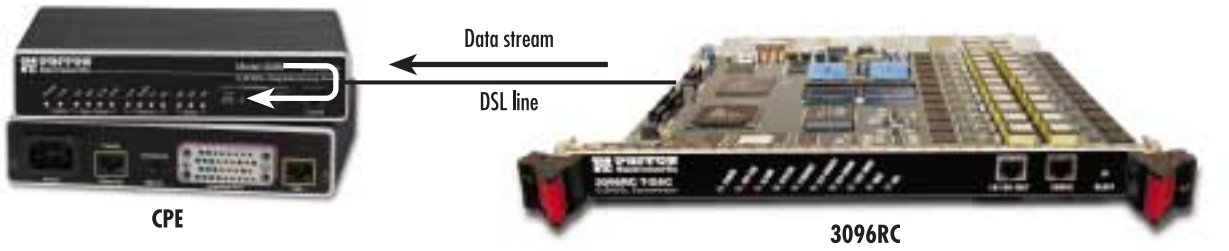


Figure 59. CPE line loopback

When the T-DAC's G.SHDSL port transmits data to CPE the CPE will loop the data back to the T-DAC.

- LocalLoop(11)—The CPE's G.SHDSL port is operating in local loopback mode as shown in figure 60.

Figure 60. CPE local loopback

When the CPE is in Local Loop mode (see figure 60), the T-DAC can communicate with the CPE for management information. However the CPE cannot receive user data from the T-DAC.

Hardware Loop Status Parameters

The CPE Parameters table will only display Hardware Loop Status parameters when the remotely connected CEP device is a Patton Model 3086. The Hardware Loop Status parameters indicate the state of the *Test Modes* toggle switches located on the Model 3086 front panel (see figure 61).

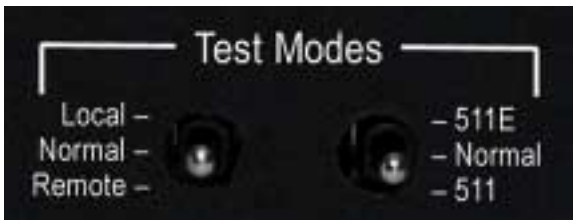


Figure 61. Model 3086 front panel test mode switches

- **Pattern State** [**gsRM511State**]—Indicates the currently selected position of the right-most Test Mode toggle switch on the 3086 front panel. One of the following values will be displayed:
  - Idle—No test pattern is in use.
  - ser511(1)—511 test pattern
  - ser511E(2)—511E test pattern

- **Local Loop State [gsRMLLBState]**—Indicates whether the 3086 CPE modem is operating in local loopback mode. Reflects the currently selected position of the left-most Test Mode toggle switch on the 3086 front panel. One of the following values will be displayed:
  - Idle—The switch is in the Normal position. The 3086 is not operating in local loopback mode.
  - Active—The switch is toggled to the top position. The 3086 is operating in Local Loop mode as shown in figure 60.
- Remote Loop State [gsRMRLBState] Display Only. Indicates whether the 3086 CPE modem is operating in Remote Loopback mode. Reflects the currently selected position of the left-most Test Mode toggle switch on the 3086 front panel. One of the following values will be displayed:
  - Idle—The switch is in the Normal position. The 3086 is not operating in remote loopback mode.
  - Active—The switch is toggled to the bottom position. The 3086 is operating in Remote Loopback mode as shown in figure 62.

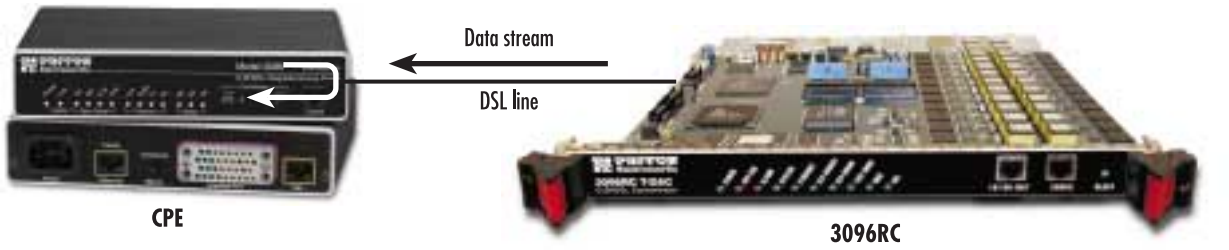


Figure 62. CPE remote loopback

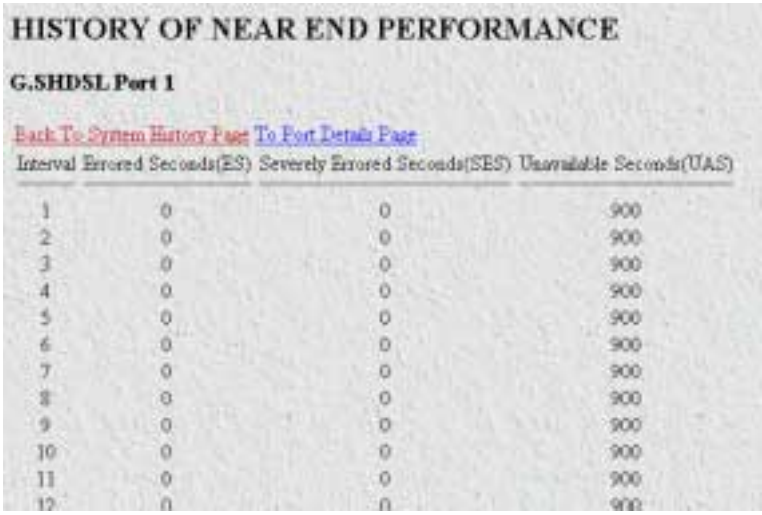
Saving your work

Once you have defined your desired values for of the configurable parameters shown in the G.SHDSL port configuration tables, you must click the **Submit Query** button (see figure 58) to save your settings into volatile DRAM. Once you click the button, the T-DAC will implement the new parameter values immediately.

Note To save your changes persistently (i.e. through a power cycle), you must visit the T-DAC HOME page, and click the **Save Current Configuration** button. When you click the **Save Current Configuration** button, the T-DAC will copy the configuration currently stored in volatile DRAM into non-volatile Flash memory for persistent storage.

Hard Reset This Port button

When you click the **Hard Reset This Port** button (see figure 58), the T-DAC will reset the port hardware for the the G.SHDSL port indicated in the page title. When the value of State for this G.SHDSL port is error(5) (displayed on the G.SHDSL Port Configuration page), you can click this button to clear the error condition for the port.


HISTORY OF NEAR END PERFORMANCE

G.SHDSL Port 1

Back To System History Page To Port Details Page

Interval	Errored Seconds(ES)	Severely Errored Seconds(SES)	Unavailable Seconds(UAS)
1	0	0	900
2	0	0	900
3	0	0	900
4	0	0	900
5	0	0	900
6	0	0	900
7	0	0	900
8	0	0	900
9	0	0	900
10	0	0	900
11	0	0	900
12	0	0	900

Figure 63. History of Near-End Performance window

G.SHDSL Port History of Near-End Performance window

For each of the T-DAC 16 G.SHDSL ports, the T-DAC collects port error statistics in 15-minute intervals for the most recent 24-hour period. The T-DAC discards port statistics information more than 24 hours old. The G.SHDSL Port History of Near End Performance page (see figure 63) displays a record of the errors counted during the last 24 hours for the single G.SHDSL port indicated at the top of the window (*G.SHDSL Port 1* in figure 63).

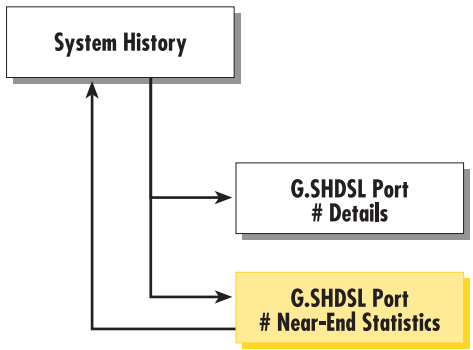


Figure 64. Links to and from the G.SHDSL Port History of Near End Performance window

You can reach the G.SHDSL Port History of Near End Performance in one of the following ways (see map in figure 64):

- To display the G.SHDSL Port History of Near End Performance page, on the G.SHDSL Port Details page click the History Details hyperlink.
- To display the G.SHDSL Port History of Near End Performance page, on the System History web management page in the gshDSL history table, find the column for port you wish to view, then click the History hyperlink for the port you wish to view.

The G.SHDSL Port History of Near End Performance window also provides hyperlinks for returning to the System History and Port Details windows as shown in figure 64 on page 101. The following paragraphs describe the contents of the G.SHDSL Port History of Near End Performance window.

Back To System History Page hyperlink

Click the Back To System History Page link (see figure 63 on page 101) to display the System History window. For a complete description of the System History window, see Chapter 5, "System History" on page 33.

To Port Details Page hyperlink

Click the To Port Details Page link (see figure 63 on page 101) to display the Port Details window. For a complete description of The Port Details window, see section "G.SHDSL Port Details window" on page 87.

Error Statistics table

The G.SHDSL Port History of Near End Performance window displays G.SHDSL Port error statistics in a table of 96 rows. Each row shows error statistics counted during a 15-minute interval, starting with the most recent 15-minute interval (at the top of the page) and moving chronologically backward as you scroll down the page. The first row (row 1) shows the most recent 15-minute interval, Interval number 1. The last row (row 96) shows the oldest 15-minute interval, Interval number 96. (15 minutes x 96 rows = 24 hours).

- **G.SHDSL Port x [gshDSLIntervalNumber]**—Indicates the number of the completed 15 minute interval. The Interval Number may range from 1 to 96, where 1 is the most recently completed 15 minute interval and 96 is the least recently completed 15 minute interval.

Columns in the Error Statistics table show the recorded values for the following G.SHDSL port statistics:

- **Errored Seconds (ES) (historyESgshDSL)**—Indicates the total cumulative number of seconds in which there were one or more FIFO errors on this port during the 15-minute interval.
- **Severely Errored Seconds (SES) (historySESgshDSL)**—Indicates the total cumulative number of seconds in which there were one or more CRC errors on this port during the 15-minute interval. The T-DAC will not increment the SES count for this port when the T-DAC is incrementing the Unavailable Seconds count.
- **Unavailable Seconds (UAS) (historyUASgshDSL)**—Indicates the total cumulative number of seconds that the G.SHDSL port was unavailable during the 15-minute interval. Total cumulative time in seconds that the link state for this port has been down(0). The UAS counter is incremented under the following criteria.
  - The port state must be datamode(1) and the port link state must have been up(1) for 5 seconds or more.
  - When the port state changes to down(0) the 3096RC will begin counting UAS. The 3096RC will not increment ES or SES during the UAS count.

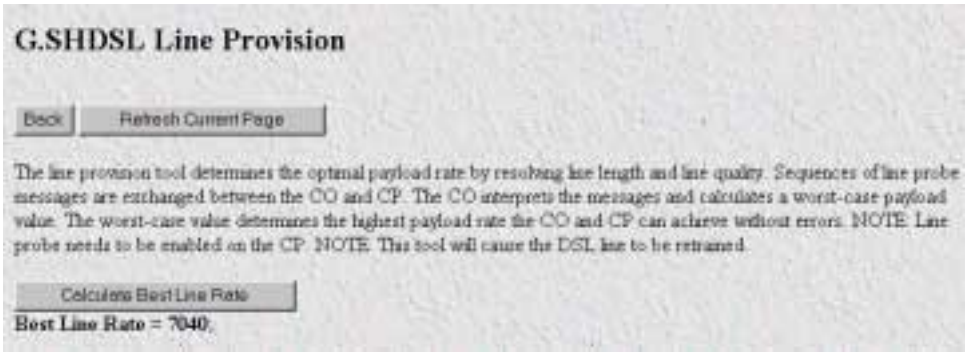


Figure 65. G.SHDSL Line Provision window

G.SHDSL Line Provision window

The G.SHDSL Line Provision window provides an automated tool for calculating the optimum payload rate the G.SHDSL link connected to this port. The line provision tool determines the optimal payload rate by resolving line length and line quality. The CO and CP exchange sequences of line probe messages. The CO interprets the messages and calculates a worst-case payload value. The worst-case value determines the highest payload rate the CO and CP can achieve without errors.

Note Line probe must be enabled on the CP.

Note This tool will cause the DSL line to be retrained.

Back button

The **Back** button (see figure 65) provides a hyperlink to the previously displayed G.SHDSL Port Details page.

Refresh Current Page button

The **Refresh Current Page** button (see figure 65) refreshes the display. After clicking the **Calculate Best Line Rate** button, click the **Refresh Current Page** button often to update the current operating status of the tool, and to display the calculated rate when the tool has completed its calculations.

Calculate Best Line Rate button

Click the **Calculate Best Line Rate** button (see figure 65) to activate the tool. The T-DAC will compute the best line rate for the link given current conditions. During the procedure, the button will disappear, and the page will transition through the following displays:

WORKING.....idle(0)

WORKING.....training(2)

Once the calculations are completed the button will reappear, and the page will display calculated rate, as shown below:

Best Line Rate = 7040

Cancel button

Clicking the **Cancel** button cancels line probe operation.

Chapter 10 Ethernet

Chapter contents

Introduction

The 3096RC T-DAC Ethernet window (see figure 66) provides Ethernet statistics and management and statistical information. The Ethernet window also displays the current values of certain variables from the T-DAC's message information base (MIB) (see RFC 1643 for descriptions for these MIB variables).

Click on the Ethernet link in the T-DAC configuration menu pane to open the Ethernet window.

Figure 66. T-DAC Ethernet window

Ethernet window

The following sections describe the contents of the Ethernet window.

Alignment Errors (dot3StatsAlignmentErrors)

A count of frames received that are not an integral number of octets in length and do not pass the FCS check. The count represented by an instance of this object is incremented when the alignmentError status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions obtain are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.

FCS Errors (dot3StatsFCSErrors)

A count of frames received that are an integral number of octets in length but do not pass the FCS check. The count represented by an instance of this object is incremented when the frameCheckError status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions obtain are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC."

Single Collision Frames (dot3StatsSingleCollision Frames)

A count of successfully transmitted frames for which transmission is inhibited by exactly one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts, ifOutMulticastPkts, or ifOutBroadcastPkts, and is not counted by the corresponding instance of the dot3StatsMultipleCollisionFrames object.

Multiple Collision Frames (dot3StatsMultipleCollisionFrames)
The number of successfully transmitted frames for which transmission is inhibited by more than one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts, ifOutMulticastPkts, or ifOutBroadcastPkts, and is not counted by the corresponding instance of the dot3StatsSingleCollisionFrames object.

SQE Test Errors (dot3StatsSQETestErrors)
A count of times that the SQE TEST ERROR message is generated by the PLS sublayer. The SQE TEST ERROR message is defined in section 7.2.2.2.4 of ANSI/IEEE 802.3-1985 and its generation is described in section 7.2.4.6 of the same document.

Deferred Transmissions (dot3StatsDeferredTransmissions)
The number of times for which the first transmission attempt is delayed because the medium is busy. This number does not include frames involved in collisions.

Late Collisions (dot3StatsLateCollisions)
The number of times that a collision is detected later than 512 bit-times into the transmission of a packet. Five hundred and twelve bit-times corresponds to 51.2 microseconds on a 10 Mbps system. A (late) collision included in a count of late collisions is also considered as a (generic) collision for purposes of other collision-related statistics.

Excessive Collisions (dot3StatsExcessiveCollisions)
The number of frames in which transmission failed due to excessive collisions.

Other Errors (dot3StatsInternalMacTransmitErrors)
The number of frames for which transmission fails due to an internal MAC sublayer transmit error. A frame is only counted if it is not counted by the corresponding instance of either the dot3StatsLateCollisions object, the dot3StatsExcessiveCollisions object, or the dot3StatsCarrierSenseErrors object. The precise meaning of the count represented by an instance of this object is implementation-specific. In particular, an instance of this object may represent a count of transmission errors on a particular interface that are not otherwise counted.

Carrier Sense Errors (dot3StatsCarrierSenseErrors)
The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame. The is incremented at most once per transmission attempt, even if the carrier sense condition fluctuates during a transmission attempt.

Received Frames Too Long (dot3StatsFrameTooLongs)
The number of frames received that exceed the maximum permitted frame size. The count is incremented when the frameTooLong status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions obtain are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.

Other Received Errors (dot3StatsInternalMacReceiveErrors)
The number of frames in which reception fails due to an internal MAC sublayer receive error. A frame is only counted if it is not counted by either the dot3StatsFrameTooLongs object, the dot3StatsAlignmentErrors object, or the dot3StatsFCSErrors object. The precise meaning of the count represented by an instance of this

object is implementation-specific. In particular, an instance of this object may represent a count of receive errors on a particular interface that are not otherwise counted.

Chip Set ID (dot3StatsEtherChipSet)

Identifies the chipset to implement the Ethernet interface. The chipset ID identifies the chipset which gathers the transmit and receive statistics and error indications.

Chapter 11 IP Filtering

Chapter contents

Introduction

The 3096RC T-DAC provides an IP filtering system that enables you to set up security for the internal management system.

Each filter is a defined list of parameters based upon attributes in the IP, TCP, and UDP headers. There are two major steps to filter creation: first defining the filter, then applying it to a user connection. The same filter can be shared by several users.

The T-DAC enables 20 separate filters to be defined, of which up to 10 can be used during a single user connection. Since the IP connections in the T-DAC are only for the superuser and the monitor user, these will be the only two users. The application of the filters is done on the Filter IP main web page.

Filter IP main window

The Filter IP window provides the means for you to manage the T-DAC's IP Filtering sub-system. Click the on Filter IP link under the Configuration Menu to display the Filter IP main window (see figure 67).

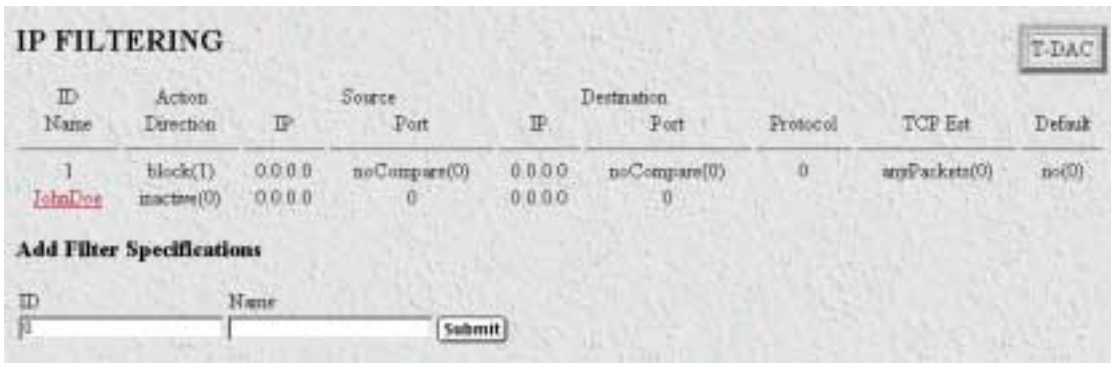


Figure 67. Filter IP main window

The Filter IP page provides a link to the Filter window as shown in figure 68.

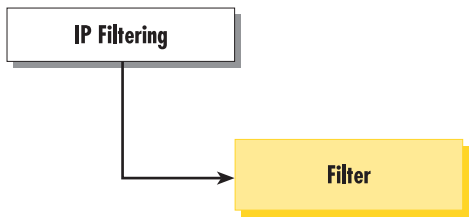


Figure 68. Filter IP diagram

The IP Filtering main window enables you to do the following:

- View the IP FILTERING table which displays the currently configured filters (see section "IP FILTERING table" on page 111)
- Use the Add Filter Specifications section to define a new filter ID and assign a filter name (see section "Defining a filter" on page 112)
- Use the Add Filter Specifications section to delete a filter (see section "Deleting a filter" on page 115).

IP FILTERING table

The following sections describe the IP FILTERING table.

ID

Each filter is assigned an identifier (a number between 1 and 20 inclusive) when it is created.

Name

This is the name of the filter.

Action

Specifies the action to effect the packet. The action decides whether to block or pass the packet. The following options are available:

- **pass(0)**—If pass is selected, checking will continue on to other filters until either a match occurs, a block occurs, or there are no more filters remaining to check.

  Note If there are any applied PASS filters, then at least one of them must match or the packet will be dropped.

- **block(1)**—If a filter has block set and the filter matches the block, the packet is discarded and no further processing is done.
- **wrap(2)**—All packets received on the specified link will be encapsulated in an extra IP header as defined in RFC 2003. The destination IP address of the wrapper is given by the destination IP setting in the filter. The source IP address of the wrapper is the ethernet address of the T-DAC.

  Note All wrap filters are inbound only.

Direction

Specifies the direction of the filter (that is, whether it applies to data packets inbound or outbound from the T-DAC). The filter only applies to the *Superuser* and the *Monitor* users through the Ethernet interface. (Since the mDSL G.SHDSL modem and WAN connections function as a transparent pipe, neither of the two users can utilize these interfaces, only the Ethernet interface.) The following options are available:

- **inactive(0)**—Disables filter operation
- **inbound(1)**—Relates to packets coming into the T-DAC
- **outbound(2)**—Relates to packets leaving the T-DAC
- **both(3)**—Specifies both inbound and outbound operation

Source IP

This is the Source IP address in the IP header, it is used when comparing a packet's source address.

Source Port

Specifies the source port number (TCP or UDP) that the access server T-DAC compares. The source port Action (see Action (filterIpSourcePortCmp) next) action will determines how the source port is treated.

whether the source port in the IP packet is not compared, equal, less than, or greater than the Source Port designated in the filter.

Destination IP
This is the destination IP address in the IP header used when comparing a packet's destination address.

Destination Port
Specifies the destination port number which the T-DAC compares. The destination action functions similarly to the Source Port and its Action defined above.

Protocol
Specifies the IP Protocol number to use for filtering. Some examples of protocol numbers are 1 for ICMP; 6 for TCP; and 17 for UDP. A list of protocol numbers can be found in RFC 1340. A setting of 0 disables processing based on protocol number.

TCP Est (Established)
Specifies whether the filter should match only those packets which indicate in the TCP header flags that the connection is established. The following choices are available:

- **anyPackets(0)**—Applies the filter to all packets
- **onlyEstablishedConnections(1)**—Only applies the filter to established TCP connections

Defining a filter

To define a new filter, do the following:

1. Type an ID number in the ID field (see figure 69). The number must not already exist in the IP FILTERING list, and the number must be an integer between 1 and 20
2. Type a name in the Name field. The name must not already exist in the IP FILTERING list.
3. Click on the **Submit Query** button to submit the request. The new filter will appear in the IP FILTERING list.

Figure 69. Add Filter Specifications section of IP Filtering main window

Note Block filters take priority, therefore any applied and matching block filters will drop the packet. Next, pass filters are examined, if PASS filters have been defined, then at least one of them must match or else the packet will be dropped. After the block and pass filters are examined, the WRAP filter, if it exists, will be applied.

4. Click on the name of the newly created filter to display the FILTER parameters window (see figure 70).

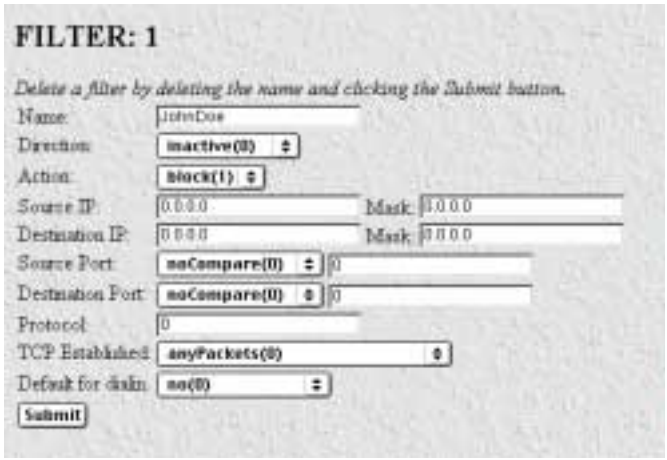


Figure 70. Filter modification window

Note Any changes to a filter take effect immediately upon clicking **Submit Query**. This can aid in troubleshooting a filter profile while the user is online.

The following sections provide detailed descriptions of the parameters.

Name (filterIpName)

This is the name of the filter.

Direction (filterIpDirection)

Specifies the direction of the filter (that is, whether it applies to data packets inbound or outbound from the T-DAC). The filter only applies to the *Superuser* and the Monitor Users through the Ethernet interface. (Since the mDSL G.SHDSL modem and WAN connections function as a transparent pipe, neither of the two users can utilize these interfaces, only the Ethernet interface.) The following options are available:

- **inactive(0)**—Disables filter operation
- **inbound(1)**—Relates to packets coming into the T-DAC
- **outbound(2)**—Relates to packets leaving the T-DAC
- **both(3)**—Specifies both inbound and outbound operation

Action (filterIpAction)

Specifies the action to effect the packet. The action decides whether to block or pass the packet. The following options are available:

- **pass(0)**—If pass is selected, checking will continue on to other filters until either a match occurs, a block occurs, or there are no more filters remaining to check.

Note If there are any applied PASS filters, then at least one of them must match or the packet will be dropped.

- **block**(1)—If a filter has block set and the filter matches the block, the packet is discarded and no further processing is done.
- **wrap**(2)—All packets received on the specified link will be encapsulated in an extra IP header as defined in RFC2003. The destination IP address of the wrapper is given by the destination IP setting in the filter. The source IP address of the wrapper is the ethernet address of the T-DAC.

Note All wrap filters are inbound only.

Source IP (filterIpSourceIp)
This is the Source IP address in the IP header, it is used when comparing a packet's source address.

Source IP Mask (filterIpSourceMask)
This is the Source IP Mask (filterIpSourceMask) used when comparing a packet's source address. Bit positions that are set to 1 will be compared and 0's will be ignored. Thus, a setting of 0.0.0.0 will have the effect of disabling source IP address comparison.

Destination IP (filterIpDestinationIp)
This is the destination IP address in the IP header used when comparing a packet's destination address.

Destination Mask (filterIpDestinationMask)
This is the destination mask used when comparing a packet's destination address. Bit positions that are set to 1 will be compared and 0's will be ignored. Thus, a setting of 0.0.0.0 will have the effect of disabling destination IP address comparison.

Source Port (FilterIpSourcePort)
Specifies the source port number (TCP or UDP) that the access server T-DAC compares. The source port Action (see Action (filterIpSourcePortCmp) next) action will determines how the source port is treated. whether the source port in the IP packet is not compared, equal, less than, or greater than the Source Port designated in the filter.

Action (filterIpSourcePortCmp)
Specifies the Action (filterIpSourcePortCmp) that the T-DAC compares. The source port action determines whether the source port in the IP packet is not compared, equal, less than, or greater than the Source Port designated in the filter.

- **noCompare**(0)—No Comparison to the source port in the IP packet.
- **equal**(1)—The port in the source IP packet is the same
- **lessThan**(2)—The port in the source IP packet is less than
- **greaterThan**(3)—The port in the source IP packet is greater than

Destination Port (filterIpDestinationPort)
Specifies the destination port number which the T-DAC compares. The destination action functions similarly to the Source Port and its Action defined above.

Action (filterIpDestinationPortCmp)

Specifies the action (TCP or UDP) which the T-DAC compares. The destination action will determine how the destination port is treated.

- **noCompare(0)**—No Comparison to the destination port in the IP packet.
- **equal(1)**—The port in the destination IP packet Is the same
- **lessThan(2)**—The port in the destination IP packet is less than
- **greaterThan(3)**—The port in the destination IP packet is greater than

Protocol (filterIpProtocol)

Specifies the IP Protocol number to use for filtering. Some examples of protocol numbers are 1 for ICMP; 6 for TCP; and 17 for UDP. A list of protocol numbers can be found in RFC 1340. A setting of 0 disables processing based on protocol number.

TCP Established (filterIpTcpEstablished)

Specifies whether the filter should match only those packets which indicate in the TCP header flags that the connection is established. The following choices are available:

- **anyPackets(0)**—Applies the filter to all packets
- **onlyEstablishedConnections(1)**—Only applies the filter to established TCP connections

Deleting a filter

To delete a filter, do the following:

1. Type the ID number of the filter you want to delete in the ID field (see figure 69 on page 112).
2. Leaving the Name field blank, click on the **Submit Query** button to delete the filter.

Chapter 12 **Frame Relay**

Chapter contents

Introduction

The Model 3096RC T-DAC offers in-band management over Frame Relay or PPP (point-to-point protocol) links in the T1/E1 channels. The T-DAC's Frame Relay subsystem manages the in-band management function over Frame Relay links. This chapter discusses in-band management using Frame Relay (for PPP, see chapter "PPP" on page 127).

Any T1/E1 WAN link can carry user data, management information, or both. To set up in-band management over Frame Relay, you will allocate selected DS0s for management channels. You can select any number of DS0s from any of the T1 or E1 links to carry management information instead of user data.

Configuring a Frame Relay link

The most common configuration is setting up the T-DAC as a DCE and connecting to a provider's Frame switch via a T1/E1 line. In this application, the T-DAC will establish a point-to-point link via one or more DLCI's or virtual channels. Each DLCI is a pipe with an associated far-end IP address.

A Frame Relay link is configured as follows:

- Selecting a T1/E1 DS0 for management using Frame Relay
- Selecting the correct Frame Relay configuration parameters (LMI)
- Assigning an IP address to the DLCI
- Assigning next-hop routes to the new DLCI

T1/E1 port and DS0 selection

The first stage in setting up a Frame Relay WAN link is configuring one or more DS0s on any T1 or E1 line for Frame Relay in-band management. See chapter "T1/E1 Link" on page 211 for T1/E1 port configuration.

1. Click on the T1/E1 Link under the configuration menu to display the *T1/E1 Link Activity* main window. Select which T1/E1 port will carry the Frame Relay Link, then click on the *View Link* of the selected port.
2. Click on Channel Assignment link to access the WAN Circuit Channel Assignment window. Options for the T1/E1 DS0s displayed on this window are:
   - clear(9). The T1/E1 DS0s carry user data (default)
   - framerelay(3). The selected DS0s will carry management data using Frame Relay
   - ppp(5). The selected DS0s will carry management data using PPP
3. Use the drop down menu to select Frame Relay for the designated management channel(s). Set user data DS0s to *Clear*.
4. Click on the **Submit Query** button for the configuration to take effect.

The Management DS0 IS now active on your T-DAC. The next stage is to configure Frame Relay and IP routing.

The Frame Relay main window

The Frame Relay main window displays diagnostic information about the Frame Relay link, and lists complete statistics/configuration information for each WAN link that has been selected for in-band management over Frame Relay service. Click on **Frame Relay** on the left hand frame to display this window. (see Figure 71).

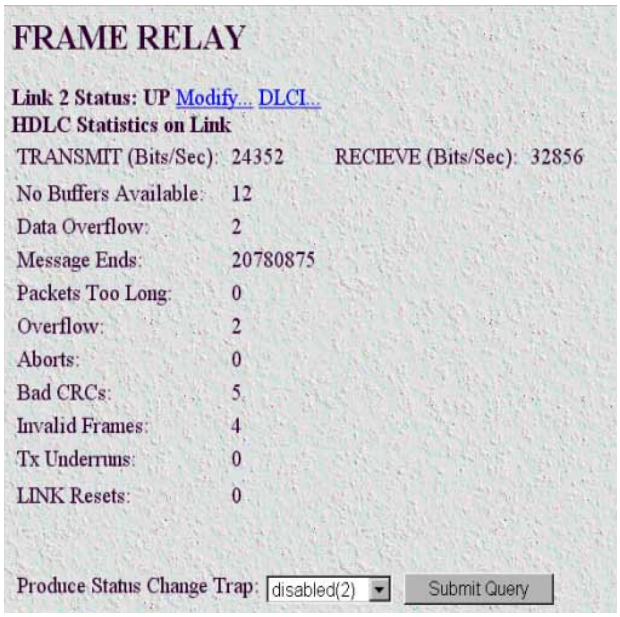


Figure 71. Frame Relay main window

Note If frame relay has not already been configured under T1/E1, this window will only show the Produce Status Change Trap setting.

The Frame Relay main window also has the following links:

- Modify—Clicking on the Modify link enables you to set-up Frame Relay or to change any configuration parameters (see section "DLMI window" on page 122).
- DLCI—The Data Link Connection Identifier (DLCI) provides each PVC with a unique identifier at both the T-DAC and the Frame Relay switch. Within each link (DLMI) there can be multiple Permanent Virtual Circuits (PVC). Each of these PVCs are point-to-point links to remote locations, and define the data path between the T-DAC and the Frame Relay network. Clicking on the DLCI link displays the DLCI window (see "DLCI window" on page 124) that enables you to configure PVCs on the T-DAC.

Link X (frDlcmiIfIndex)

The Data Link Management Interface number.

Status: X (framerelStatus)

This specifies LMI Link Status. If the management DLCI (either DLCI 0 or 1023) is established, then the status will be UP. If the management channel has not been established, the status will indicate DOWN.

HDLC Statistics on Link

The HDLC statistics on the link are defined as follows:

Transmit (Bits/Sec) (framerelTxOctets)
This statistic shows the transmit rate in bits-per-second.

Receive (Bits/Sec) (framerelRxOctets)
This statistic shows the receive rate in bits-per-second.

No Buffers Available (framerelRxNoBufferAvailable)
The number of packets received when no buffers were available.

Data Overflow (framerelRxDataOverflow)
The number of packets received with overflow (as indicated by hardware).

Message Ends (framerelRxMessageEnds)
The number of packets received with message-correct endings. This value increases each time a valid Frame Relay packet is received.

Packets Too Long (framerelRxPacketTooLong)
The number of packets received that were too long.

Overflow (framerelRxOverflow)
The number of packets received with overflow (as indicated by software).

Aborts (FramerelRxAbort)
The number of packets received that were aborted.

Bad CRC (framerelRxBadCrc)
The number of packets received that had bad CRC values.

Invalid Frames (framerelRxInvalidFrame)
The number of packets received that had invalid frames.

Tx Underrruns (framerelTxUnderrun)
The number of times the transmit buffer was not replenished in time to be sent out on the line.

LINK Resets (framerelResets)
Number of times the link management (LMI) was reset.

Produce Status Change Trap (frTrapState)
This feature is not currently implemented.

DLMI window

Each Frame Relay instance with the T-DAC is known as the Data Link Management Interface or DLMI. The T-DAC software currently supports one Frame Relay Link, or DLMI, on each of the T1/E1 WAN ports. Frame Relay has a set of protocols responsible for maintaining the link. This is known as the management link interface or LMI.

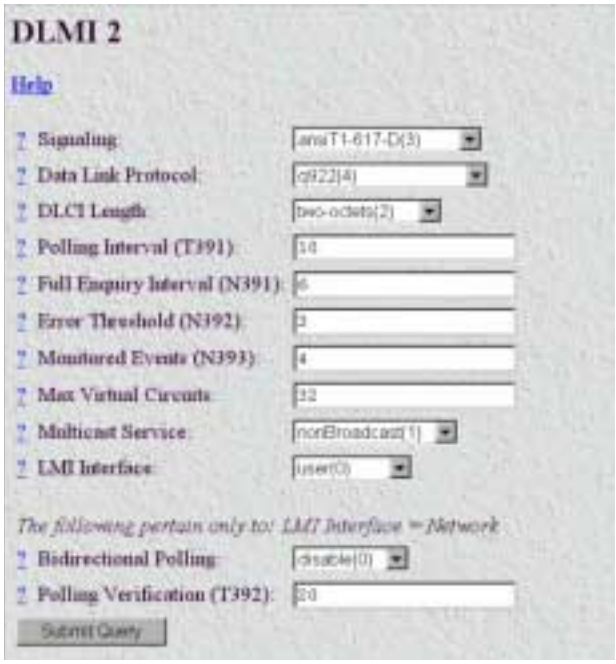


Figure 72. DLMI window

Signalling (frDlcmiState)

Inband signalling used to communicate link and PVC status between the User equipment and the Network equipment. LMI is the generic term used to indicate Frame Relay signaling, however the three specific types of signaling are:

- LMI Frame Relay Forum Implementation agreement. Uses DLCI = 1023 for management
- Annex D. ANSI T1.617 Uses DLCI = 0 for management
- Annex A. ITU Q.933 Uses DLCI = 0 for management

Data Link Protocol (frDlcmiAddress)

The layer 2 link protocol for Frame Relay is LAPF, otherwise referred to as Q.922. The factory default of q922(4) will be the most common.

DLCI Length (frDlcmiAddressLen)

The DLCI identifies the virtual connection on the bearer channel for the Frame Relay Interface. The factory setting of two-octets(2) represents 10-bit addressing. Your T-DAC can support a maximum of 32 separate PVCs or virtual channels per Frame Relay link.

Polling Interval (T391)(frDlcmiPollingInterval)
Each side of the Frame Relay interface, the Network side and the User side, communicate status. T391 is the number of seconds between subsequent Status Enquiry messages. An Error Count is logged if no response from the previous Status Enquiry message was received during the T391 interval. The default value is 10.

Full Enquiry Interval (N391)(frDlcmiFullEnquiryInterval)
Status Enquiry messages are of two different varieties: 1) Link Integrity Verification, which simply exchange sequence numbers between peers and 2) Full Status messages, which is a request from the peer for the list of all active/inactive PVCs. The default is 6.

Error Threshold (N392)(frDlcmiErrorThreshold)
N392 is the number of errors (T392 and T391 timeouts and sequence number errors) before action is taken. Action consists of changing all the PVCs from active to inactive. N392 must be less than or equal to N393. The default value is 3.

Monitored Events (N393)(frDlcmiMonitoredEvents)
Expected and unexpected events are counted up till the Event Count reaches N393, whereupon the Event Count is cleared and the Error Threshold Count is cleared. Events consist of timer (T391 and T392) expirations and received Status Enquiry messages. N393 must be greater or equal to N392. The default value is 4.

MultiCast Service (frDlcmiMulticast)
Not currently implemented.

Max Virtual Circuits (frDlcmiMaxSupportedVCs)
The maximum number of PVCs determines the amount of internal resources are allocated for the Frame Relay system. The default value is 32.

LMI Interface (frDlcmiInterface)
LMI is used in the generic sense as an in-band signaling system. The signaling is slightly different depending on which end of the Frame Relay Interface it is, or in other words its orientation. The User end issues periodic STATUS ENQUIRY messages and waits for a STATUS reply from the Network. The USER setting is correct if the T-DAC is a DCE connecting to a Frame Relay network. It is possible to configure an T-DAC to "look" like a Frame Relay Network. By setting the LMI Interface to NETWORK, you can connect another Frame Device directly to the T-DAC. This is also the setting if you were to connect two T-DAC back-to-back without the benefit of an established Frame Relay network.

Bidirectional Polling (frDlcmiPollingBiDir)
Bidirectional Polling pertains only to the Network LMI side. If enabled, the Network LMI issues STATUS ENQUIRY messages and waits for a STATUS reply from the User.

Polling Verification (T392)(frDlcmiPollingVerification)
Polling Verification pertains only to the Network LMI side. It is the amount of time permitted without receiving a STATUS ENQUIRY message from the User before Counting an Error.

DLCI window

The Data Link Connection Identifier (DLCI) provides each PVC with a unique identifier at both the T-DAC and the Frame Relay switch. Within each link (DLMI) there can be multiple Permanent Virtual Circuits (PVC). Each of these PVCs are point-to-point links to remote locations, and define the data path between the T-DAC and the Frame Relay network.

Within each DLMI are one or more Data Link Channel Identifier (DLCIs). This is the identification of a PVC within the Frame Relay link.

There will be at least one PVC automatically installed. This is the management DLCI or LMI. This DLCI, often DLCI 0, is the communication channel between the T-DAC and the Frame Relay network switch. This management channel communicates configuration and health information of the Frame Relay link. See Figure 73.

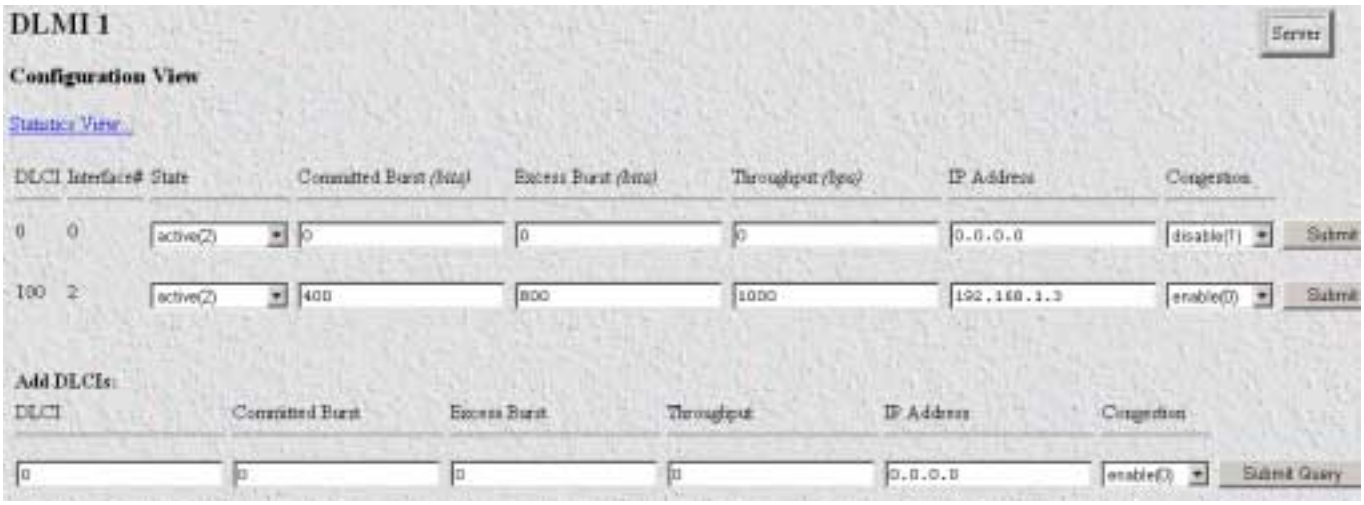


Figure 73. DLMI—Configuration View window

DLCI (frCircuitDlci)

The Data Link Connection Identifier (DLCI) for this virtual circuit.

Note DLCIs can automatically appear if your Frame Relay Service provider has already configured your link. In this case, all you will need to enter is the IP address of the router at the far end of the link.

Interface # (FrameIPInterfaceNum)

The interface number assigned to a DLCI. This is a variable number which is assigned from a resource pool within the T-DAC.

State (frCircuitState)

This is the state of the interface with the following definitions:

- invalid(1)—Use this setting to delete DLCI's on your T-DAC's configuration view. To delete a DLCI, simply set the state to invalid(1) and Submit Query. Note: A deleted DLCI will reappear if your service pro-

vider's Frame Relay switch is still configured to recognize that DLCI. This occurs after a Frame Relay Full Status Enquiry.

- active(2)—The link is up and passing data. This is the desired condition of the link.
- invalid(3)—The link is down and not passing data. Reasons for this may be your service provider hasn't enabled your service or the link is not yet connected to your T-DAC.
- needIPaddr(4)—This is when the IP address needs to be entered for this DLCI.
- wait4peer(5)—In this state, the Link is waiting for the far end to synchronize.

Committed Burst (bits) (frCircuitCommitedBurst)

This specifies the committed data rate for the link in bits-per-second.

Excess Burst (bits) (frCircuitExcessBurst)

This specifies the excess data rate for the link in bits-per-second.

Throughput (bits) (frCircuitThroughput)

This specifies the throughput for the link in bits-per-second.

IP Address (FrameIPAddr)

As all of the interfaces on the T-DAC run in un-numbered mode, the IP address to enter is that of the far end router. This is not the IP address of the T-DAC. After the IP address is entered, it will appear as a point-to-point link in the IP routing table with this address.

Congestion (frameEnableCongestion)

This option enables or disables congestion tracking.

- enable(0)—Enables Congestion tracking
- disable(1)—Disables Congestion tracking

Chapter 13 PPP

Chapter contents

Introduction

The Model 3096RC T-DAC offers in-band management over Frame Relay or PPP (point-to-point protocol) links in the T1/E1 channels. The T-DAC's PPP subsystem manages the T-DAC's in-band management function over PPP links. This chapter discusses in-band management using PPP (for Frame Relay, see chapter "Frame Relay" on page 117).

Any T1/E1 WAN link can carry user data, management information, or both. To set up in-band management over PPP, you will allocate selected DS0s for management channels. You can select any number of DS0s from any of the T1 or E1 links to carry management information instead of user data.

T1/E1 port and DS0 selection

The first stage in setting up a Frame Relay WAN link is configuring one or more DS0s on any T1 or E1 line for Frame Relay in-band management. See Chapter 21 for T1/E1 port configuration

1. Click on the T1/E1 Link under the configuration menu to display the T1/E1 Link Activity main window. Select which T1/E1 port will carry the Frame Relay Link then click on the View Link of the selected port.
2. Click on Channel Assigment link to access the WAN Circuit Channel Assignment Page. Options for the T1/E1 DS0s displayed on this page are:
   - clear(9). The T/E1 DS0s carry user data (default)
   - framerelay(3). The selected DSO(s) will carry management data using Frame Relay.
   - ppp(5). The selected DSO(s) will carry management data using PPP
3. Use the drop down menu to select PPP for the designated management channels. Set user data DS0s to *Clear*.

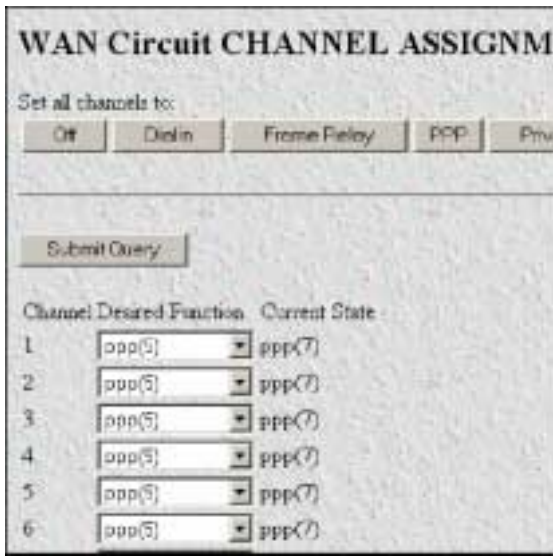


Figure 74. Channel assignment showing PPP config

Once the channel(s) is set to PPP, the PPP negotiation phase will begin. Only one PPP link can be established per WAN link. The bandwidth will be the number of channels using PPP times 64k. For example, if 2 channels are set for ppp(5), the bandwidth will be 2 x 64 kbps or 128 kbps.

4. Click on the **Summit Query** button for the configuration to take effect.

PPP main window

After the WAN has been configured for PPP, the PPP parameters can be configured. Clicking on the PPP link on the left side of the screen shows the PPP main window. This window shows the status of all PPP links and provides links for configuration each link and the default parameters.

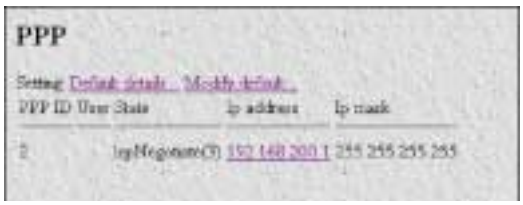


Figure 75. The PPP main window

PPP ID (pppIndex)

This provides a unique identifier for each active PPP link. This is a read only variable and is for display purposes only.

User (pppAuthenticationUsername)

If authentication is used, this is the username used during authentication.

State (pppActState)

This is the current state of the PPP negotiation process.

- restarting(1)—the link is currently restarting due to a configuration change or line error
- connecting(2)—the link is currently connecting
- lcpNegotiate(3)—PPP Lcp negotiation is in progress
- authenticating(4)—Either local or remote side is authenticating the user if enabled
- pppUp(5)—The PPP link is up
- disconnecting(6)—The link is currently disconnecting
- dead(7)—the link is currently dead
- onlineBcp(8)—Bcp has been negotiated and data can be passed across the link
- onlineIpcp(9)—Ipcp has been negotiated and both sides have agreed on Ip addresses and data can be passed across the link

IP Address (pppServiceIpAddress)

The IP address assigned and negotiated for this interface. The default IP address is 192.168.200.1 and should be changed.

IP Mask (pppServiceIpMask)
The IP netmask configured for this link.

Default settings

Clicking on the Default Details… or Modify default… links on the PPP main window brings up the default settings window (see figure 76). These are the default settings each PPP link will take when first initialized. Settings for individual links can be changed (this is described in a later section).

Figure 76. Default settings window

Authentication Technique (pppDefaultAuthenticationTechnique)
Technique to be used for authenticating:

- none(0)—No authentication will be used
- pap(3)—password authentication protocol will be used
- chap(4)—challenge handshake authentication protocol will be used
- chapORpap(5)—chap will be negotiated first, if that fails, pap will be attempted

Authentication Side (pppDefaultAuthenticationSide)
This is the side of the link which will be authenticating:

- local(1)—local server will be authenticating. Remote needs to log into local server.
- remote(2)—remote server will be authentication. Local needs to log into remote server.

Authentication Username (pppDefaultAuthenticationUsername)
This is the username that will be sent to the remote side if the remote machine is authenticating. If the local server is authenticating, the username that the remote sends will be compared to this username. Maximum size is 40 characters.

Authentication Password (pppDefaultAuthenticationPassword)

This is the password that will be sent to the remote side if the remote machine is authenticating. If the local server is authenticating, the password that the remote sends will be compared to this username. Maximum size is 40 characters.

MRU (pppDefaultInitialMRU)

This is the initial maximum received unit that will be negotiated for the link. This could possibly be changed during PPP negotiations.

Link Compression (pppDefaultLinkCompression)

This object enables the PPP link layer address and protocol field compression. When enabled the PPP negotiations will DESIRE link compression but may disable the compression due the other end of the link not accepting link compression. When disabled the PPP negotiations will FORCE no compression on the PPP link.

- enabled(1)—enable link compression
- disabled(2)—disable link compression

Allow Magic Number Negotiation(pppDefaultMagicNumber)

Determines if magic number negotiation should be done

- enabled(1)—enable magic number negotiation
- disabled(2)—disable magic number negotiation

Compression (pppDefaultIpCompression)

If none(1) then the local node will not attempt to negotiate any IP compression option. Otherwise, the local node will attempt to negotiate compression mode indicated by the enumerated value. Changing this object will have effect when the link is next restarted.

- none(1)—do not negotiate Ip compression negotiated
- vj-tcp(2)—van-jacobson TCP/IP header compression will be negotiated per RFC 1332.

PPP link window

Clicking on the IP address link on the main PPP page will bring up the PPP Link window. This gives a status of the current link.

Figure 77. PPP Link Window

HDLC statistics on link

Link (frDlcmiIfIndex)
The HDLC link management number

Status (framerelStatus)
The status of the HDLC link. If HDLC management has been established for this link the status will be *UP*.

TRANSMIT(framerelTxOctets)
Transmit rate in bits per second.

RECEIVE (framerelRxOctets)
Receive rate in bits per second.

No Buffers Available (framerelRxNoBufferAvailable)
The number of packets received when no receive buffers were available.

Data Overflow (framerelRxDataOverflow)
The number of packets received with overflow indicated by the hardware.

Message Ends (framerelRxMessageEnds)
The number of packets received with message-correct endings. This value increases each time a valid packet is received.

Packets Too Long (framerelRxPacketTooLong)
The number of packets received that were too long.

Overflow (framerelRxOverflow)
The number of packets received with overflow indicated by software.

Aborts (framerelRxAbort)
The number of packets received that were aborted.

Bad CRCs (framerelRxBadCrc)
The number of packets received with bad CRC values.

Invalid Frames (framerelRxInvalidFrame)
The number of packets received with invalid frames.

Tx Underruns (framerelTxUnderrun)
The number of times the transmit buffer was not replenished in time to be sent out on the line.

LINK Resets (framerelResets)
Number of times the link was reset.

Link Configuration

PPP Protocol (pppDesiredFunction)
This is the actual desired kind of ppp protocol

- ppp(1) —point-to-point protocol
- ppp-bcp(2)—bridge control protocol

Authentication Technique (pppAuthenticationTechnique)
The login technique to use for authentication.

- none(0)—No authentication will be used
- pap(3)—password authentication protocol will be used
- chap(4)—challenge handshake authentication protocol will be used
- chapORpap(5)—chap will be negotiated first, if that fails, pap will be attempted

Authentication Side (pppAuthenticationSide)
This is the side of the link which will be authenticating

- local(1)—local server will be authenticating. Remote needs to log into local server.
- remote(2)—remote server will be authentication. Local needs to log into remote server.

Authentication username (pppAuthenticationUsername)
This is the username that will be sent to the remote side if the remote machine is authenticating. If the local server is authenticating, the username that the remote sends will be compared to this username. Maximum size is 40 characters.

Authentication password (pppAuthenticationPassword)
This is the password that will be sent to the remote side if the remote machine is authenticating. If the local server is authenticating, the password that the remote sends will be compared to this username. Maximum size is 40 characters.

Security level (pppAccessLevel)
The security level given to this call.

- passthru(1)—allows no access in the configuration screens
- monitor(2)—allows read-only access to the configuration screens
- change(3)—allows full read and write access to the configuration screens

MRU (pppInitialMRU)
Initial setting for Maximum Receive Unit (MRU), used for the PPP negotiation

IP Address (pppServiceIpAddress)
This object defines the IP address which will be used for the ppp link

IP Mask (pppServiceIpMask)
This object defines the IP mask, which will be used for the ppp link

IP Compression (pppIpCompression)
This object defines the IP comprssion for the link

IP Force Next Hop (pppForceNextHop)
This object defines the IP address of the interface, which should be the next hop for the packets—fast routing

Link Compression (pppLinkCompression)
This object enables the PPP link layer address and protocol field compression. When enabled the PPP negotiations will *desire* link compression but may disable the compression due the other end of the link not accepting link compression. When disabled the PPP negotiations will *force* no compression on the PPP link.

- enabled(1)—enable link compression
- disabled(2)—disable link compression

Allow Magic Number Negotiation (pppMagicNumber)
Determines if magic number negotiation should be done

- enabled(1)—enable magic number negotiation
- disabled(2)—disable magic number negotiation

PPP Statistics

Bad Address (pppStatBadAddresses)
The number of packets received with an incorrect address field.

Bad Controls (pppStatBadControls)
The number of packets received on this link with an incorrect control field.

Packets Too Long (pppStatPacketTooLongs)
The number of packets received that have been discarded because their length exceeded the maximum receive unit (MRU).

LCP Statistics

This portion of the Statistics window shows LCP statistics of the PPP link selected.

Local MRU (pppStatLocalMRU)
The current value of the MRU for the local PPP entity. This value is the MRU that the remote entity is using when sending packets to the local PPP entity. This setting becomes active when the link is in the up—able to pass packets—operational state

Remote MRU (pppStatRemoteMRU)
The current value of the MRU for the remote PPP entity. This value is the MRU that the local entity is using when sending packets to the remote PPP entity. This setting becomes active when the link is in the up—able to pass packets operational state.

LCP Authentication (pppStatLcpAuth)
Authentication type used by the dial-in user. The following options are available:

- none(1)
- pap(2)
- chap(3)
- MSChap(4)—not currently implemented

Local ACC Map (pppStatLocalToPeerACCMap)
The current value of the ACC Map used for sending packets from the local unit to the remote unit. The local unit sends this character map to the remote peer modem to ensure that the data being transferred is interpreted correctly. This setting becomes active when the link is in the up—able to pass packets operational state.

Remote ACC Map (pppStatPeerToLocalACCMap)
The current value of the ACC Map used by the remote peer unit when transmitting packets to the local unit. The local unit sends this character map to the remote peer unit to ensure that the data being transferred is interpreted correctly. The remote peer unit combines its ACC Map with the map received from the local unit. This setting becomes active when the link is in the up—able to pass packets—operational.

Local PPP Protocol Comprsn (pppStatLocalToRemoteProtComp)

Indicates whether the local PPP entity will use protocol compression when transmitting packets to the remote PPP entity. This setting becomes active when the link is in the up—able to pass packets—operational state.

These are the available options:

- disabled(0)—PPP compression is disabled
- enabled(1)—PPP compression is enabled

Remote PPP Protocol Comprsn (diStatRemoteToLocalProtComp)

Indicates whether the remote PPP entity will use protocol compression when transmitting packets to the local PPP entity. This setting becomes active when the link is in the up—able to pass packets—operational state These are the available options:

- disabled(0)—PPP compression is disabled
- enabled(1)—PPP compression is enabled

Local AC Comprsn (pppStatLocalToRemoteACComp)

Indicates whether the local PPP entity will use address and control compression (ACC) when transmitting packets to the remote PPP entity. This setting becomes active when the link is in the up—able to pass packets —operational state.

These are the available options:

- disabled(0)—ACC is disabled
- enabled(1)—ACC is enabled

Remote AC Comprsn (pppStatRemoteToLocalACComp)

Indicates whether the remote PPP entity will use address and control compression (ACC) when transmitting packets to the local PPP entity. This setting becomes active when the link is in the up—able to pass packets—operational state.

These are the available options:

- disabled(0)—ACC is disabled
- enabled(1)—ACC is enabled

Transmit Frame Check Seq. Size (pppStatTransmitFcsSize)

The size of the Frame Check Sequence (FCS) in bits that the local node will generate when sending packets tothe remote node. This setting becomes active when the link is in the up—able to pass packets—operational State.

The values are from *0* to *128*.

Receive Frame Check Seq. Size (pppStatReceiveFcsSize)

The size (in bits) of the frame check sequence (FCS) that the remote node will generate when sending packets to the local node. This setting becomes active when the link is in the up—able to pass packets—operational state. The values are from *0* to *128*.

IP Statistics

Operational Status (pppIpOperStatus)
The current operational state of the interface. These are the available options:

- up(1)—able to pass packets
- down(2)—unable to pass packets
- testing(3)—in test mode and unable to pass packets

Local VJ Protocol Comprsn (pppIpLocalToRemoteCompProt)
The IP compression protocol that the local IP entity uses when sending packets to the remote IP entity. The available settings are:

- none(1)—no compression
- vjTCP(2)—compression is enabled

Remote VJ Protocol Comprsn (pppIpRemoteToLocalCompProt)
The IP compression protocol that the remote IP entity uses when sending packets to the local IP entity. The available settings are:

- none(1)—no compression
- vjTCP(2)—enabled

Remote Max Slot ID (pppIpRemoteMaxSlotId)
The Max-Slot-Id access server parameter that the remote node has announced and that is in use on the link. If vjTCP header compression is not in use on the link, the value of this object will be *0*. The range is from *0* to *255*.

Local Max Slot ID (pppIpLocalMaxSlotId)
The Max-Slot-Id access server parameter that the local node has announced and that is in use on the link. If vjTCP header compression is not in use on the link, the value of this object will be *0*. The range is from *0* to *255*.

Data Statistics

Octets Sent (pppActSentOctets)
The number of octets (bytes) sent during this session.

Octets Received (pppActReceivedOctets)
The number of octets (bytes) received during this session.

Packets Sent (pppActSentDataFrames)
The number of packets sent during this session . Version 6 nomenclature for a packet is Ipv6 header plus payload.

Packets Received (pppActReceivedDataFrames)
The number of packets received during this session. Version 6 nomenclature for a packet is Ipv6 header plus payload.

Modify Link Configuration window

Clicking on the Modify… link in the PPP link window will allow configuration of the individual link settings.

Figure 78. Link configuration

Refer to section "Default settings" on page 131 for descriptions of the following options.

- PPP protocol (pppDesiredFunction)
- Authentication Technique (pppAuthenticationTechnique)
- Authentication Side (pppAuthenticationSide)
- Authentication Username (pppAuthenticationUsername)
- Authentication Password (pppAuthenticationPassword)
- MRU (pppInitialMRU)
- IP Address (pppServiceIpAddress)
- IP Mask (pppServiceIpMask)
- IP Compression (pppIpCompression)
- IP Force Next Hop (pppForceNextHop)
- Link Compression (pppLinkCompression)
- Allow Magic Number Negotiation (pppMagicNumber)

Chapter 14 ICMP

Chapter contents

Introduction

When networking problems or undesirable conditions occur, the ICMP protocol is used for communicating control or error information plus testing. The statistics listed on the 3096RC T-DAC ICMP window (see figure 79) comprise those contained in *RFC 792—Internet Control Message Protocol (ICMP)*. Implementation of the ICMP group is mandatory for all TCP/IP networks. *RFC 1312—ICMP Group of MIB-II Variables*—provides the definitions of these variables. It is important to remember that any RFC can be superseded by a newer version.

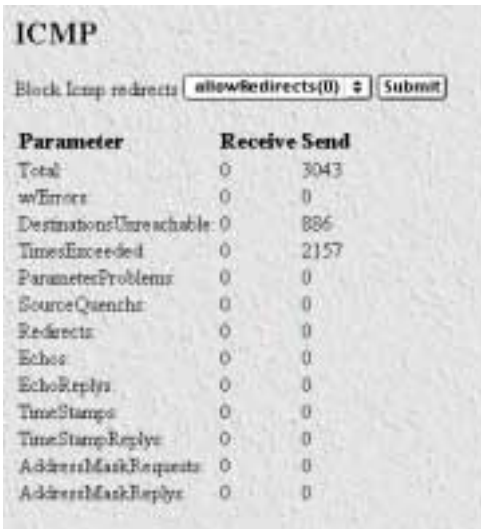


Figure 79. ICMP window

To display the ICMP management web page, on the T-DAC configuration menu pane, click the ICMP hyperlink

ICMP window

The ICMP window provides the means for you to manage the T-DAC's ICMP subsystem. Managing the T-DAC's ICMP subsystem involves monitoring ICMP statistics, and defining whether the T-DAC will receive or block ICMP Redirect messages sent from gateway routers and/or hosts.

Block ICMP redirects (boxBlockIcmpRedirects)

The two options for "Block ICMP Redirects" either allow the reception of ICMP Redirect messages [allowRedirects(0)] or block the reception of ICMP Redirect messages [stopRedirects(1)]. The recommended configuration is to block the ICMP redirect messages because in some instances they could alter the routing table with undesirable effects, which is considered a breach of security.

ICMP Receive/Send Messages table

The ICMP window statistics table displays the ICMP message counters. ICMP messages are displayed in the window table as columns comprising two types of messages:

- Messages received by the T-DAC (InMibVariable)
- Messages sent by the T-DAC (OutMibVariable)

The numbers following the parameters can be a good source of what is happening on the network to point out potential problems. Both gateways (routers) and hosts can send ICMP messages.

Total Received (icmpInMsgs)

The total number of ICMP messages which the 3096RC Multiplexer T-DAC has received.

> **Note** This counter includes all those counted by icmpInErrors (see "w/ Errors (icmpInErrors, icmpOutErrors)").

Total Sent (imcpOutMsgs)

Similar to icmpInMsgs, Total Sent represents the total number of ICMP messages which the 3096RC T-DAC has attempted to send. This variable includes all ICMP messages counted by icmpOutErrors (see "w/Errors (icmpInErrors, icmpOutErrors)").

w/Errors (icmpInErrors, icmpOutErrors)

The number of ICMP messages which the Model 3096RC T-DAC received/sent but having ICMP-specific errors (for example, bad ICMP checksums, bad length, or non-routable errors).

Destinations Unreachable (IcmpInDestUnreachs, IcmpOutDestUnreachs)

The number of ICMP destination unreachable messages received/sent. For instance, if the information in a gateway's routing table determines that the network specified in a packet is unreachable, the gateway will send back an ICMP message stating that the network is unreachable. The following conditions will send back an unreachable message:

- The network is unreachable
- The host is unreachable
- The protocol is not available to the network
- The port on the host is unavailable; a specified source route failed
- A packet must be fragmented (that is, broken up into two or more packets) but the packet was sent anyway with instructions not to be fragmented.

Times Exceeded (icmpInTimeExcds, icmpOutTimeExcds)

The number of ICMP time exceeded messages received/sent. Each time a packet passes through a gateway, that gateway reduces the time-to-live (TTL) field by one. The default starting number is defined under the IP section. If the gateway processing a packet finds that the TTL field is zero it will discard the packet and send the ICMP time exceeded message. Time exceeded will also be incremented when a host which is reassembling a fragmented packet cannot complete the reassembly due to missing packets within its time limit. In this case, ICMP will discard the packet and send the time exceeded message.

Parameter Problems (icmpInParmProbs, icmpOutParmProbs)

The number of ICMP parameter problem messages received/sent. If while processing a packet, a gateway or host finds a problem with one or more of the IP header parameters which prohibits further processing, the gateway or host will discard the packet and return an ICMP parameter problem message. One potential source of this problem may be with incorrect or invalid arguments in an option. ICMP sends the parameter problems message if the gateway or host has discarded the whole packet.

Source Quenchs (icmpInSrcQuenchs, icmpOutSrcQuenchs)
The number of ICMP source quench messages received/sent. A gateway will discard packets if it cannot allocate the resources, such as buffer space, to process the packet. If a gateway discards the packet, it will send an ICMP source quench message back to the sending device. A host may send this messages if packets arrive too fast to be processed or if there is network congestion. The source quench message is a request to reduce the rate at which the source is sending traffic. If the T-DAC receives a source quench, it will wait for acknowledgement of all outstanding packets before sending more packets to the remote destination. Then it will begin sending out packets at an increasing rate until the connection is restored to standard operating conditions.

Redirects (icmpInRedirects, icmpOutRedirects)
The number of ICMP redirect messages received/sent. A gateway sends a redirect message to a host if the network gateways find a shorter route to the destination through another gateway.

Echos (icmpInEchos, icmpOutEchos)
The number of ICMP echo request messages received/send. The ICMP echo is used whenever one uses the diagnostic tool ping. Ping is used to test connectivity with a remote host by sending regular ICMP echo request packets and then waiting for a reply. Received echos (icmpInEchos) will increment when the T-DAC is pinged.

Echo Replys (icmpInEchoReps, icmpOutEchoReps)
The number of ICMP echo reply messages received/sent. An echo reply is a response to an echo request. Send echos (icmpOutEchos) will increment when the T-DAC sends an echo reply message in response to a ping.

Time Stamps (icmpInTimestamps, icmpInTimestamps)
The number of ICMP time stamp messages received/sent. Time stamp and time stamp replies were originally designed into the ICMP facility to allow network clock synchronization. Subsequently, a new protocol—Network time protocol (NTP) has taken over this function. Normally, this number will be zero.

Time Stamp Replys (icmpInTimestampsReps) (icmpOutTimestampsReps)
The number of ICMP timestamp reply messages received/sent. This message is part of a time stamp (see "Time Stamps (icmpInTimestamps, icmpInTimestamps)") request. Normally, this number will be zero.

Address Mask Requests (icmpInAddrMasks) (icmpOutAddrMasks)
The number of ICMP address mask request messages received/sent. This message is generally used for diskless workstations which use this request at boot time to obtain their subnet mask. This number will increase if there are hosts on the network which broadcast these requests.

Address Mask Replys (icmpInAddrMasksReps) (icmpOutAddrMasksReps)
The number of ICMP address mask reply messages received/sent. Normally, this number will be zero.

Chapter 15 IP

Chapter contents

Introduction

The T-DAC's IP subsystem manages addressing and routing parameters and statistics pertaining to IP protocol operation on the T-DAC. Managing the IP subsystem involves monitoring IP statistics and parameters, and defining IP addressing and routing parameters.

Note All items described in this chapter are defined in *RFC 1213: Management Information Base for Network Management of TCP/IP-based internets: MIB-II*.

Click on the IP link in the T-DAC's configuration menu pane, to display the IP main window (see figure 80).

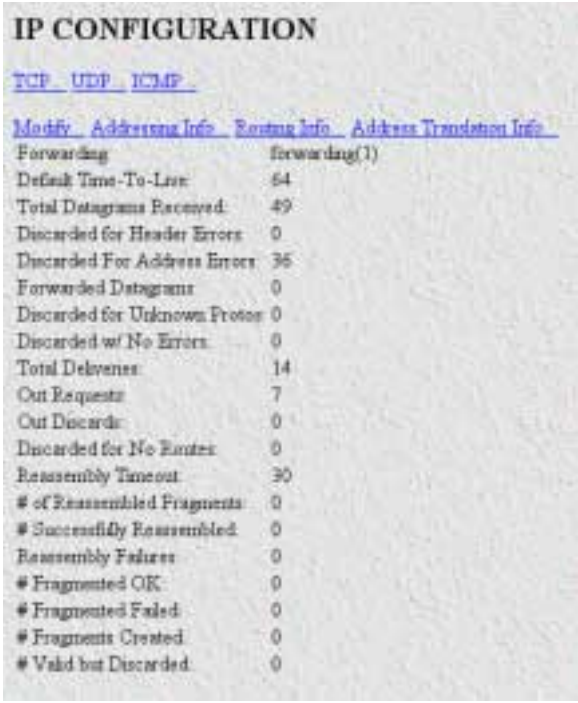


Figure 80. IP main window

IP main window

The IP Overview Main Window provides hyperlinks to the windows shown in figure 81.

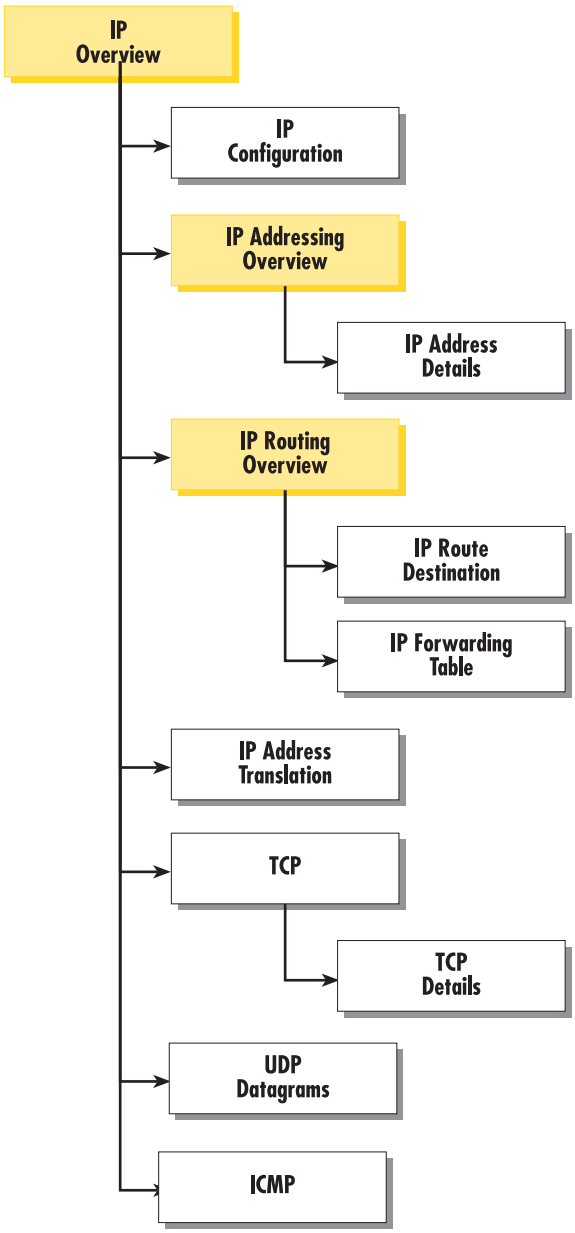


Figure 81. IP main window and related windows

The IP Overview main window displays certain IP statistics as well as the status of the IP forwarding mechanism (forwarding or not forwarding). The following sections describe the contents of the IP main window.

Hyperlinks

The IP window provides the following hyperlinks to the windows shown in figure 81. You can use these sub-pages to view and modify the values of certain IP parameters:

- **TCP**—Clicking the TCP hyperlink displays the TCP window (see section "TCP main window" on page 162).
- **UDP**—Clicking the UDP hyperlink displays the UDP Datagrams window (see section "UDP Datagrams main window" on page 168).
- **ICMP**—Clicking the ICMP hyperlink displays the ICMP window (see section "ICMP window" on page 142).
- **Modify**—Clicking the Modify hyperlink displays the IP Forwarding sub-window where you can modify the values of the IP forwarding and time-to-live parameters (see "Modify IP Configuration window" on page 152).
- **Addressing Info**—Clicking the Addressing hyperlink displays the IP Addressing Overview sub-window. This window (see "IP Addressing Information window" on page 153) displays each IP address and its associated T-DAC interface ID number, and a Details…. for each IP address. The Details hyperlink displays the IP address Details sub-window for that IP address.
- **Routing Info**—Clicking the Routing Info hyperlink displays IP Routing Overview sub-window. This window displays the defined IP Routes table that the T-DAC uses to routing IP datagrams. For each route, the table shows the IP address, subnet mask, next hop router, and interface) You can use this window to add IP routes to the T-DAC's routing table by defining IP routing parameters (see "IP Routing Information window" on page 154).
- **Address Translation Info**—Clicking the Address Translation hyperlink displays the IP address translation sub-window where you can view and define the T-DACs physical to logical (MAC to IP) address correlations (mappings) (see "Address Translation Information window" on page 160).

IP parameters and statistics

The following sections describe the IP parameters and statistics displayed on the IP Overview main window.

Forwarding

The Forwarding parameter defines whether the T-DAC acts as an IP gateway in respect to the forwarding of datagrams received by, but not addressed to the T-DAC. IP gateways forward datagrams. IP hosts do not forward datagrams, except in the case when the host is the source of the datagram.

> **Note** For some managed nodes, this object may take on only a subset of the values possible. Accordingly, it is appropriate for an agent to return a "badValue" response if a management station attempts to change this object to an inappropriate value.

One of the following values may be defined for ipForwarding:

- **forwarding(1)**—acting as a gateway and will forward IP datagrams to other gateways
- **not-forwarding(2)**—not acting as a gateway so it will discard IP datagrams destined for other gateways

Default Time-To-Live
The default value inserted into the time-to-live field of the IP header of datagrams originated at the T-DAC, whenever a TTL value is not supplied by the transport layer protocol.

Total Datagrams Received
The total number of input datagrams received from interfaces, including those received in error.

Discarded for Header Errors
The number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, and so on.

Discarded for Address Errors
The number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at the T-DAC. This count includes invalid addresses (e.g., 0.0.0.0) and addresses of unsupported Classes (e.g., Class E). For entities which are not IP Gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.

Forwarded Datagrams
The number of input datagrams for which the T-DAC was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities which do not act as IP Gateways, this counter will include only those packets which were source-routed via the T-DAC, and the source-route option processing was successful.

Discarded for Unknown Protos
The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.

Discarded with No Errors
The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for example, due to lack of buffer space).

Note The *Discarded w/No Errors* counter does not include any datagrams discarded while awaiting re-assembly.

Total Deliveries
The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).

Out Requests
The total number of IP datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for transmission.

Note The Out Requests counter does not include any datagrams counted in ipForwDatagrams.

Out Discards
The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space).

Note The Out Discards counter would include datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion.

Discarded for No Routes
The number of IP datagrams discarded because no route could be found to transmit them to their destination.

Note The Discarded for No Routes counter includes any packets counted in ipForwDatagrams which meet this "no-route" criterion. This includes any datagrams which a host cannot route because all of its default gateways are down.

Reassembly Timeout
The maximum number of seconds which received fragments are held while they are awaiting reassembly at the T-DAC.

of Reassembled Fragments
The number of IP fragments received which needed to be reassembled at the T-DAC.

Successfully Reassembled
The number of IP datagrams successfully reassembled.

Reassembly Failures
The number of failures detected by the IP reassembly algorithm (for whatever reason: timed out, errors, etc.).

Note The Reassembly Failures value is not necessarily a count of discarded IP fragments since some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received.

Fragmented OK
The number of IP datagrams that have been successfully fragmented at the T-DAC.

Fragmented Failed
The number of IP datagrams that have been discarded because they required fragmenting at the T-DAC, but were not fragmented because their *Don't Fragment* option was set.

Fragments Created
The number of IP datagram fragments that have been generated at the T-DAC.

Valid but Discarded

The number of routing entries which were chosen to be discarded even though they are valid. One possible reason for discarding such an entry could be to make more buffer space available for other routing entries.

Modify IP Configuration window

The IP Configuration window (see figure 82) provides the means for you to view and modify the values of the IP Forwarding and Default Time-to-Live parameters for the T-DAC.

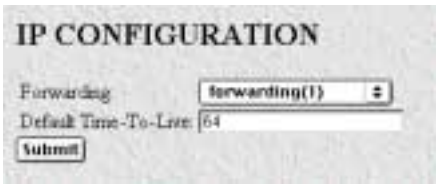


Figure 82. IP Configuration window

To display the IP Configuration window, on the IP management web page, click the Modify… link.

Forwarding (ipForwarding)

Determines whether the T-DAC is acting as an IP gateway that will forward datagrams received by-but not addressed to-the T-DAC. IP gateways forward datagrams, IP hosts do not (except those source-routed via the host).

> **Note** For some managed nodes, this object may take on only a subset of the values possible. Accordingly, it is appropriate for an agent to return a "badValue" response if a management station attempts to change this object to an inappropriate value.

The following options are available:

- **forwarding**(1)—acting as a gateway
- **not-forwarding**(2)—not acting as a gateway

Default Time-To-Live (ipDefaultTTL)

The default value inserted into the Time-To-Live (TTL) field in the IP header of datagrams originating from the T-DAC, whenever a TTL value is not already supplied by the transport layer protocol.

Saving Your Work

Once you have defined your desired values for the configurable parameters shown in the IP Configuration sub-page, you must click the **Submit Query** button to save the new values into volatile DRAM. Once you click the button, the T-DAC will implement the changes immediately.

> **Note** To save your changes permanently, you must visit the T-DAC HOME page, and click the Save Current Configuration button. When you click the Save Current Configuration button, the T-DAC will copy the configuration currently stored in volatile DRAM into non-volatile Flash memory for persistent storage.

IP Addressing Information window

The IP addressing Information window (ipAdEntAddr) window (see figure 83) provides the means for you to view the default address for outgoing IP datagrams, the IP addresses defined for the T-DAC and the interface ID associated with each address.

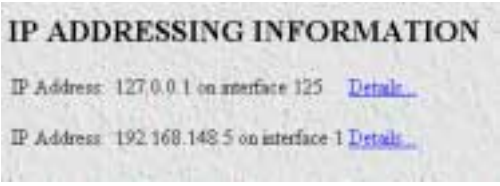


Figure 83. IP addressing Information window

For each IP address on the page, there is a Details hyperlink. Clicking the Details hyperlink displays the Address window.

Address window

The Address window (see figure 84) displays the contents of the T-DAC's IP address table for each network interface defined on the blade. To display the Address window, on the IP ADDRESSING INFORMATION page, select the interface you wish to view, and click the Details hyperlink.

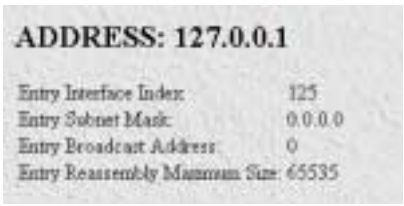


Figure 84. Address window

Entry Interface Index (ipAdEntIfIndex)
The index value that identifies the interface to which this entry applies.

Entry Subnet Mask (ipAdEntNetMask)
The subnet mask associated with the IP address of this entry. The value of the mask is an IP address with all the network bits set to 1 and all the hosts bits set to 0.

Entry Broadcast Address (ipAdEntBcastAddr)
The value of the least-significant bit in the IP broadcast address used for sending datagrams on the interface associated with the IP address of this entry. For example, when the Internet standard all-ones broadcast address is used, the value will be 1. This value applies to both the subnet and network broadcast addresses used by the entity on this interface.

Entry Reassembly Maximum Size (ipAdEntReasmMaxSize)
The size of the largest IP datagram which the T-DAC can re-assemble from incoming IP fragmented datagrams received on this interface.

IP Routing Information window

The IP Routing Information window (see figure 85) displays information required to route IP datagrams, including the IP address, subnet mask, next-hop router, and interface for each network interface defined in the DACS.

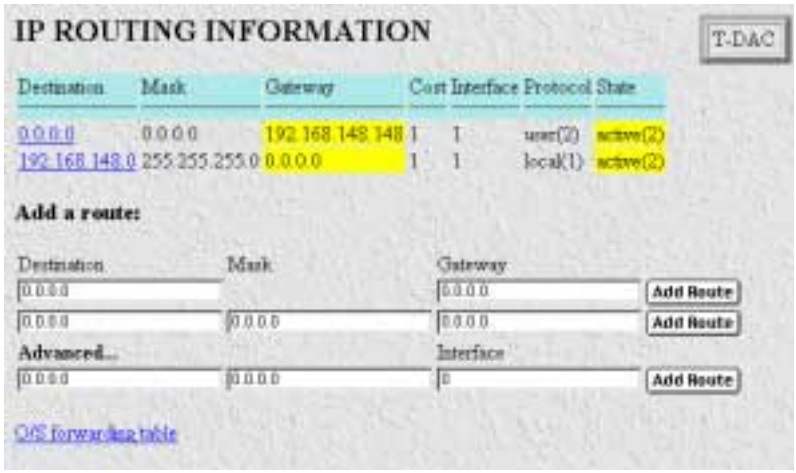


Figure 85. IP Routing Information sub-page

The following paragraphs describe the contents of the IP Routing Information sub-page.

The IP Routing Information window also provides a link to the Forwarding Table window. The Forwarding Table sub-page displays the IP forwarding parameters that the T-DAC's operating system uses to make IP forwarding decisions. (see "Forwarding Table" on page 158).

Destination (genRouteDest)

The destination IP address of this route. An entry with a value of 0.0.0.0 is considered a default route. Multiple routes to a single destination can appear in the table, but access to such multiple entries is dependent on the table-access mechanisms defined by the network management protocol in use.

Each IP address displayed in the Destination column of the table also functions as a link to the Route Destination window. To view or modify next-hop routing information for a selected destination address, click on the Address hyperlink in the Destination column. For more information about modifying next-hop routing information settings, refer to "Route Destination window" on page 156.

Mask (genRouteMask)

Indicates the mask to be logical-ANDed with the destination address before being compared to the value in the ipRouteDest field. For those systems that do not support arbitrary subnet masks, an agent constructs the value

of the ipRouteMask by determining whether the value of the correspondent ipRouteDest field belongs to a Class A, B, or C network, and then using the appropriate mask from table 5.

Table 5. Masks

Mask	Network
255.0.0.0	class-A
255.255.0.0	class-B
255.255.255.0	class-C

Gateway (genRouteGateway)
Specifies the IP address to which the packets should be forwarded.

Cost (genRouteCost)
This is the cost of the route as defined by RIP standards. Cost is sometimes considered to be number of hops. A cost of 16 is considered to be infinite. A cost can be given to user-entered routes so their preference in relation to learned routes can be calculated.

Interface (genRouteIfIndex)
The index value that identifies the local interface through which the next hop of this route should be reached. The interface identified by a particular value of this index is the same interface as identified by the same value of ifIndex. This may be zero in the case that the route is not active or no interface could be found which has access to the gateway.

Protocol (genRouteProto)
The mechanism by which this route was learned is defined by protocol. The parameters are:

- unknown(0)
- local(1)—Added by O/S to support an interface
- user(2)—Added through row creation in this MIB
- rip(4)—Added by reception of a RIP packet
- icmp(5)—Added by reception of an ICMP packet
- radius(6)—Provided in a RADIUS response packet

State (RouteState)
- invalid(1)—This setting deletes the route.
- active(2)—A valid route is in use.
- nopath(3)—No route is available to the specified gateway. The gateway is not known to local networks.
- agedout(4)—Invalid route (soon to be removed).
- costly(5)—A valid route, but not in use because of it's higher cost.

Add a route:

This portion of the IP Routing Information window is where you can add a new route to the IP Routing Information table. Fill in the Destination (genRouteDest), Mask (genRouteMask), and Gateway (genRouteGateway) information, then click **Add Route**.

Destination (ipRouteDest)
The destination IP address of this route. An entry with a value of 0.0.0.0 is considered a default route. Multiple routes to a single destination can appear in the table, but access to such multiple entries is dependent on the table-access mechanisms defined by the network management protocol in use.

Mask (ipRouteMask)
Indicates the mask to be logical-ANDed with the destination address before being compared to the value in the ipRouteDest field. For those systems that do not support arbitrary subnet masks, an agent constructs the value of the ipRouteMask by determining whether the value of the correspondent ipRouteDest field belongs to a Class A, B, or C network, and then using the appropriate mask from table 5 on page 155.

Gateway (genRouteGateway)
Specifies the IP address to which the packets should be forwarded.

Advanced...

Enables a route to be attached to an interface. Packets to a network will be routed to that interface, allowing the gateway IP address to be dynamic. Fill in the Destination (genRouteDest), Mask (genRouteMask), and Inter-face (genRouteIfIndex) information, then click **Add Route**.

Destination (ipRouteDest)
The destination IP address of this route. An entry with a value of 0.0.0.0 is considered a default route. Multiple routes to a single destination can appear in the table, but access to such multiple entries is dependent on the table-access mechanisms defined by the network management protocol in use.

Mask (ipRouteMask)
Indicates the mask to be logical-ANDed with the destination address before being compared to the value in the ipRouteDest field. For those systems that do not support arbitrary subnet masks, an agent constructs the value of the ipRouteMask by determining whether the value of the correspondent ipRouteDest field belongs to a Class A, B, or C network, and then using the appropriate mask from table 5 on page 155.

Gateway (genRouteGateway)
Specifies the IP address to which the packets should be forwarded.

Route Destination window

The Route Destination sub-page (see figure 86) displays the next-hop routing parameters for the single destination address displayed in the page title to display the Route Destination window, on the IP Routing Information page, identify the destination address you wish to view then click the address link.

Figure 86. Routing Destination window

The following paragraphs describe the parameters displayed on the The Route Destination sub-page.

Route Destination (genRouteDest)

The destination IP address of this route. An entry with a value of 0.0.0.0 is considered a default route. Multiple routes to a single destination can appear in the table, but access to such multiple entries is dependent on the table-access mechanisms defined by the network management protocol in use.

Mask (genRouteMask)

Indicates the mask to be logical-ANDed with the destination address before being compared to the value in the ipRouteDest field. For those systems that do not support arbitrary subnet masks, an agent constructs the value of the ipRouteMask by determining whether the value of the corresponding ipRouteDest field belongs to a Class A, B, or C network, and then using the appropriate mask from table 5 on page 155.

Interface (genRouteIfIndex)

The index value which uniquely identifies the local interface through which the next hop of this route should be reached. The interface identified by a particular value of this index is the same interface as identified by the same value of ifIndex.

Protocol (genRouteProto)

The routing mechanism via which this route was learned. Inclusion of values for gateway routing protocols is not intended to imply that hosts must support those protocols.

- unknown(0)
- local(1)—Added by the DACS to support an interface.
- user(2)—Added by an administrator on the IP Routing Information table or via SNMP management tools.
- dspf(3)—Not currently implemented.
- rip(4)—Learned via reception of RIP packet.
- icmp(5)—Learned via reception of ICMP packet.

Seconds Since Updated (genRouteAge)

The number of seconds since this route was last updated or otherwise determined to be correct.

Tag (genRouteTag)
An identifier associated with the route. This can have different meanings depending on the protocol. For example, this gives the tag that was passed with a learned RIP route.

Gateway (genRouteGateway)
Specifies the IP address to which the packets should be forwarded.

Cost (genRouteCost)
This is the cost of the route as defined by RIP standards. Cost is sometimes considered to be number of hops. A cost of 16 is considered to be infinite. A cost can be given to user-entered routes so their preference in relation to learned routes can be calculated.

State (genRouteState)
Defines the state which a route may be in during its lifetime.

- invalid(1)—This setting deletes the route.
- active(2)—A valid route is in use.
- nopath(3)—No route is available to the specified gateway. The gateway is not known to local networks.
- agedout(4)—Invalid route (soon to be removed).
- costly(5)—A valid route, but not in use because of it's higher cost.

Forwarding Table

The Forwarding Table window (see figure 87) displays the IP forwarding parameters for all routes in the T-DAC's forwarding table. To display the Forwarding Table window, on the IP Routing Information sub-page, click the O/S forwarding table link.

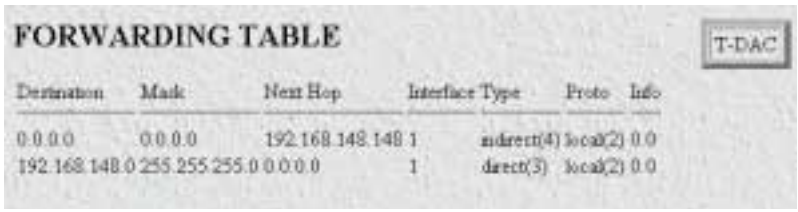


Figure 87. Forwarding Table window

Destination (ipRouteDest)
The destination IP address of this route. An entry with a value of 0.0.0.0 is considered a default route. Multiple routes to a single destination can appear in the table, but access to such multiple entries is dependent on the table-access mechanisms defined by the network management protocol in use.

Mask (ipRouteMask)
Indicates the mask to be logical-ANDed with the destination address before being compared to the value in the ipRouteDest field. For those systems that do not support arbitrary subnet masks, an agent constructs the value of the ipRouteMask by determining whether the value of the correspondent ipRouteDest field belongs to a Class A, B, or C network, and then using the appropriate mask from table 5 on page 155.

Next Hop (ipRouteNextHop)
The IP address of the next hop of this route. (In the case of a route bound to an interface which is realized via a broadcast media, the value of this field is the agent's IP address on that interface.)

Interface (ipRouteIfIndex)
The index value that identifies the local interface through which the next hop of this route should be reached. The interface identified by a particular value of this index is the same interface as identified by the same value of ifIndex.

Type (ipRouteType)
One of the following route types:

- other(1)—none of the following
- invalid(2)—an invalidated route
- direct(3)—route to directly connected (sub-)network
- indirect(4)—route to a non-local host/network/sub-network

> **Note** The values direct(3) and indirect(4) refer to the notion of direct and indirect routing in the IP architecture. Setting this object to the value invalid(2) has the effect of invalidating the corresponding entry in the ipRouteTable object. That is, it effectively disassociates the destination identified with said entry from the route identified with said entry. It is an implementation-specific matter as to whether the agent removes an invalidated entry from the table. Accordingly, management stations must be prepared to receive tabular information from agents that corresponds to entries not currently in use. Proper interpretation of such entries requires examination of the relevant ipRouteType object.

Protocol (ipRouteProto)
The routing mechanism via which this route was learned. Inclusion of values for gateway routing protocols is not intended to imply that hosts must support those protocols.

- unknown(0)
- local(1)—Added by the DACS to support an interface.
- user(2)—Added by an administrator on the IP Routing Information table or via SNMP management tools.
- dspf(3)—Not currently implemented.
- rip(4)—Learned via reception of RIP packet.
- icmp(5)—Learned via reception of ICMP packet.

Info (ipRouteInfo)
A reference to MIB definitions specific to the particular routing protocol which is responsible for this route, as determined by the value specified in the route's ipRouteProto value. If this information is not present, its value should be set to the OBJECT IDENTIFIER { 0 0 }, which is a syntactically valid object identifier, and any conformant implementation of ASN.1 and BER must be able to generate and recognize this value.

Address Translation Information window

The Address Translation Information window (see figure 88) displays the contents of the T-DAC's logical-to-physical address translation table. The T-DAC uses the table to resolve the correspondence between a logical IP network address and a physical Media Access Control (MAC) address.

Note Some interface types do not use translation tables to determine address equivalences (for example, DDN-X.25 uses an algorithmic method). If the Address Translation table is empty (there are no entries), that indicates that none of the T-DAC's interfaces are using an address translation table.

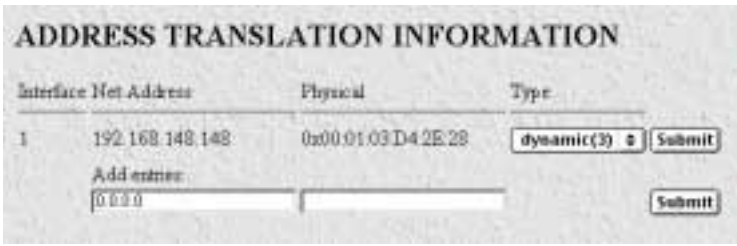


Figure 88. Address Translation Information window

The following sections describe the information displayed on the Address Translation Information window.

Interface (ipNetToMediaIfIndex)

Each entry contains one IP address to physical address equivalence.

Net Address (ipNetToMediaNetAddress)

The IP address corresponding to the media-dependent physical address.

Physical (ipNetToMediaPhysAddress)

The media-dependent physical address.

Type (ipNetToMediaType)

The type of mapping. Setting this object to the value invalid(2) has the effect of invalidating the corresponding entry in the ipNetToMediaTable. That is, it effectively disassociates the interface identified with said entry from the mapping identified with said entry. It is an implementation-specific matter as to whether the agent removes an invalidated entry from the table. Accordingly, management stations must be prepared to receive tabular information from agents that corresponds to entries not currently in use. Proper interpretation of such entries requires examination of the relevant ipNetToMediaType object.

- other(1)-none of the following
- invalid(2)-an invalidated mapping
- dynamic(3)
- static(4)

Chapter 16 TCP

Chapter contents

Introduction

Transmission Control Protocol (TCP) fits in the Transport layer (layer 4) of the OSI model, above the Internet Protocol (IP). It is among the most widely used protocols in the TCP/IP suite. The T-DAC TCP subsystem provides management information in the form of TCP parameters and operating statistics. Managing the TCP subsystem involves monitoring the TCP parameters and statistics.

Note You can download detailed information about the SNMP MIB variables for the TCP subsystem from *RFC1213: Management Information Base for Network Management of TCP/IP-based internets: MIB-II*.

To display the TCP main window (see figure 89) and monitor TCP statistics, on the T-DAC Configuration Menu pane, click the TCP hyperlink.

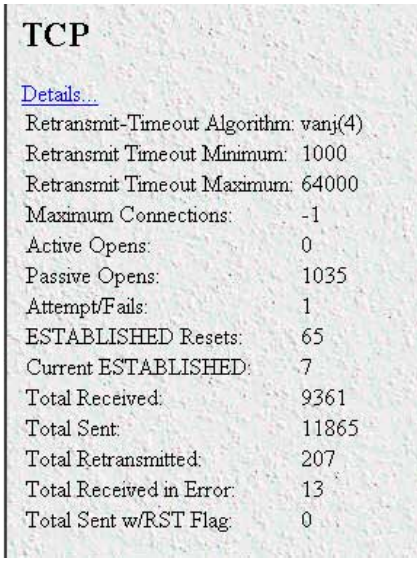


Figure 89. TCP main window

TCP main window

The TCP main window (see figure 89) provide the means for you to manage the T-DAC's TCP subsystem. The TCP main window displays the current values of certain TCP operating parameters and TCP operating statistics. The TCP main window provides a hyperlink to the TCP Details window as shown in figure 90.

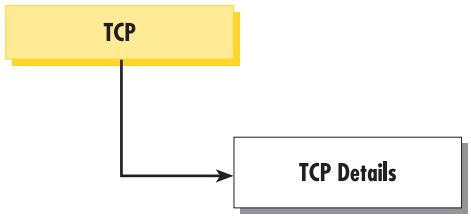


Figure 90. TCP windows map

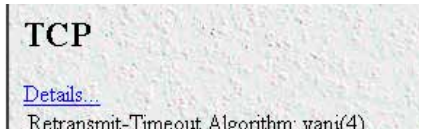


Figure 91. Details… link location on TCP main window

Details... hyperlink

Click on the Details… link (see figure 91) to display the TCP Details window. The TCP Details window is described in section "TCP Details window" on page 164.

TCP parameters and statistics table

The TCP main window displays certain parameters and statistics in a table. The following paragraphs describe the parameters and statistics the T-DAC displays on the TCP main window.

Retransmit-Timeout Algorithm (tcpRtoAlgorithm)
Indicates the algorithm the TCP subsystem uses to calculate the TCP retransmission timer delay. The TCP retransmission timer defines how long the T-DAC will wait before retransmitting unacknowledged octets.

Retransmit-Timeout Minimum (tcpRtoMin)
The minimum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission timeout. In particular, when the timeout algorithm is rsre(3), an object of this type has the semantics of the LBOUND quantity described in RFC 793.

Retransmit-Timeout Maximum (tcpRtoMax)
The maximum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission timeout. In particular, when the timeout algorithm is rsre(3), an object of this type has the semantics of the UBOUND quantity described in RFC 793.

Maximum Connections (tcpMaxConn)
The limit on the total number of TCP connections the entity can support. In entities where the maximum number of connections is dynamic, this object should contain the value -1.

Active Opens (tcpActiveOpens)
The number of times TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state.

Passive Opens (tcpPassiveOpens)
The number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state.

Attempt/Fails (tcpAttemptFails)
The number of times TCP connections have made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state.

ESTABLISHED Resets (tcpEstabResets)
The number of times TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.

Current ESTABLISHED (tcpCurrEstab)
The number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT.

Total Received (tcpInSegs)
The total number of segments received, including those received in error. This count includes segments received on currently established connections.

Total Sent (tcpOutSegs)
The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.

Total Retransmitted (tcpRetransSegs)
The total number of segments retransmitted—that is, the number of TCP segments transmitted containing one or more previously transmitted octets.

Total Received in Error (tcpInErrs)
The total number of segments received in error (e.g., bad TCP checksums).

Total Sent w/RST Flag (tcpOutRsts)
The number of TCP segments sent containing the RST flag.

TCP Details window

The TCP Details sub-window (see figure 92) provides port state and connection information for each TCP port currently active on the T-DAC. To view the TCP Details window, on the TCP main window, click the Details… link.

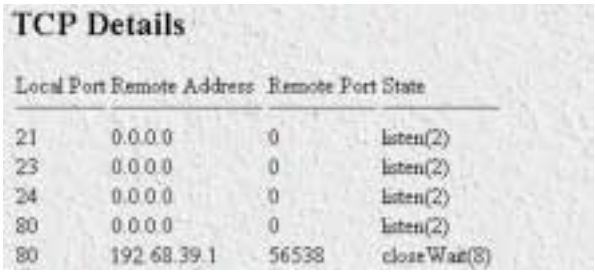


Figure 92. TCP Details window

The following paragraphs describe the information displayed on the TCP Details window.

Local Port (tcpConnLocalPort)
The local port number for this TCP connection.

Remote Address (tcpConnRemAddress)
The remote IP address for this TCP connection.

Remote Port (tcpConnRemPort)
The remote port number for this TCP connection.

State (tcpConnState)
The state of this TCP connection. The only value which may be set by a management station is deleteTCB(12). Accordingly, it is appropriate for an agent to return a 'badValue' response if a management station attempts to set this object to any other value.

If a management station sets this object to the value deleteTCB(12), Transmission Control Block, then this has the effect of deleting the TCB (as defined in RFC 793) of the corresponding connection on the managed node, resulting in immediate termination of the connection. As an implementation-specific option, a RST segment may be sent from the managed node to the other TCP endpoint (note however that RST segments are not sent reliably).

- closed(1)
- listen(2)
- synSent(3)
- synReceived(4)
- established(5)
- finWait1(6)
- finWait2(7)
- closeWait(8)
- lastAck(9)
- closing(10)
- timeWait(11)
- deleteTCB(12)—The only value which may be set by a management station.

Chapter 17 UDP

Chapter contents

Introduction

The 3096RC T-DAC provides support for User Datagram Protocol (UDP). UDP resides in the Transport Layer (layer 3) of the Open Systems Interconnection (OSI) model. Certain networking applications are designed to use UDP instead of TCP for end-to-end data transport.

The T-DAC TCP subsystem provides management information in the form of UDP parameters and operating statistics. Managing the UDP subsystem involves monitoring those UDP parameters and statistics.

Note *RFC1213: Management Information Base for Network Management of TCP/IP-based internets: MIB II* provides detailed information about the SNMP management information base (MIB) variables that the T-DAC UDP subsystem uses.

UDP Datagrams main window

The UDP Datagrams main window (see figure 93) displays the current values of certain UDP operating parameters and UDP operating statistics. To display the UDP main window, on the T-DAC configuration menu pane, click the UDP link.

Figure 93. UDP Datagrams window

The following sections describe the UDP operating parameters and UDP operating statistics that the UDP main window displays.

Received (udpInDatagrams)

The total number of UDP datagrams delivered to UDP users.

Received With No Ports (udpNoPorts)

The total number of received UDP datagrams for which there was no application at the destination port.

Others Received with No Delivery (udpInErrors)

The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.

Sent (udpOutDatagrams)
The total number of UDP datagrams sent from this entity.

Listener Table (udpTable)
The UDP Listener Table contains information about this entity's UDP end-points on which a local application is currently accepting datagrams.

Local Address (udpLocalAddress)
The local IP address for this UDP listener. In the case of a UDP listener that is willing to accept datagrams for any IP interface associated with the node, the value 0.0.0.0 is used.

Local Port (udpLocalPort)
The local port number for this UDP listener.

Chapter 18 RIP Version 2

Chapter contents

Introduction

The 3096RC T-DAC provides support for Routing Information Protocol (RIP) Version 2. The T-DAC RIP version 2 subsystem provides management information in the form of RIP Version 2 addresses, parameters, and statistics. Managing the RIP version 2 subsystem involves defining RIP Version 2 addresses and parameters, and monitoring RIP Version 2 parameters and statistics on TCP.

All object identifiers described in this chapter comply with those contained in RFC 1724: RIP Version 2 MIB Extension.

RIP Version 2 main window

The RIP Version 2 main window (see figure 94) provides the means for you to manage the T-DAC's RIP Version 2 subsystem. The window displays the current values of certain RIP Version 2 operating parameters and statistics, and provides the means for you to add IP addresses to the T-DAC's RIP Version 2 table. The window displays information in the following three tables:

- The RIP status section at the top of the window.
- The RIP Configuration section in the middle of the window.
- The Add a RIP Address section at the bottom of the window.

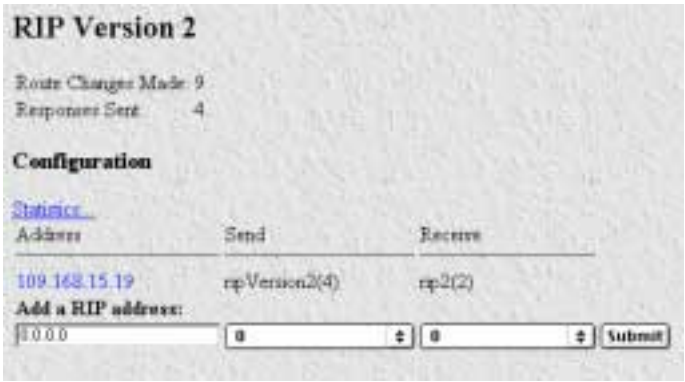


Figure 94. RIP Version 2 window

To display the RIP Version 2 main window, on the T-DAC configuration menu pane, click on the RIP Version 2 link.

The RIP Version 2 main window provides links to the RIP Version 2 Statistics and Parameters windows, as shown in figure 95.

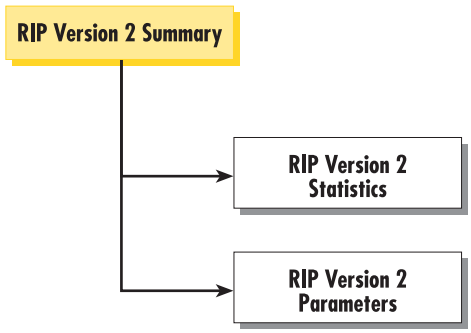


Figure 95. RIP Version 2 windows map

The following sections describe the contents of the tables displayed on the RIP Version 2 main window.

RIP status table

- **Route Changes Made (rip2GlobalRouteChanges)**—The number of route changes made to the IP Route Database by RIP. This does not include the refresh of a route's age.
- **Responses Sent (rip2GlobalQueries)**—The number of responses sent to RIP queries from other systems.

RIP Configuration table

- **Statistics hyperlink**—Clicking on the Statistics link displays the RIP Version 2 Statistics window (see "RIP Version 2 (Status)" on page 175). For each subnet IP address in the T-DAC's RIP Version 2 table, the RIP Version 2 Statistics window displays the RIP route status and statistical counts for Bad Packets, Bad Routes, and Sent Updates.
- **Address (xxx.xxx.xxx.xxx) [rip2IfConfAddress]**—Each IP Address in the table defines a single routing domain in a single subnet for the T-DAC—to use when making RIP routing decisions.

  Note Each IP Address displayed in the RIP Version 2 table also functions as a hyperlink to the RIP Version 2 Parameters window (see section "RIP Version 2 (Configuration) window" on page 176). You can use the RIP Version 2 Parameters window to view and modify the parameters for a single address.

  Initially, because the T-DAC RIP Version 2 table is empty, the RIP Version 2 main window will not display any address hyperlinks. You can use the Adding a RIP Address table to add one more IP addresses to the T-DAC RIP Version 2 table (see Adding a RIP address). Once you have defined a RIP version 2 address, that address will appear in the table. To view the configurable parameters for an address, click on the Address hyperlink under the Address column to display the RIP Version 2 Parameters window (see "RIP Version 2 (Status)" on page 175).
- **Send (rip2IfConfSend)**—Send is what the router sends on this interface. ripVersion 1 implies sending RIP updates compliant with RFC 1058 rip1Compatible(3), and ripVersion2(4). The following options are available:
  - doNotSend(1)

- ripVersion1(2)
- rip1Compatible (3)—rip1Compatible implies broadcasting RIP-2 updates using RFC 1058 route subsumption rules
- ripVersion2 (4)—ripVersion2 implies multicasting RIP-2 updates

- **Receive (rip2IfConfReceive)**—This indicates which version of RIP updates are to be accepted.
  - rip1 (1)
  - rip2 (2)
  - rip1OrRip2 (3)
  - doNotRecieve (4)

Note rip2 and rip1OrRip2 implies reception of multicast packets.

Adding a RIP Address table

To add a RIP address to the T-DAC's RIP Version 2 table, do the following:

1. Enter the IP network address of the interface on the 3096RC T-DAC that you want to enable RIP. This will be the LAN IP address, in other words, the IP address of the 3096RC. This is not the IP address of the device you want to direct RIP packets to.
2. Enter the protocol version to be used for sending RIP packets. The following choices are available:
   – doNotSend (1)
   – ripVersion1 (2)—ripVersion 1 implies sending RIP updates compliant with RFC 1058
   – rip1Compatible (3)—rip1Compatible implies broadcasting RIP-2 updates using RFC 1058 route subsumption rules
   – ripVersion2 (4)—ripVersion2 implies multicasting RIP-2 updates
3. Enter the protocol version to be used for receiving RIP packets. The following choices are available:
   – rip1 (1)—ripVersion 1 implies sending RIP updates compliant with RFC 1058
   – rip2(2)—rip1Compatible implies broadcasting RIP-2 updates using RFC 1058 route subsumption rules
   – rip1OrRip2(3)
   – doNotReceive(4)

   Note rip2 and rip1OrRip2 implies reception of multicast packets.
4. Click on **Submit Query**.

   Note To delete the RIP address, click on the IP Address under the column named Address. Select Status to be invalid(2) and click on **Submit Query**.

To view and modify additional configurable parameters for the RIP address, click on the Address hyperlink to display the RIP Version Configuration window.

RIP Version 2 (Status)

For each subnet IP address defined in the T-DAC's RIP Version 2 table, the RIP Version 2 (Status) window (see figure 97) displays the RIP route status and the following statistical counts:

- Bad Packets
- Bad Routes
- Sent Updates

To display the RIP Version 2 (Status) window, on the RIP Version 2 main window, click the Statistics… link.

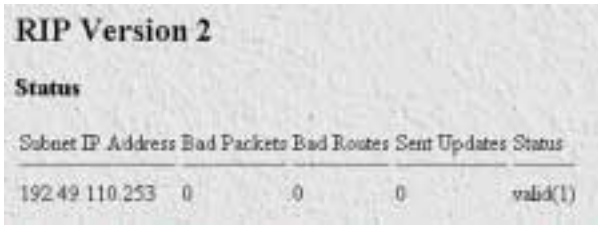


Figure 96. RIP Version 2 (Status) window

The following sections describe the information displayed on the RIP Version 2 (status) window.

Subnet IP Address (rip2IfStatAddress)

The IP Address of this system on the indicated subnet. For unnumbered interfaces, the value 0.0.0.N, where the least significant 24 bits (N) is the ifIndex for the IP Interface in network byte order.

Bad Packets (rip2IfStatRcvBadPackets)

The number of RIP response packets received by the RIP process which were subsequently discarded for any reason (e.g. a version 0 packet, or an unknown command type).

Bad Routes (rip2IfStatRcvBadRoutes)

The number of routes, in valid RIP packets, which were ignored for any reason (e.g. unknown address family, or invalid metric).

Sent Updates (rip2IfStatSentUpdates)

The number of triggered RIP updates actually sent on this interface. This explicitly does NOT include full updates sent containing new information.

Status (rip2IfStatStatus)

Displays whether the RIP status for the Subnet IP Address is valid or invalid. One of the following values will be displayed:

- valid(1)—Data may be routed on this interface.
- invalid(2)—Effectively deletes this interface.

RIP Version 2 (Configuration) window

The RIP Version 2 (Configuration) window (see figure 97) displays the configurable parameters for the single RIP routing domain defined by the IP Address displayed at the top of the table. You can use the RIP Version 2 Configuration window to view and modify the parameters for the routing domain. The configurable parameters are Domain, Authentication Type, Authentication Key, Send, Receive, Metric, and Status.

Do the following to display the RIP Version 2 Configuration -window:

1. On the RIP Version 2 main window, in the RIP Configuration table, under the Address column, identify the RIP address you wish to view.
2. Click the Address link.

Figure 97. RIP Version 2 (Configuration) window

The following sections describe the configurable parameters displayed on the RIP Version 2 Configuration window.

Address (rip2IfConfAddress)

The IP Address of this system on the indicated subnet. For unnumbered interfaces, the value 0.0.0.N, where the least significant 24 bits (N) is the ifIndex for the IP Interface in network byte order.

Domain (rip2IfConfDomain)

Value inserted into the Routing Domain field of all RIP packets sent on this interface.

Authentication Type (rip2IfConfAuthType)

The type of Authentication used on this interface.

- noAuthentication (1)
- simplePassword (2)

Authentication Key (rip2IfConfAuthKey)

This value is used as the Authentication Key whenever Authentication Type (rip2IfConfAuthType) has a value other than noAuthentication(1). A modification of Authentication Type does not change the value of Authentication Key. If the Authentication Key string is shorter than 16 octets, it will be left justified, then padded to 16 octets with nulls (0x00) on the right.

Reading this object always results in an octet string of length zero. Authentication may not be bypassed by reading the MIB object.

Metric (rip2IfConfDefaultMetric)

This variable indicates the metric that is to be used for the default route entry in RIP updates originated on this interface. A value of zero indicates that no default route should be originated; in this case, a default route via another router may be propagated.

Status (rip2IfConfStatus)

Writing invalid has the effect of deleting this interface.

- valid (1)
- invalid (2)

Chapter 19 SNMP

Chapter contents

Introduction

The 3096RC T-DAC SNMP subsystem provides management and statistical information about the operation of the SNMP protocol on the T-DAC.

RFC 3418: Management Information Base (MIB) for the Simple Network Management Protocol (SNMP) provides detailed information about the SNMP MIB variables that the T-DAC SNMP subsystem utilizes.

SNMP window

The SNMP window (see figure 98) displays statistics about the operation of the SNMP protocol on the T-DAC. Two columns display the statistical counts for incoming and outgoing SNMP messages. The window also provides the means for you to enable or disable SNMP traps for authentication failures. To display the SNMP main window, on the T-DAC configuration menu pane, click the SNMP hyperlink.

Figure 98. SNMP window

The SNMP window provides hyperlinks to the SNMP sub-windows shown in the diagram below., which display the MIB diagrams for the Corporate, Enterprise and Products MIBs that the T-DAC's SNMP subsystem uses. When you clicking one of the MIB hyperlinks, your browser will download and display the document containing the diagram for that MIB.

The following sections describe the statistical counts displayed in the In and Out columns on the SNMP window, as well as the configurable parameter for Authentication Failure Traps.

SNMP Statistics—In

This section describes the statistical counts displayed in the In column on the SNMP window.

Packets (snmpInPkts)
The total number of Messages delivered to the SNMP entity from the transport service. Typically this would be UDP since the SNMP engine sits on top of UDP

Bad Version (snmpInBadVersions)
The total number of SNMP Messages that were delivered to the SNMP protocol entity and were for an unsupported SNMP version.

Bad Community Names (snmpInBadCommunityNames)
The total number of SNMP Messages delivered to the SNMP protocol entity which used a SNMP community name not known to said entity.

Bad Community Uses (snmpInBadCommunity Uses)
The total number of SNMP messages delivered to the SNMP protocol entity which represented an SNMP operation which was not allowed by the SNMP community named in the message.

ASN ParseErrors (snmpInASNParseErrs)
The total number of ASN.1 or BER errors encountered by the SNMP protocol entity when decoding received SNMP messages.

Error Status "Too Big" (snmpInTooBigs)
The total number of SNMP PDUs that were delivered to the SNMP protocol entity and for which the value of the error-status field is tooBig.

No Such Names (snmpInNoSuchNames)
The total number of SNMP PDUs that were delivered to the SNMP protocol entity and for which the value of the error-status field is noSuchName.

Bad Values (snmpInBadValues)
The total number of SNMP PDUs that were delivered to the SNMP protocol entity and for which the value of the error-status field is badValue.

Error Status "Read Only" (snmpInReadOnlys)
The total number of valid SNMP PDUs that were delivered to the SNMP protocol entity and for which the value of the error-status field is readOnly. It should be noted that it is a protocol error to generate an SNMP PDU which contains the readOnly value in the error-status field, as such this object is provided as a means of detecting incorrect implementations of the SNMP.

Generated Errors (snmpInGenErrs)
The total number of SNMP PDUs that were delivered to the SNMP protocol entity and for which the value of the error-status field is genErr.

Get/Get Next Variables (snmpInTotalReqVars)
The total number of MIB objects that have been retrieved successfully by the SNMP protocol entity as the result of receiving valid SNMP Get-Request and Get-Next PDUs.

Set Variables (snmpInTotalSetVars)
The total number of MIB objects that have been altered successfully by the SNMP protocol entity as the result of receiving valid SNMP Set-Request PDUs.

Get Requests (snmpInGetRequests)
The total number of SNMP Get-Request PDUs that have been accepted and processed by the SNMP protocol entity.

Get Next Requests (snmpInGetNexts)
The total number of SNMP Get-Next PDUs that have been accepted and processed by the SNMP protocol entity.

Set Requests (snmpInSetRequests)
The total number of SNMP Set-Request PDUs that have been accepted and processed by the SNMP protocol entity.

Get Responses (snmpInGetResponses)
The total number of SNMP Get-Response PDUs that have been accepted and processed by the SNMP protocol entity.

Traps (snmpInTraps)
The total number of SNMP Trap PDUs that have been accepted and processed by the SNMP protocol entity.

SNMP Statistics—Out

This section describes the statistical counts displayed in the Out column on the SNMP window.

Out Packets (snmpOutPkts)
The total number of SNMP messages that were passed from the SNMP protocol entity to the transport service.

Error Status "Too Big" (snmpOutTooBigs)
The total number of SNMP PDUs that were generated by the SNMP protocol entity and for which the value of the error-status field is tooBig.

No Such Names (snmpOutNoSuchNames)
The total number of SNMP PDUs that were generated by the SNMP protocol entity and for which the value of the error-status is noSuchName.

Bad Values (snmpOutBadValues)
The total number of SNMP PDUs that were generated by the SNMP protocol entity and for which the value of the error-status field is badValue.

Generated Errors (snmpOutGenErrs)
The total number of SNMP PDUs that were generated by the SNMP protocol entity and for which the value of the error-status field is genErr.

Get Requests (snmpOutGetRequests)
The total number of SNMP Get-Request PDUs that have been generated by the SNMP protocol entity.

Get Next Requests (snmpOutGetNexts)
The total number of SNMP Get-Next PDUs that have been generated by the SNMP protocol entity.

Set Requests (snmpOutSetRequests)
The total number of SNMP Set-Request PDUs that have been generated by the SNMP protocol entity.

Get Responses (snmpOutGetResponses)
The total number of SNMP Get-Response PDUs that have been generated by the SNMP protocol entity.

Traps (snmpOutTraps)
The total number of SNMP Trap PDUs that have been generated by the SNMP protocol entity.

Configurable Parameter—Authentication Failure Traps (snmpEnableAuthenTraps)

This value indicates whether the SNMP agent process is permitted to generate authentication-failure traps. The variable is global. This means that by being disabled, all authentication-failure traps are disabled.

The two options for this variable are:

- enabled(1)
- disabled(2)

Saving your work

Once you have modified the value of Authentication Failure Traps you must click the **Submit Query** button to save your settings into volatile DRAM. Once you click the button, the T-DAC will implement the changes immediately.

> **Note** To save your changes persistently, (i.e. through a T-DAC power cycle) you must visit the T-DAC HOME page, and click the **Save Current Configuration** button. When you click the **Save Current Configuration** button, the T-DAC will copy the configuration currently stored in volatile DRAM into non-volatile Flash memory for persistent storage.

Chapter 20 System

Chapter contents

Introduction

The System main window (see figure 99) provides system-level information about the 3096RC T-DAC. Such information includes system-level operating status, statistics, and hardware and software configuration.

The Patton Enterprise MIB specifies object identifiers for most of the T-DAC's system parameters. However, a small number of the system parameters for the T-DAC system are defined by *RFC 1213, Management Information Base for Network Management of TCP/IP-based internets: MIB-II*.

To display the System main window, on the T-DAC configuration menu pane, click the System hyperlink.

Figure 99. System main window (CPU, SNMP and HTTP, LAN IP, Manufacturer, and Message Blocks)

System main window

The System main window displays information in the following System information tables:

- CPU
- SNMP and HTTP
- LAN IP
- Manufacturer

- Message Blocks
- Operating System Heap Memory
- Enclosure System
- Installation
- Other

The main window also provides the System (configurable Parameters) sub-window and the System (message Block) sub-window as shown in figure 100.

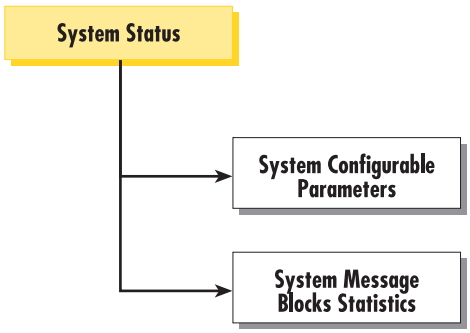


Figure 100. System windows map

All the information on the System main window is shown in display-only format. However, certain fields show the current values of user configurable parameters. You can use the System (configurable Parameters) sub-window (described later in this chapter) to modify the configurable parameters. The following paragraphs describe the contents of the System main window.

Hyperlinks

- Modify—Click the Modify Hyperlink to display the System (configurable Parameters) window. The System (configurable Parameters) window provides the means for you to modify the user-configurable system parameters in the SNMP and HTTP, LAN IP, Installation, and Other tables (see section "System (configurable parameters) window" on page 194 for more information).
- Packet Holding Message Blocks—click on the Packet Holding Message Blocks hyperlink to display the System Message Blocks Statistics window and view the statistics (see section "System (Message Blocks) window" on page 197 for more information).

System Information—CPU

This portion of the System main window shown in figure 99 on page 187 contains information described in the following sections.

Percentage CPU Idle (boxIdletime)

This indicates what percentage of the i960 CPU processing power is not being utilized.

Time Slices Fully Utilized (boxCPUcritical)

This value represents a count of how many times the CPU was fully utilized expressed in 1/100th seconds.

Time Slices 90% Utilized (boxCPUWarning)
This value represents a count of how many times the CPU approached full utilization expressed in 1/100th seconds.

System Information—SNMP and HTTP

This portion of the System main window provides information about the SNMP version and the HTTP accessibility.

Version (boxSnmpVersion)
This parameter indicates the SNMP version number supported by this unit (for example snmpv1(1) means SNMP version 1 is supported). Select snmpv1(1) only since SNMP2 is not currently supported.

Super User Password (boxSnmpMasterPassword)
This is the super user password for complete access and configurability of the T-DAC through SNMP and HTTP (see figure on page 137).

User Password (boxSnmpMonitorPassword)
This displays the user monitoring password for read only access of certain selected information. Not all parameters shown using the superuser password are displayed under the user password. (see figure on page 137).

System Information—LAN IP

This portion of the System main window shown in figure 99 on page 187) contains information described in the following sections.

How to Obtain Address (boxIpAddressTechnique)
This displays the current method for obtaining the LAN IP address.

Address(boxIpAddress)
If the address technique in use above is static, then the value displayed in the Address field is the LAN IP address.

Mask(boxIpMask)
If the address technique in use above is static, then the value displayed in the Address field is the LAN IP mask.

System Information—Manufacturer

This portion of the System main window shown in figure 99 on page 187) contains manufacturing information described in the following sections.

Serial Number (boxManufactureDatecode)
The datecode of manufacture and serial number.

PCB Revision (boxManufacturePcbRevision)
The revision of the printed circuit board.

General Information (boxManufactureGeneralInfo)
A manufacturing notes area for additional information.

System Information—Message Blocks

This portion of the System main window (shown in figure 99 on page 187) contains information about the usage of message blocks. A message block is essentially memory available for creating or storing packets where a packet is usually an Ethernet frame. There are four types of message blocks, and each type represents a collection of buffers which are of the same size.

Packet Holding Message Blocks...
Provides buffer usage of T-DAC message blocks based upon message block sizes.

Total (boxMsgBlksConfigured)
The total number of message blocks on the system.

Free (boxMsgBlksFree)
The number of free message blocks available.

Total Time Waited (boxCountMsgBlkTaskWait)
The total number of times that the proper size message block was not available to hold a packet, and the CPU task went to sleep while waiting for it.

Total Times Unavailable (boxCountMsgBlkUnavailable)
The total number of times that the proper size message block was not available to hold a packet, and the CPU task dumped the packet. The difference between Total Time Waited and Total Times Unavailable is whether the CPU task goes to sleep or simply dumps the packet to continue on.

Figure 101. System main window (Operating System Heap Memory, Enclosure System, Installation, and Other)

System Information—Operating System Heap Memory

This portion of the System main window shown in figure 101 contains information about the memory used by the CPU and its management tasks.

Total Size (boxHeapSize)
The size in octets of the operating system heap memory.

Free (boxHeapFreeSpace)
The amount of operating system heap memory in octets currently available.

Largest (boxHeapLargestSpace)
The largest contiguous memory block in octets in the memory heap.

System Information—Enclosure System

This portion of the System main window shown in figure 101 contains information about the internal temperature of the DACS.

Internal Temperature (boxTemperature)
Displays the current temperature in celsius (centigrade).

Highest Temperature (boxMaxTemperature)
The highest temperature registered in celsius (centigrade) since the DACS was last re-booted.

System Information—Installation

This portion of the System main window shown in figure 101 on page 191 contains information described in this following section.

Country (installCountry)
Specifies the country that the DACS is installed in so it can be configured in accordance with local laws.

System Information—Other

This portion of the System main window shown in figure 101 on page 191 contains information described in the following sections.

Total DRAM Detected (boxDetectedMemory)
The total number of bytes of DRAM detected by the CPU.

SystemID (sysObjectID)
This SNMP variable defines the type of the DACS being managed as defined by specification RFC1213.MIB.

Running Since Last Boot (sysUpTime)
This SNMP variable represents the time since the network management portion of the system was last re-initialized.

System Manager (sysContact)
This SNMP variable represents the textual identification of the contact person for this managed node, which may include information on how to contact this person as defined by specification RFC1213.MIB. The maximum length of this field is 256 octets.

Box Name (sysName)
This is "An administratively assigned name for this managed node. By convention, this is the node's fully-qualified domain name." (RFC1213.MIB).

Physical Location (sysLocation)
"The physical location of this node (e.g., telephone closet, 3rd floor)." (RFC1213.MIB).

Background Image (boxBackgroundFlag)
The following options are available:

- disableGraphics(0)—When this option is selected, graphics on WWW pages will not be displayed. This results in faster page display times, but may make it more difficult to navigate WWW sites that rely heavily on graphics.
- enableGraphics(1)—When this option is selected, graphics on WWW pages are displayed.
- disableWeb(2)—When this option is selected, access to the WWW pages is denied for everyone.

Monitor Privilege (boxMonitorPrivilege)

Specifies the privileges given to the monitor user. Privileges can be removed or additional write access can be given beyond read-only access. The following options are available:

- none(0)—The monitor user can not log in.
- read only(2)—This is the default setting. The monitor user can view but not change any parameters. Monitor can not view passwords.
- writeUser(18)—Not supported.
- writeUserlp(50)—The monitor user can change all parameters—except passwords— IP links.
- writeUserlpWan(114)—The monitor user can change all parameters—except passwords— IP, and T1/E1.
- writeUserlpWanSystem(242)—The monitor user can change all parameters—except passwords— IP, T1/E1, System, and System Log links.
- writeUserlpWanSystemUpload(498)—The monitor user can change all parameters—except passwords—IP, T1/E1, System, and System Log links. The monitor user can also load firmware updates into the T-DAC.

System (configurable parameters) window

The System (configurable Parameters) window (see figure 102) provides the means for you to modify the values for T-DAC System configurable parameters in the SNMP and HTTP, LAN IP, Installation, and Other System Information tables. To display the System (configurable parameters) window, on the System main window, click the Modify… link.

Figure 102. System (configurable parameters) window

The following sections describe the configurable parameters displayed on the System window.

SNMP and HTTP

This portion of the System window shown in figure 102 provides information about the SNMP version and the HTTP accessibility.

Version (boxSnmpVersion)

This parameter selects the SNMP version number supported by this unit. Select snmpv1(1) only, SNMP2 is not currently supported.

Superuser Password (boxSnmpMasterPassword)

This accesses the super user password for complete access and configurability of the T-DAC through SNMP and HTTP. Up to 64 octets (characters).

Superuser Password Verification (boxSnmpVerifyMasterPassword)
This is verification for the password. It must be set before replacing the old password with the new one.

User Password (boxSnmpMonitorPassword)
This accesses the user monitoring password for read only access of certain selected information. Not all parameters shown using the superuser password are displayed under the user password.

User Password Verification (boxSnmpVerifyPassword)
This is verification for the password. It must be set before replacing the old password with the new one.

LAN IP

This portion of the System window shown in figure 102 on page 194 contains configurable information for the IP addressing of the Ethernet LAN port.

Method to Obtain Address (boxIpAddressTechnique)
This indicates how to obtain the LAN IP address. The following options are available:

- disable(0)—Ethernet port is disabled
- static(1)—LAN IP address is obtained from EIA-232 Control Port
- rarp(2)—Reverse Address Resolution Protocol—A protocol defined in RFC 903 which provides the reverse function of ARP. RARP maps a hardware address (MAC address) to an Internet address. It is used primarily by diskless nodes, when they first initialize, to find their Internet address.
- bootp(3)—The Bootstrap Protocol. A protocol described in RFCs 951 and 1084 and used for booting diskless workstations.
- dhcp(4)—Dynamic Host Configuration Protocol—A protocol introduced by Microsoft on their NT server with version 3.5 in late 1994. This protocol provides a means to dynamically allocate IP addresses to IBM PCs running on a Microsoft Windows local area network. The system administrator assigns a range of IP addresses to DHCP and each client PC on the LAN has its TCP/IP software configured to request an IP address from the DHCP server. The request and grant process uses a lease concept with a controllable time period. More information can be found in the Microsoft documentation on NT Server.

Address (boxIpAddress)
If the address technique above is static then this represents the LAN IP address.

Mask (boxIpMask)
If the address technique above is static then this represents the LAN IP mask.

Installation

This portion of the System window shown in figure 102 on page 194 contains information described in the following section.

Country (installCountry)

Specifies the country that the T-DAC is installed in so it can be configured in accordance with local laws. The following options are available:

- other(0)
- unitedStates(1)
- australia(2)
- canada(3)
- europeanUnion(4)
- france(5)
- germany(6)

Other

This portion of the System window (shown in figure 102 on page 194) contains information described in the following sections.

System Manager (sysContact)

This SNMP variable represents the textual identification of the contact person for this managed node, together with information on how to contact this person as defined by specification RFC1213.MIB.

Box Name (sysName)

This is "An administratively assigned name for this managed node. By convention, this is the node's fully-qualified domain name." (RFC1213.MIB)

Physical Location (sysLocation)

"The physical location of this node (e.g., 'telephone closet, 3rd floor')." (RFC1213.MIB)

Web Settings (boxBackgroundFlag)

The following options are available:

disableGraphics(0)—When this option is selected, graphics on WWW pages will not be displayed. This results in faster page display times, but may make it more difficult to navigate WWW sites that rely heavily on graphics.

enableGraphics(1)—When this option is selected, graphics on WWW pages are displayed.

disableWeb(2)—When this option is selected, access to the WWW pages is denied for everyone.

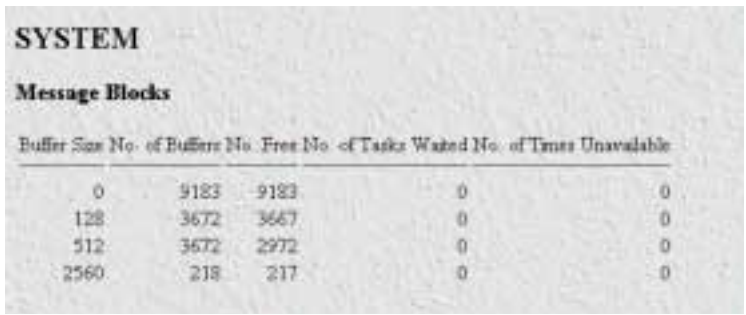
Monitor Privilege (boxMonitorPrivilege)

Specifies the privileges given to the monitor user. Privileges can be removed or additional write access can be given beyond read-only access. The following options are available:

- none(0)—The monitor user can not log in.
- read only(2)—This is the default setting. The monitor user can view but not change any parameters. Monitor can not view passwords.
- writeUser(18)—The monitor user can change all parameters—except passwords— under authentication, drop-and-insert, and dial-in links.
- writeUserIp(50)—The monitor user can change all parameters—except passwords— under authentication, drop-and-insert, dial-in, and IP links.
- writeUserIpWan(114)—The monitor user can change all parameters—except passwords— under authentication, drop-and-insert, dial-in, IP, T1/E1, and Frame Relay links.
- writeUserIpWanSystem(242)—The monitor user can change all parameters—except passwords— under authentication, drop-and-insert, dial-in, IP, T1/E1, Frame Relay, System, and System Log links.
- writeUserIpWanSystemUpload(498)—The monitor user can change all parameters—except passwords— under authentication, drop-and-insert, dial-in, IP, T1/E1, Frame Relay, System, and System Log links. The monitor user can also load firmware updates into the DACS.

System (Message Blocks) window

The 3096RC T-DAC system manages the i960 processor utilization by allocating message blocks for packet management. The System (Message Blocks) window (see figure 103) displays statistics about the T-DAC's buffer usage for messages according to the size of the message block size required. To display the System (Message Blocks) window, on the System main window, click the Packet Holding Message Blocks... hyperlink


SYSTEM

Message Blocks

Buffer Size	No. of Buffers	No. Free	No. of Tasks Waited	No. of Times Unavailable
0	9183	9183	0	0
128	3672	3667	0	0
512	3672	2972	0	0
2560	218	217	0	0

Figure 103. Packet Holding Message Blocks window

The following sections describe the statistical counters displayed on the System (Message Blocks) window.

Buffer Size (boxBufferSize)

The size in bytes of the buffer.

No. of Buffers (boxBufferCount)

The total number of buffers this size.

No. Free (boxBuffersFree)

The number of buffers this size which are currently free for use.

No. of Tasks Waited (boxCountBufferTaskWait)

The total number of times that the proper size message block was not available to hold a packet, and the CPU task went to sleep while waiting for it.

No. of Times Unavailable(boxCountBufferUnavailable)

The total number of times that the proper size message block was not available to hold a packet, and the CPU task dumped the packet. The difference between Total Time Waited and Total Times Unavailable is whether the CPU task goes to sleep or simply dumps the packet to continue on.

Chapter 21 System Log

Chapter contents

Introduction

The T-DAC software provides a system log utility. The system log subsystem generates an event message for certain errors and significant occurrences within the T-DAC system. The T-DAC can store these system log messages in memory, or send them to another device for processing and/or monitoring by an operator. Each message type has a defined priority level. You can tell the T-DAC where to send system log messages based on the priority of the message. The T-DAC can send system log messages to the following destinations:

- Flash memory—The T-DAC's Non-volatile Read-only Memory (NVRAM)
- RAM—The T-DAC's Random Access Memory (RAM)
- Config port—The T-DAC's RS-323 control port presented as an RJ-45 connector on the front panel
- SNMP Trap Daemon—An external host computer running SNMP TRAP Daemon software. An SNMP Trap Daemon collects and stores SNMP trap messages for processing and/or operator monitoring.
- SysLog Daemon—An external host computer running SysLog Daemon software. A SysLog Daemon collects and stores SysLog messages for processing and/or operator monitoring.

Note Object identifiers specified in the Patton Enterprise MIB define the T-DAC's System Log parameters.

System Log main window

The System Log main window (see figure 104) provides the means for you to manage the T-DAC's System Log subsystem. To display the System Log main window, on the T-DAC's configuration menu pane, click the System Log link.

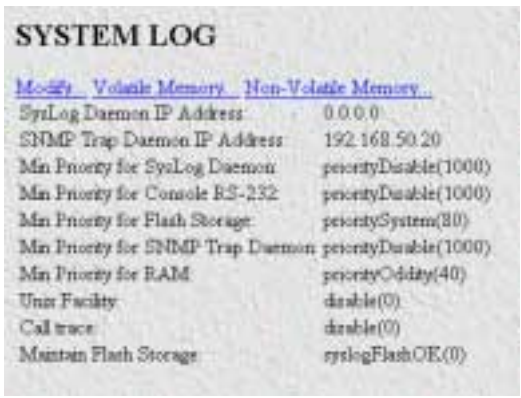


Figure 104. System Log main window

The System Log main window provides hyperlinks to the System Log (configuration), System Log (volatile Memory) and System Log (Non-Volatile Memory) windows, as shown in figure 105.

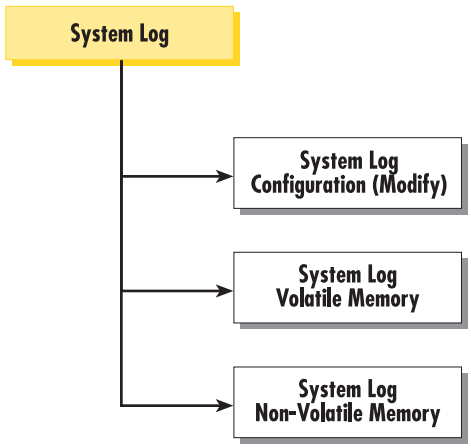


Figure 105. System Log windows map

You can use the System Log windows to

- View and define configurable parameters that control the operation of the System Log subsystem
- View the System Log messages the T-DAC currently stores in
  - Volatile Memory
  - Non-Volatile memory

The following sections describe the contents of the System Log main window.

Figure 106. Hyperlinks section of the System Log main window

Hyperlinks

The System Log main window displays the following hyperlinks (see figure 106):

- Modify—Clicking on the Modify… link displays the System Log (configuration) window. You can use the System Log (configuration) sub-window to view and modify the values of syslog configurable parameters. The System Log (configuration) window is described later in this chapter "System Log (configuration) window" on page 205
- Volatile Memory—Clicking on the Volatile Memory… link displays the System Log (Volatile Memory) window, where you can view the system log messages currently stored in the T-DAC's volatile Direct Random Access Memory (DRAM). The System Log (Volatile Memory) window is described later in this chapter "System Log—Volatile Memory window" on page 208
- Non-Volatile Memory—Clicking on the Non-Volatile Memory… link displays the System Log (Non-Volatile Memory window) where you can view the system log messages currently stored in the T-DAC

NVRAM. The System Log (Non-Volatile Memory window is described later in this chapter "System Log—Non-Volatile Memory window" on page 209

Figure 107. Parameters section of the System Log main window

System Log parameters

The following sections describe the System Log parameters (see figure 107).

SysLog Daemon IP Address(syslogDaemonIP)

The IP address of a host computer system which is running a syslog daemon. System messages with a priority greater than or equal to the configurable syslogDaemonPriority will be sent to this IP address (see section "Priority" on page 206).

SNMP Trap Daemon IP Address (syslogTrapIP)

The IP address of a host system which is running a SNMP trap daemon. SNMP Trap messages with a priority greater than or equal to the configurable syslogTrapPriority will be sent to this IP address.

Min Priority for SysLog Daemon (syslogDaemonPriority)

System messages which have a priority equal to or greater than this setting will be sent to the syslog daemon defined by the SysLog Daemon IP Address (syslogDaemonIP).

- priorityVerbose(5)
- priorityDebug(10)
- priorityInfo(20)
- priorityOddity(40)
- priorityService(60)
- prioritySystem(80)
- priorityDisable(1000)

Min Priority for Console RS-232 (syslogConsolePriority)

System messages which have a priority equal to or greater than this setting will be sent directly to the RS-232 Config control port (RJ-45 connector labeled "Config") on the front panel of the 3096RC T-DAC. Messages will be sent regardless of the current operating state of the RS- 232 configuration port. The lower the number

next to the priority listed below, the more details system logging will provide. priorityVerbose will generate the most messages, while priorityDisable will turn off all messages.

- priorityVerbose(5)
- priorityDebug(10)
- priorityInfo(20)
- priorityOddity(40)
- priorityService(60)
- prioritySystem(80)
- priorityDisable(1000)

Min Priority for Flash Storage (syslogFlashPriority)

System messages which have a priority equal to or greater than this setting will be permanently stored in the Flash PROM. Due to being permanent memory, the Flash memory eventually becomes filled. When this occurs, the memory must be cleared before accepting more messages. Some maximum number of messages may be stored in the Flash PROM before this storage area must be cleared.

- prioritySystem(80)—Flash PROM will be used to store system-level messages.
- priorityDisable(1000)—No messages will be stored.

Min Priority for SNMP Trap Daemon (syslogTrapPriority)

System messages which have a priority equal to or greater than this setting will be sent to the SNMP Trap Daemon IP Address (syslogTrapIP). The lower the number next to the priority listed below, the more details system logging will provide. Selecting *priorityVerbose* will generate the most messages, while selecting *priorityDisable* will turn off all messages.

- priorityVerbose(5)
- priorityDebug(10)
- priorityInfo(20)
- priorityOddity(40)
- priorityService(60)
- prioritySystem(80)
- priorityDisable(1000)

Min Priority for RAM (SyslogTablePriority)

System messages which have a priority equal to or greater than this setting will appear in System Log—Volatile Memory. The lower the number next to the priority listed below, the more details system logging will provide. Selecting *priorityVerbose* will generate the most messages, while selecting *priorityDisable* will turn off all messages.

- priorityVerbose(5)
- priorityDebug(10)
- priorityInfo(20)

- priorityOddity(40)
- priorityService(60)
- prioritySystem(80)
- priorityDisable(1000)

Unix Facility (syslogUnixFacility)

This setting is used when syslog messages are sent to a Unix-type syslog daemon. In this case the message will include the facility and priority coding.

- disable(0)
- user(1)
- mail(2)
- daemon(3)
- auth(4)
- syslog(5)
- lpr(6)
- news(7)
- uucp(8)
- cron(9)
- authpriv(10)
- ftp(11)
- local0(16)
- local1(17)
- local2(18)
- local3(19)
- local4(20)
- local5(21)
- local6(22)
- local7(23)

Call Trace (syslogCallTrace)

Enabling this will activate the call tracing utility. This is a powerful debugging utility which will log every single function call and return. At the death of a box the call trace will be printed out and can be sent to tech support. This utility will take a large amount of CPU power.

- disable(0)—Disable function call tracing.
- enable(1)—Enable function call tracing.
- dump(2)—Display function call tracing on the computer monitor.

Maintain Flash Storage (syslogFlashClear)

This parameter provides two functions:

- You can read the value of this parameter to learn the status of the System Log Message cache in flash memory.
- You can set the value to syslogFlashClear to erase (clear) the messages in the System Log Message cache in flash memory.

The following values are defined:

- syslogFlashOK(0)—As long as the T-DAC's flash memory is accepting system log messages, the T-DAC will set the value of syslogFlashClear(2) to syslogFlashOK(0).
- syslogFlashFull(1)—When Flash is rejecting system log messages because the message cache is full, the T-DAC will set the value of syslogFlashClear(2) to syslogFlashFull(1). To correct this condition by erasing the messages in (clearing) flash memory, select the value syslogFlashClear(2) from the drop-down menu, and click the [submit query] button.
- syslogFlashClear(2)—When you set the value of syslogFlashClear to syslogFlashClear(2) and click the [submit query] button, the T-DAC will erase all system log messages stored in Flash.

System Log (configuration) window

The System Log (configuration) window (see figure 108) provides the means for you to view and modify the values of System Log parameters. The parameters define displays SysLog and SNMP Trap Daemon IP Address locations, message priorities for the offered SysLog message destinations, and other priority and maintenance information. To display the System Log (configuration) window, on the System Log main window, click the Modify… link.

Figure 108. System Log—Modify window

The following sections describe the System Log configurable parameters.

Daemons

This portion of the System Log (Configuration) window displays the parameters that define the IP address for the SysLog Daemon and the IP address for the SNMP Trap Daemon.

SysLog Daemon IP Address(syslogDaemonIP)

The IP address of a host computer system which is running a syslog daemon. System messages with a priority greater than or equal to the configurable syslogDaemonPriority will be sent to this IP address (see section "Priority" on page 206).

SNMP Trap Daemon IP Address (syslogTrapIP)

The IP address of a host system which is running a SNMP trap daemon. SNMP Trap messages with a priority greater than or equal to the configurable syslogTrapPriority will be sent to this IP address.

Priority

This portion of the System Log (Configuration) window displays the parameters that define the Message Priority level for the System Log message destinations.

Min Priority for SysLog Daemon (syslogDaemonPriority)

System messages which have a priority equal to or greater than this setting will be sent to the syslog daemon defined by the SysLog Daemon IP Address (syslogDaemonIP).

- priorityVerbose(5)
- priorityDebug(10)
- priorityInfo(20)
- priorityOddity(40)
- priorityService(60)
- prioritySystem(80)
- priorityDisable(1000)

Min Priority for Console RS-232 (syslogConsolePriority)

System messages which have a priority equal to or greater than this setting will be sent directly to the RS-232 control port (RJ-45 connector labeled "Config") on the front panel of the 3096RC T-DAC. Messages will be sent regardless of the current operating state of the RS- 232 configuration port. The lower the number next to the priority listed below, the more details system logging will provide. Selecting *priorityVerbose* will generate the most messages, while selecting *priorityDisable* will turn off all messages.

- priorityVerbose(5)
- priorityDebug(10)
- priorityInfo(20)
- priorityOddity(40)
- priorityService(60)
- prioritySystem(80)
- priorityDisable(1000)

Min Priority for Flash Storage (syslogFlashPriority)

System messages which have a priority equal to or greater than this setting will be permanently stored in the Flash PROM. Due to being permanent memory, the Flash memory eventually becomes filled. When this occurs, the memory must be cleared before accepting more messages. Some maximum number of messages may be stored in the Flash PROM before this storage area must be cleared.

- prioritySystem(80)—Flash PROM will be used to store system-level messages.
- priorityDisable(1000)—No messages will be stored.

Min Priority for SNMP Trap Daemon (syslogTrapPriority)

System messages which have a priority equal to or greater than this setting will be sent to the SNMP Trap Daemon IP Address (syslogTrapIP). The lower the number next to the priority listed below, the more details system logging will provide. Selecting *priorityVerbose* will generate the most messages, while selecting *priorityDisable* will turn off all messages.

- priorityVerbose(5)
- priorityDebug(10)
- priorityInfo(20)
- priorityOddity(40)
- priorityService(60)
- prioritySystem(80)
- priorityDisable(1000)

Min Priority for RAM (SyslogTablePriority)

System messages which have a priority equal to or greater than this setting will appear in System Log—Volatile Memory. The lower the number next to the priority listed below, the more details system logging will provide. Selecting *priorityVerbose* will generate the most messages, while selecting *priorityDisable* will turn off all messages.

- priorityVerbose(5)
- priorityDebug(10)
- priorityInfo(20)
- priorityOddity(40)
- priorityService(60)
- prioritySystem(80)
- priorityDisable(1000)

Unix Facility (syslogUnixFacility)

This setting is used when syslog messages are sent to a Unix-type syslog daemon. In this case the message will include the facility and priority coding.

- disable(0)
- user(1)
- mail(2)
- daemon(3)
- auth(4)
- syslog(5)
- lpr(6)
- news(7)
- uucp(8)
- cron(9)
- authpriv(10)
- ftp(11)
- local0(16)
- local1(17)
- local2(18)
- local3(19)
- local4(20)
- local5(21)
- local6(22)
- local7(23)

Call Trace (syslogCallTrace)
Enabling this will activate the call tracing utility. This is a powerful debugging utility which will log every single function call and return. At the death of a box the call trace will be printed out and can be sent to tech support. This utility will take a large amount of CPU power.

- disable(0)—Disable function call tracing.
- enable(1)—Enable function call tracing.
- dump(2)—Display function call tracing on the computer monitor.

Maintenance
This portion of the System Log (configuration) window displays the parameter used to manage the System Log Message cache in the T-DAC's flash memory.

Maintain Flash Storage (syslogFlashClear)
This parameter provides two functions:

- You can read the value of this parameter to learn the status of the System Log Message cache in flash memory.
- You can set the value to syslogFlashClear to erase (clear) the messages in the System Log Message cache in flash memory.

The following values are defined:

- syslogFlashOK(0)—As long as the T-DAC's flash memory is accepting system log messages, the T-DAC will set the value of syslogFlashClear(2) to syslogFlashOK(0).
- syslogFlashFull(1)—When Flash is rejecting system log messages because the message cache is full, the T-DAC will set the value of syslogFlashClear(2) to syslogFlashFull(1). To correct this condition by erasing the messages in (clearing) flash memory, select the value syslogFlashClear(2) from the drop-down menu, and click the [submit query] button.
- syslogFlashClear(2)—When you set the value of syslogFlashClear to syslogFlashClear(2) and click the [submit query] button, the T-DAC will erase all system log messages stored in Flash.

System Log—Volatile Memory window
The System Log—Volatile Memory window (see figure 109) displays the time-stamped system log messages currently stored in the T-DAC's volatile memory. To display the System Log (Volatile Memory) window, on the System Log main window, click the Volatile Memory… hyperlink.

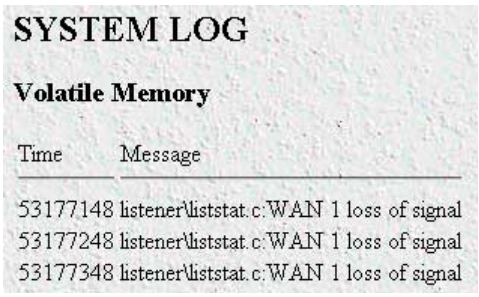


Figure 109. System Log—Volatile Memory window

The System Log—Volatile window displays information described in the following sections.

Time (slTick)
Time stamps are generated every 10 ms.

Message (slMessage)
This is the message stored in RAM. If the T-DAC loses power, the messages stored in volatile RAM will be lost.

System Log—Non-Volatile Memory window

The System Log—Non-Volatile window (see figure 110) displays the time-stamped system log messages currently stored in the T-DAC's non-volatile Flash memory. To display the System Log (Non-Volatile Memory) window, on the System Log main window, click the Non-Volatile Memory… hyperlink.

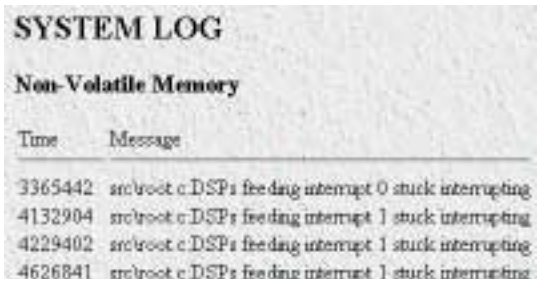


Figure 110. System Log—Non-Volatile Memory window

The System Log—Non-Volatile window displays information described in the following sections.

Time (slfTick)
Time stamps are generated every 10 ms.

Message (slfMessage)
This is the message stored in Flash memory. If the T-DAC loses power, the messages stored in non-volatile flash memory will ***not*** be lost.

Chapter 22 T1/E1 Link

Chapter contents

Introduction

T1/E1 Link Activity Overview window (see figure 111) provides the means for you to manage the T1/E1 Link subsystem. The T1/E1 Link Activity Overview page provides a quick summary of all 4, 8, 12 or 16 WAN ports. For each of the T-DAC's WAN ports, the summary shows the "Circuit ID," "Line Type," and "Line Status" for that T1 or E1 link. By clicking of the View Link hyperlink for a certain port, you can view that port's configuration, line status, and statistics. Line Status indicates whether or not an alarm condition exists. Statistics provide information about the quality of the WAN connection.

Note *RFC 140—Definitions of Managed Objects for the DS1 and E1 Interface Types* specifies the statistics the T-DAC's T1/E1 Link subsystem displays.

To display the T1/E1 Link Activity Overview window, on the T-DAC's Configuration Menu pane, click the T1/E1 Link hyperlink.

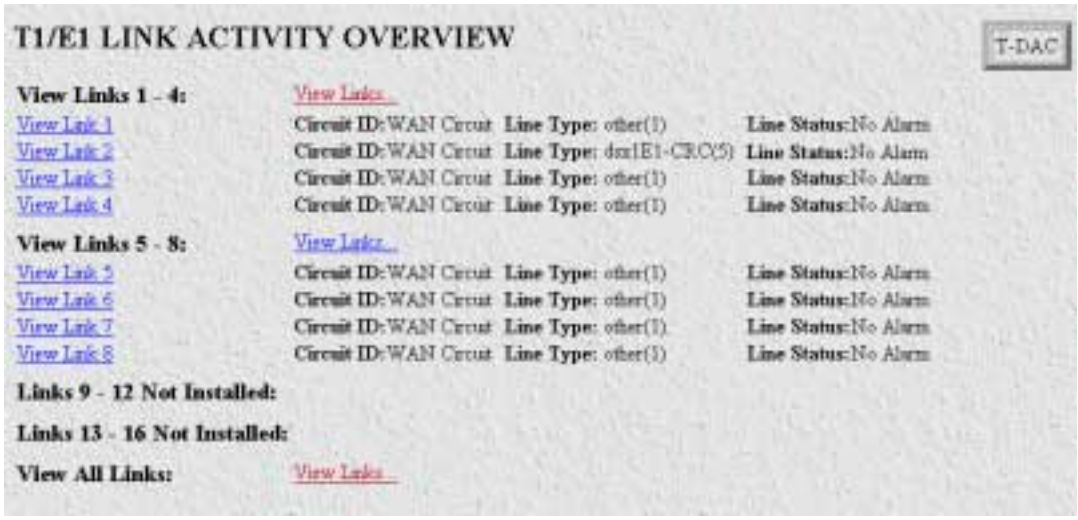


Figure 111. T1/E1 Link Activity Overview window

The T1/E1 Link Activity Overview window provides links to the windows shown in figure 112.

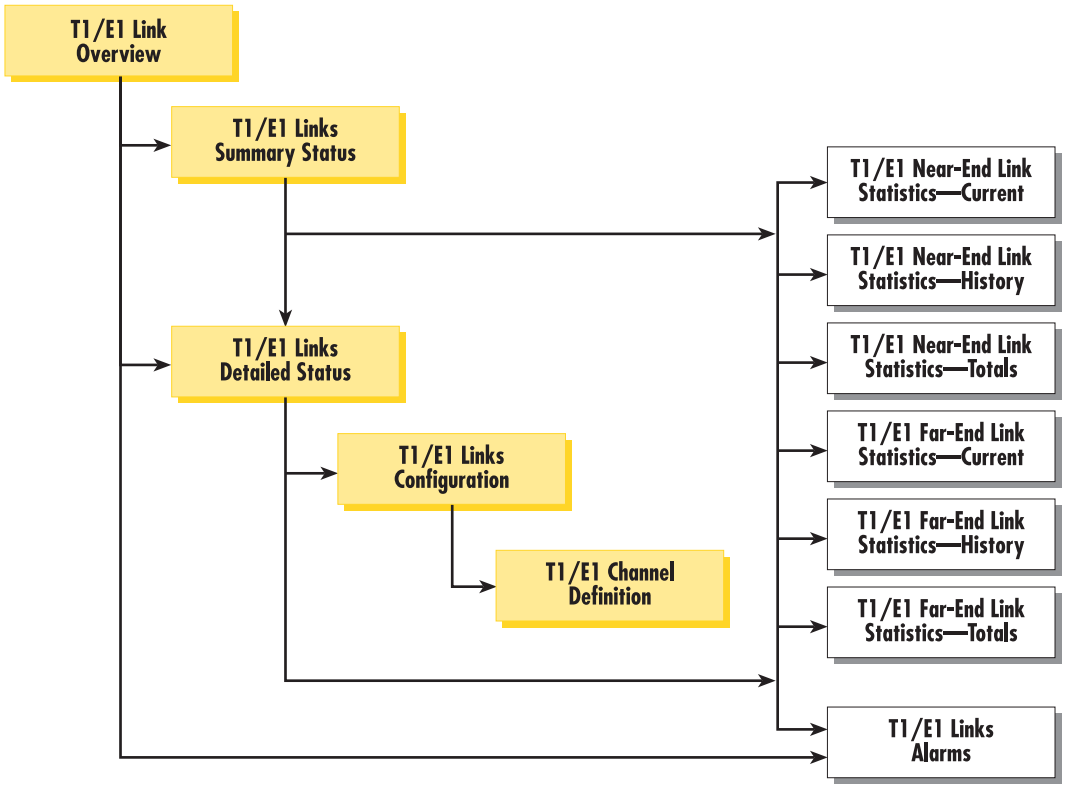


Figure 112. T1/E1 Link Activity windows map

The T1/E1 Link Activity Overview main window contains the following items:

- View Links 1–4, View Links 5–8, View Links 9–12, and View Links 13–16. These links lead to windows that display supporting information on the WAN ports.
- View Links…. Clicking on these links display the T1/E1 Link Activity Ports windows which display Line Status, Near End Line Statistics, and Far End Line Statistics for each WAN port.
- The four groups have individual hyperlinks named View Link 1, View Link 2, … View Link 16 to windows named WAN Circuit Configuration Link: 1, … WAN Circuit Configuration Link: 16. Each of these windows displays the configuration settings for the T1/E1 port, the line status showing whether any alarms are present, hyperlinks to statistical data, and another hyperlink for modifying the configuration (Modify Configuration…).

- If an alarm or alarms are present for a specific WAN port, a hyperlink beside Line Status: will state *Alarms Present* (see figure 113). The associated web page called Circuit ID # Line Status Alarms points out the indication for the type of alarm.

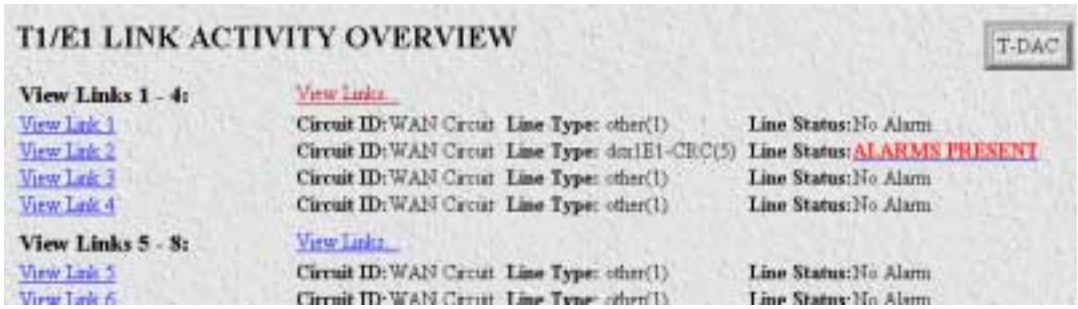


Figure 113. T1/E1 Link Activity Overview window displaying an alarm condition

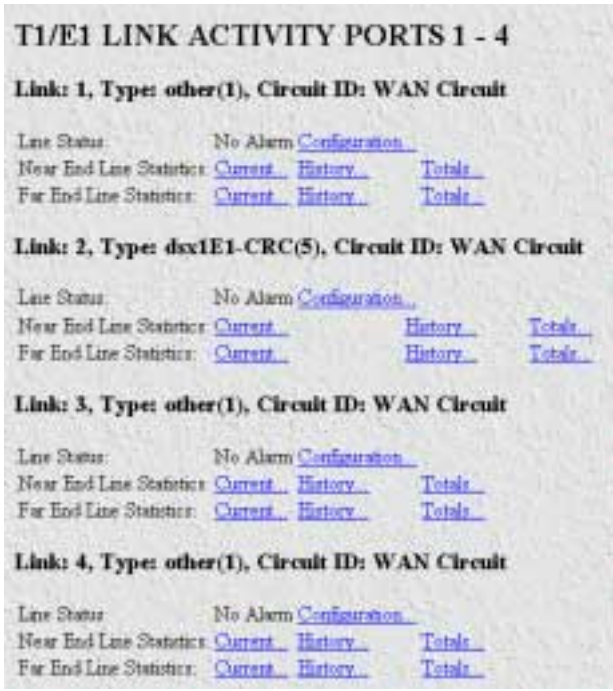


Figure 114. T1/E1 Link Activity Ports 1 - 4 window

T1/E1 Link Activity Ports window

Click on a View Links… link in the T1/E1 Link Activity Overview window to display the T1/E1 Link Activity Ports window (see figure 114). The T1/E1 Link Activity Ports window is divided into sections that display the following T1/E1 parameters:

- Line Status—Shows the configuration of the T1/E1 Interface and service provided on each user time slot.
- Configuration—Links to a window where you can configure the WAN port.
- Near End Line Statistics—Show error statistics collected from the near-end of the T1/E1 line.

- Far End Line Statistics—Show statistics collected from the far-end T1/E1 line. Far End Line Statistics can be used by devices that support the facility data link (FDL)

Link (dsx1LineIndex)

This object identifies a DS1 Interface on a managed device. If there is an ifEntry directly associated with this DS1 interface, it must have the same value as ifIndex. Otherwise, the value exceeds ifNumber, and is assigned a unique identifier by following this rule: inside interfaces (equipment side) with even numbers and outside interfaces (network side) with odd numbers.

Type (dsx1LineType)

This variable indicates the type of DS1 line using the circuit. The circuit type determines the bits-per-second rate that the circuit can carry and how it interprets error statistics. The values are as follows:

- Other(1)—Link is disabled
- dsx1ESF(2)—Extended Superframe DS1
- dsx1D4(3)—AT&T D4 format DS1
- dsx1E1(4)—Based on CCITT/ITU G.704 without CRC (Cyclical Redundancy Check)
- dsx1E1-CRC(5)—Based on CCITT/ITU G.704 with CRC (Cyclical Redundancy Check)
- dsx1E1-MF(6)—Based on CCIT/ITU G.704 without CRC (bit oriented signaling)
- dsx1E1-CRC-MF(7)—Based on CCIT/ITU G.704 with CRC (bit oriented signaling)
- dsx1E1-Transparent(8)—Based on CCIT/ITU G.703 without CRC (Cyclical Redundancy Check)

Circuit ID (dsx1CircuitIdentifier)

This is the transmission vendor's circuit identifier. Knowing the circuit ID can be helpful during troubleshooting.

Line Status (dsx1LineStatus)

This variable indicates interface line status. It contains loopback, failure, received alarm and transmitted alarm information. If any condition other than No Alarms exists, you can click on the Alarms Present link to view the Line Status Alarms page (see figure 115).

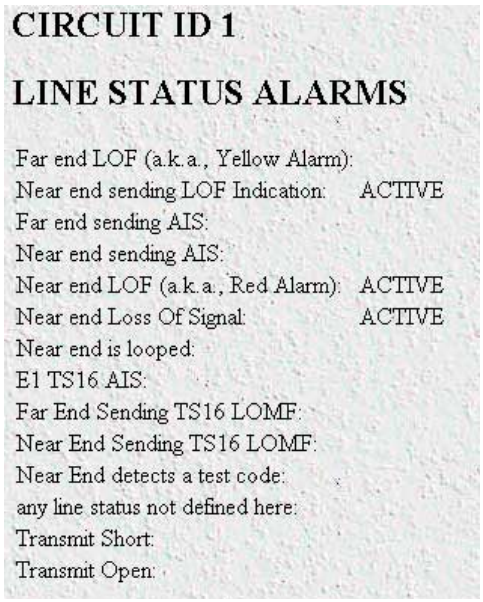


Figure 115. Line Status Alarms window

The alarms currently present on the line will be indicated by the ACTIVE label next to the alarm type.

Failure States

The following failure states are reported in the dsx1LineStatus object. The items listed in this section comprise those contained in *RFC 1406—Definitions of Managed Objects for the DS1 and E1 Interface Types*.

Far End Alarm Failure (Far end LOF)

Far End Alarm failure is also known as a Yellow Alarm in the T1 case or Distant Alarm in the E1 case. It occurs under the following conditions:

- For D4 links, the Far End Alarm failure occurs when bit 6 of all channels has been zero for at least 335 ms. The alarm is cleared when bit 6 of at least one channel is non-zero for a period T, where T is usually less than 1 second and always less than 5 seconds. The Far End Alarm failure is not declared for D4 links when a Loss of Signal is detected.
- For ESF links, the Far End Alarm failure is declared if the Yellow Alarm signal pattern occurs in at least 7 out of 10 contiguous 16-bit pattern intervals. The alarm is cleared when the Yellow Alarm signal pattern has not occurred for 10 contiguous 16-bit signal pattern intervals.
- For E1 links, the Far End Alarm failure is declared when bit 3 of time-slot zero is received set to 1 on two consecutive occasions. The Far End Alarm failure is cleared when bit 3 of time-slot zero is received set to zero.

Alarm Indication Signal (AIS) Failure (Near end or far end sending AIS)

The Alarm Indication Signal failure is declared when an AIS defect is detected at the input and the AIS defect still exists after the Loss Of Frame failure (which is caused by the unframed nature of the all-ones signal) is declared. The AIS failure is cleared when the Loss Of Frame failure is cleared.

Loss Of Frame Failure (Near end LOF)

Occurs under the following conditions:

- For T1 links, the Loss Of Frame failure is declared when an OOF or LOS defect has persisted for T seconds, where $2 \leq T \leq 10$. The Loss Of Frame failure is cleared when there have been no OOF or LOS defects during a period T where $0 \leq T \leq 20$. Many systems will perform *hit integration* within the period T before declaring or clearing the failure (for more information, see TR 62411 [16]).
- For E1 links, the Loss Of Frame Failure is declared when an OOF defect is detected.

Loss Of Signal Failure (Near end loss of signal)

Occurs under the following conditions:

- For T1, the Loss Of Signal failure is declared upon observing 175 ±75 contiguous pulse positions with no pulses of either positive or negative polarity. The LOS failure is cleared upon observing an average pulse density of at least 12.5% over a period of 175 ±75 contiguous pulse positions, starting with the receipt of a pulse.
- For E1 links, the Loss Of Signal failure is declared when greater than 10 consecutive zeroes are detected (see O.162 Section 3.4.4).

Loopback Pseudo-Failure (Near end is looped)

The Loopback Pseudo-Failure is declared when the near end equipment has placed a loopback (of any kind) on the DS1. This allows a management entity to determine from one object whether the DS1 can be considered to be in service or not (from the point of view of the near end equipment).

TS16 Alarm Indication Signal Failure (E1 TS16 AJS)

For E1 links, the TS16 Alarm Indication Signal failure is declared when time-slot 16 is received as all ones for all frames of two consecutive multiframes (see G.732 Section 4.2.6). This condition is never declared for T1.

Loss Of MultiFrame Failure (Near end sending TS16 LOMF)
The Loss Of MultiFrame failure is declared when two consecutive multiframe alignment signals (bits 4 through 7 of TS16 of frame 0) have been received with an error. The Loss Of Multiframe failure is cleared when the first correct multiframe alignment signal is received. The Loss Of Multiframe failure can only be declared for E1 links operating with G.732 [18] framing (sometimes called Channel Associated Signalling mode).

Far End Loss Of Multiframe Failure (Far end sending LOMF
The Far End Loss Of Multiframe failure is declared when bit 2 of TS16 of frame 0 is received set to one on two consecutive occasions. The Far End Loss Of Multiframe failure is cleared when bit 2 of TS16 of frame 0 is received set to zero. The Far End Loss Of Multiframe failure can only be declared for E1 links operating in Channel Associated Signalling mode.

Near End Detects a Test Code
The Near End T1/E1 port has detected an incoming loop code. Upon detecting this loop code the T1/E1 port may enter a loop status. Any coming on the particular T1/E1 port will be transmitted back to the originator.

Any Line Status not Defined Here
The T1/E1 port has detected a condition on the line that is not defined in any of the failure modes listed on this screen.

Transmit Short
An internal condition detected by the T1/E1 transceiver—useful for technical personnel while troubleshooting at the board level.

Transmit Open
An internal condition detected by the T1/E1 transceiver—useful for technical personnel while troubleshooting at the board level.

Line Status—Configuration

Clicking on the Line Status—Configuration hyperlink in the T1/E1 Link Activity Ports page displays the WAN Circuit Configuration hyperlink page (see figure 116). This page contains general information about the WAN interface, including the type of line (D4 Superframe or Extended Superframe), type of line coding (B8ZS or AMI), Near and Far End Line Statistics, and Line Status. On this page, is the ability to modify the Line Interface Settings and Test Settings by clicking on the Modify Configuration link as well as modifying the channel assignments by clicking on the Channel Assignments link. Also on this page is the ability to retrieve both Near and Far End Line Statistics by clicking on Current, History, or Totals.

Figure 116. WAN Circuit Configuration Link window

Note Click on the Modify link to change the settings of any of the following parameters (see "WAN Circuit Configuration—Modify" on page 222).

The WAN Circuit Configuration window also displays the amount of time that has passed, the number of intervals passed during which valid data was collected, and a measurement of received signal quality.

Time Elapsed (dsx1TimeElapsed)

The number of seconds that have elapsed since the beginning of the current error-measurement period.

Valid Intervals (dsx1ValidIntervals)

The number of previous intervals for which valid data was collected. The value will be 96 unless the interface was brought on-line within the last 24-hours, in which case the value will be the number of completed 15-minute intervals since the interface has been online. Statistics are collected for up to the last 24 hour period broken down into 96 individual 15-minute intervals.

Receiver Quality

Located in the Line Interface Settings portion of the WAN Circuit Configuration Link window, the Receiver Quality measurement displays the atenuation of the signal received on the link and depends on the Receiver Sensitivity setting (see "Receiver Sensitivity (linkSensitivityLevel)" on page 224). This value can be from 0dB to -43dB. The measurement displayed will be formatted as follows: a value of -3.5dB would be shown as *3_5*, a value of -11.9dB would be shown as *11_9* (the minus sign is not displayed and the decimal point is converted to an underscore).

Note This is only displayed if the receiver equalization is set to ON (see "Receive Equalizer (linkRxEqualizer)" on page 224).

WAN Circuit Configuration—Modify

Clicking on the Modify Configuration link in the WAN Circuit Configuration Link window displays the WAN Circuit Configuration Link window (see figure 117) to configure the T1/E1 WAN port. From this window, you can change line interface settings, test settings, and change the T1/E1 pulse shapes.

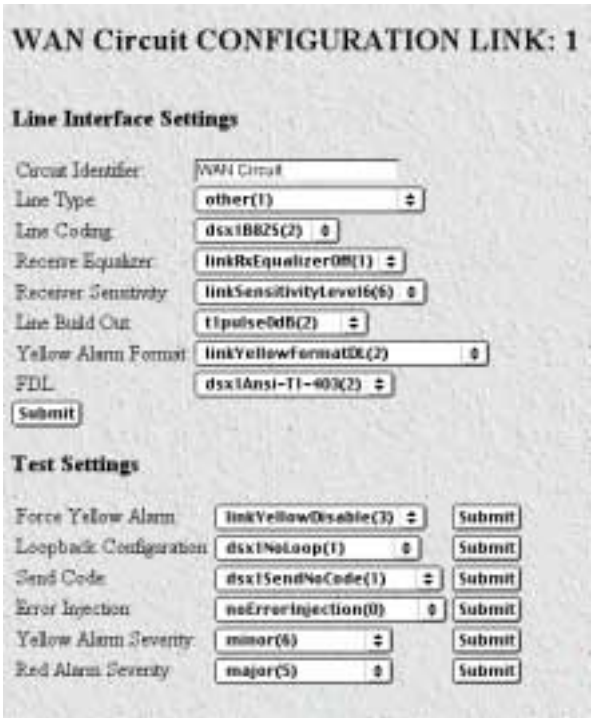


Figure 117. WAN Circuit Configuration—Modify window

Line Interface Settings

This portion of the WAN Circuit Configuration window contains information described in the following sections.

Circuit ID (dsx1CircuitIdentifier)

This variable contains the transmission vendor's circuit identifier, for the purpose of facilitating troubleshooting.

Line Type (dsx1LineType)

This variable indicates the type of DS1 Line implemented on this circuit. The type of circuit affects the number of bits per second that the circuit can reasonably carry, as well as the interpretation of the usage and error statistics. The values, in sequence, are:

- other(1)—Link is disabled
- dsx1ESF(2)—Extended Superframe DS1
- dsx1D4(3)—AT&T D4 format DS1
- dsx1E1(4)—Based on CCITT/ITU G.704 without CRC (Cyclical Redundancy Check)
- dsx1E1-CRC(5)—Based on CCITT/ITU G.704 with CRC (Cyclical Redundancy Check)
- dsx1E1-MF(6)—Based on CCIT/ITU G.704 without CRC (bit oriented signaling)
- dsx1E1-CRC-MF(7)—Based on CCIT/ITU G.704 with CRC (bit oriented signaling)
- dsx1E1-Transparent(8)—Based on CCIT/ITU G.703 without CRC (Cyclical Redundancy Check)

Line Coding (dsx1LineCoding)

This variable describes the type of Zero Code Suppression used on the link, which in turn affects a number of its characteristics.

- dsx1JBZS(1)—Jammed Bit Zero Suppression, in which the AT&T specification of at least one pulse every 8 bit periods is literally implemented by forcing a pulse in bit 8 of each channel. Thus, only seven bits per channel, or 1.344 Mbps, is available for data. This feature is not currently implemented.
- dsx1B8ZS(2)—The use of a specified pattern of normal bits and bipolar violations which are used to replace a sequence of eight zero bits. The most common coding for T1 circuits.
- dsx1HDB3(3)—This line coding is used with most E1 circuits today.
- dsx1ZBTSI(4)—May use *dsx1ZBTSI*, or Zero Byte Time Slot Interchange. This feature is not currently implemented.
- dsx1AMI(5)—Refers to a mode wherein no zero code suppression is present and the line encoding does not solve the problem directly. In this application, the higher layer must provide data which meets or exceeds the pulse density requirements, such as inverting HDLC data.
- other(6)—This feature is not currently supported.

Receive Equalizer (linkRxEqualizer)
This variable determines the equalization used on the received signal. Long haul signals should have the equalization set for more. Short haul signals require less equalization.

- linkRxEqualizerOff(1)
- linkRxEqualizerOn(2)

Receiver Sensitivity (linkSensitivityLevel)
This variable selects the minimum voltage at which the WAN ort will sense that the signal is available. The default setting is linkSensitivityLevel5.

Note This variable is only used if the receiver equalization is set to ON (see "Receive Equalizer (linkRxEqualizer)" on page 224).

- linkSensitivityLevel1(1)—Voltage threshold: 1.70V; maximum distance achievable: less than 1,000 feet (305 meters)
- linkSensitivityLevel2(2)—Voltage threshold: 0.84V; maximum distance achievable: less than 2,000 feet (610 meters)
- linkSensitivityLevel3(3)—Voltage threshold: 0.84V; maximum distance achievable: less than 3,000 feet (914 meters)
- linkSensitivityLevel4(4)—Voltage threshold: 0.45V; maximum distance achievable: less than 5,000 feet (1,524 meters)
- linkSensitivityLevel5(5)—Voltage threshold: 0.45V; maximum distance achievable: less than 5,000 feet (1,524 meters)
- linkSensitivityLevel6(6)—Voltage threshold: 0.2V; maximum distance achievable: less than 5,000 feet (1,524 meters)
- linkSensitivityLevel7(7)—Voltage threshold: 0.1V; maximum distance achievable: less than 5,000 feet (1,524 meters)

Line Build Out (linkLineBuildOut)
This variable defines the T1 or E1 pulse levels used by the T1/E1 ports:

- triState(0)—When the T1/E1 port is not in use, the user may want to place the port in tri-state mode. While in this setting, the input lines to the port are placed in high impedance protection mode.
- e1pulse(1)—Used when connecting the T1/E1 port to E1 lines.
- t1pulse0dB(2)—Strong T1 pulse amplitude.
- t1pulse-7dB(3)—Medium T1 pulse amplitude.
- t1pulse-15dB(4)—Weak T1 pulse amplitude.

Yellow Alarm Format (linkYellowFormat)
This variable identifies which standard will be used to transmit and identify the Yellow Alarm.

- link YellowFormatBit2(1)—Bit-2 equal zero in every channel

- YellowFormatDL(2)—FF00 pattern in the Data Link
- YellowFormatFrame12FS(3)—FS bit of frame 12

FDL (dsx1FDL)
This variable describes which implementation of FDL is being used, if any. FDL applies only to T1 circuits.

- other(1)—Indicates that a protocol other than one following is used.
- dsx1Ansi-T1-403(2)—Refers to the FDL exchange recommended by ANSI.
- dsx1Att-54016(3)—Refers to ESF FDL exchanges.
- dsx1Fdl-none(4)—Indicates that the device does not use the FDL.

If one of the E1 line types has been selected, this parameter is ignored.

Test Settings
This portion of the WAN Circuit Configuration Link window contains information described in the following sections.

Force Yellow Alarm (linkYellowForce)
This variable identifies which standard will be used to transmit and identify the Yellow Alarm.

- linkYellowAuto—Do *not* force the transmission of a yellow alarm. But, yellow alarm may be automatically transmitted.
- linkYellowOn—Force the transmission of a yellow alarm even if the received signal is in frame.
- linkYellowDisable—Do NOT transmit a yellow alarm even if the received signal is out of frame.

Loopback Configuration (dsx1LoopbackConfig)
This variable represents the loopback configuration of the DS1 interface. Agents supporting read/write access should return badValue in response to a requested loopback state that the interface does not support. The values mean:

- dsx1NoLoop(1)—Not in the loopback state. A device that is not capable of performing a loopback on the interface shall always return this as it's value.
- dsx1PayloadLoop(2)—The received signal at this interface is looped through the device. Typically the received signal is looped back for retransmission after it has passed through the device's framing function.
- dsx1LineLoop(3)—The received signal at this interface does not go through the device (minimum penetration) but is looped back out.
- dsx1OtherLoop(4)—Loopbacks that are not defined here.

Send Code (dsx1SendCode)
- This variable indicates what type of code is being sent across the DS1 interface by the device. The values mean:
- dsx1SendNoCode(1)—Sending looped or normal data
- dsx1SendLineCode(2)—Sending a request for a line loopback

- dsx1SendResetCode(4)—Sending a loopback termination request

Error Injection (linkInjectError)

Force an output error to see if the other end detects it

- noErrorInjection(0)
- injectCRCerrorBurst(1)
- injectLineErrorBurst(2)

Yellow Alarm Severity ()

This reference is identical to the reference on the Alarms window in the 3096RC Configuration Menu. The configuration may be changed here or in the Alarms window.

- critical(4)
- major(5)
- minor(6)
- informational(7)
- ignore(8)

Red Alarm Severity ()

This reference is identical to the reference on the Alarms page in the 3096RC Configuration Menu. The configuration may be changed here or in the Alarms page.

- critical(4)
- major(5)
- minor(6)
- informational(7)
- ignore(8)

WAN Circuit Configuration—Channel Assignment

For each T1/E1 link, the DS0s can provide two functions:

- Carrying TDM user data
- Carrying in-band management information

By factory default, the T-DAC allocates all DS0s to carry TDM user data. The WAN Circuit Channel Assignment window provides the means for you to allocate DS0s on a selected T1 or E1 WAN link to be used for in-band management of the T-DAC.

You can use the WAN Circuit Channel Assignment window to change selected DS0 channels to carry in-band management information over Frame Relay or PPP links. You can use the buttons at the top of the window to modify all 30 timeslots at once. Or you can use the 30 drop-down menus to modify selected timeslots individually.

To display the WAN Circuit Channel Assignment window:

- Determine which T1/E1 WAN circuit you wish to use for in-band management
- Display the WAN Circuit Configuration Link page for your selected T1/E1 link
- Click the Channel Assignment hyperlink

Note After modifying the channel assignments, click **Submit Query** to make activate the changes.

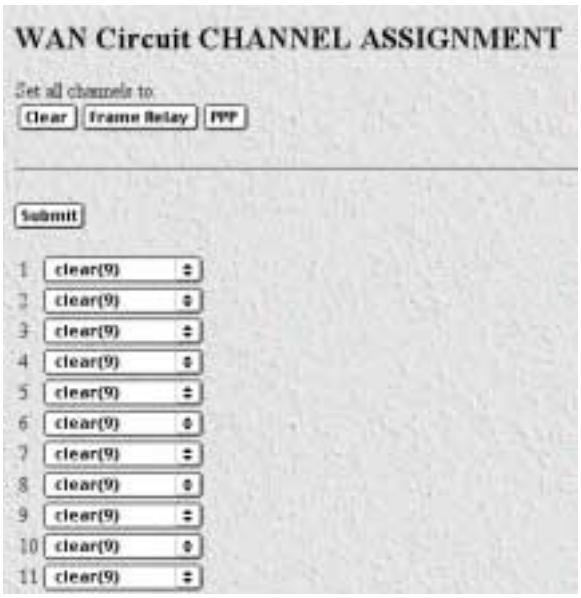


Figure 118. WAN Circuit CHANNEL ASSIGNMENT window

Near End Line Statistics—Current

Click on Near End Line Statistics—Current to display line statistics for the current 15-minute interval (see figure 119).

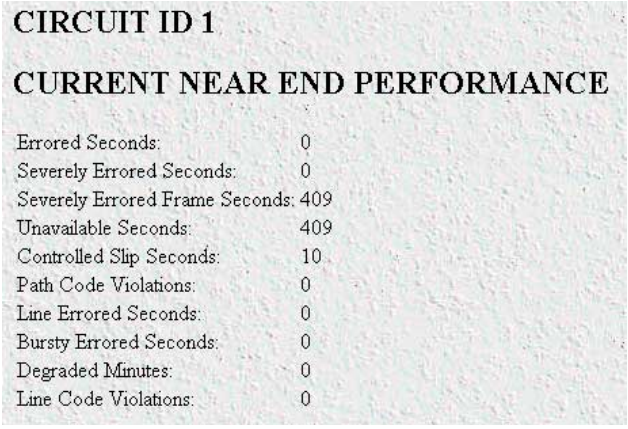


Figure 119. Current Near End Performance window

Errored Seconds (dsx1CurrentESs)

The number of errored seconds, encountered by a DS1 interface in the current 15-minute interval.

Severely Errored Seconds (dsx1CurrentSESs)

The number of severely errored seconds encountered by a DS1 interface in the current 15-minute interval.

Severely Errored Frame Seconds (dsx1CurrentSEFSs)

The number of severely errored framing seconds encountered by a DS1 interface in the current 15-minute interval.

Unavailable Seconds (dsx1CurrentUASs)

The number of unavailable seconds encountered by a DS1 interface in the current 15-minute interval.

Controlled Slip Seconds (dsx1CurrentCSSs)

The number of Controlled Slip Seconds encountered by a DS1 interface in the current 15-minute interval.

Path Code Violations (dsx1CurrentPCVs)

The number of path coding violations encountered by a DS1 interface in the current 15-minute interval.

Line Errored Seconds (dsx1CurrentLESs)

The number of line errored seconds encountered by a DS1 interface in the current 15-minute interval.

Bursty ErroredSeconds (dsx1CurrentBESs)

The number of bursty errored seconds (BESs) encountered by a DS1 interface in the current 15-minute interval.

Degraded Minutes (dsx1CurrentDMs)
The number of degraded minutes (DMs) encountered by a DS1 interface in the current 15-minute interval.

Line Code Violations (dsx1CurrentLCVs)
The number of line code violations (LCVs) encountered by a DS1 interface in the current 15-minute interval.

Near End Line Statistics—History

Click on Near End Line Statistics—History to display line statistics for prior completed 15-minute intervals within the last 24 hours (see figure 120). This does not include the current 15-minute interval.

CIRCUIT ID 1

DACS

HISTORY OF NEAR END PERFORMANCE

Interval	Errored Seconds	Severely Errored Seconds	Severely Errored Frame Seconds	Unavailable Seconds	Controlled Slip Seconds	Path Code Violations	Line Errored Seconds	Bursty Errored Seconds	Degraded Minutes	Line Code Violations
1	0	0	900	900	22	0	0	0	0	0
2	0	0	900	900	22	0	0	0	0	0
3	0	0	900	900	22	0	0	0	0	0
4	0	0	900	900	23	0	0	0	0	0
5	0	0	900	900	22	0	0	0	0	0
6	0	0	900	900	22	0	0	0	0	0
7	0	0	900	900	22	0	0	0	0	0
8	0	0	900	900	22	0	0	0	0	0
9	0	0	900	900	22	0	0	0	0	0
10	0	0	900	900	22	0	0	0	0	0
11	0	0	900	900	22	0	0	0	0	0
12	0	0	900	900	22	0	0	0	0	0
13	0	0	900	900	22	0	0	0	0	0

Figure 120. History of Near End Performance window

Interval (dsx1IntervalNumber)
A number between 1 and 96, where 1 is the most recently completed 15-minute interval and 96 is the least recently completed 15-minutes interval. When all 96 intervals are visible, then the 3096RC has been operating (powered-on) for at least 24 hours. If less than 96 intervals are visible, then it has been less than 24 hours since the 3096RC was powered up.

Errored Seconds (dsx1intervaless)
The number of errored Seconds encountered by a DS1 interface in one of the previous 96, individual 15-minute, intervals.

Severely Errored Seconds (dsx1IntervalSESs)
The number of severely errored seconds encountered by a DS1 interface in one of the previous 96, individual 15-minute, intervals.

Severely Errored Frame Seconds (dsx1IntervalSEFSs)
The number of severely errored framing seconds encountered by a DS1 interface in one of the previous 96, individual 15-minute, intervals.

Unavailable Seconds (dsx1IntervalUASs)
The number of unavailable seconds encountered by a DS1 interface in one of the previous 96, individual 15-minute, intervals.

Controlled Slip Seconds (dsx1IntervalCSSs)
The number of controlled slip seconds encountered by a DS1 interface in one of the previous 96, individual 15-minute, intervals.

Path Code Violations (dsx1IntervalPCVs)
The number of path coding violations encountered by a DS1 interface in one of the previous 96, individual 15-minute, intervals.

Line Errored Seconds (dsx1IntervalLESs)
The number of line errored seconds encountered by a DS1 interface in one of the previous 96, individual 15-minute, intervals.

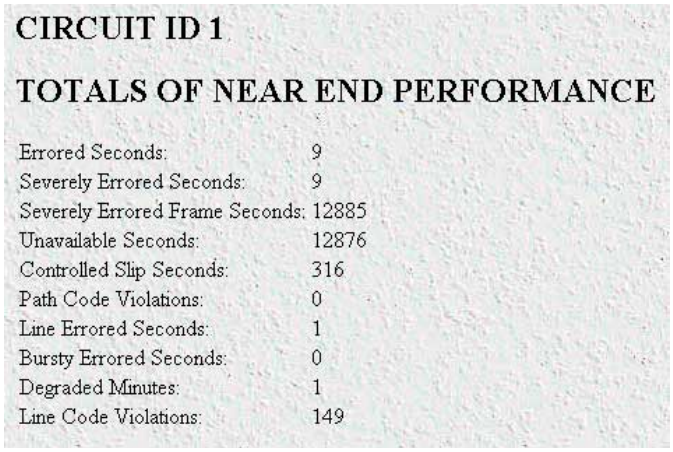
Bursty ErroredSeconds (dsx1IntervalBESs)
The number of bursty errored seconds (BESs) encountered by a DS1 interface in one of the previous 96, individual 15-minute, intervals.

Degraded Minutes (dsx1IntervalDMs)
The number of degraded minutes (DMs) encountered by a DS1 interface in one of the previous 96, individual 15-minute, intervals.

Line Code Violations (dsx1IntervalLCVs)
The number of line code violations (LCVs) encountered by a DS1 interface in the current 15-minute interval.

Near End Line Statistics—Totals

Click on Near End Line Statistics—Totals to display the total statistics of errors that occurred during the previous 24-hour period, the previous 96 15-minute intervals (see figure 121).


CIRCUIT ID 1

TOTALS OF NEAR END PERFORMANCE

Errored Seconds:	9
Severely Errored Seconds:	9
Severely Errored Frame Seconds:	12885
Unavailable Seconds:	12876
Controlled Slip Seconds:	316
Path Code Violations:	0
Line Errored Seconds:	1
Bursty Errored Seconds:	0
Degraded Minutes:	1
Line Code Violations:	149

Figure 121. Totals of Near End Performance window

Errored Seconds (dsx1TotalESs)
The number of errored seconds encountered by a DS1 interface in the previous 24-hour interval.

Severely Errored Seconds (dsx1TotalSESs)
The number of severely errored seconds encountered by a DS1 interface in the previous 24-hour interval.

Severely Errored Frame Seconds (dsx1TotalSEFSs)
The number of severely errored framing seconds encountered by a DS1 interface in the previous 24-hour interval.

Unavailable Seconds (dsx1TotalUASs)
The number of unavailable seconds encountered by a DS1 interface in the previous 24-hour interval.

Controlled Slip Seconds (dsx1TotalCSSs)
The number of controlled slip seconds encountered by a DS1 interface in the previous 24-hour interval.

Path Code Violations (dsx1TotalPCVs)
The number of path coding violations encountered by a DS1 interface in the previous 24-hour interval.

Line Errored Seconds (dsx1TotalLESs)
The number of line errored seconds encountered by a DS1 interface in the previous 24-hour interval.

Bursty ErroredSeconds (dsx1TotalBESs)
The number of bursty errored seconds (BESs) encountered by a DS1 interface in the previous 24-hour interval.

Degraded Minutes (dsx1TotalDMs)
The number of degraded minutes (DMs) encountered by a DS1 interface in the previous 24-hour interval.

Line Code Violations (dsx1TotalLCVs)
The number of line code violations (LCVs) encountered by a DS1 interface in the previous 24-hour interval.

Far End Line Statistics—Current

Click on Near End Line Statistics—Current to display far-end statistics for the current 15-minute interval (see figure 122).

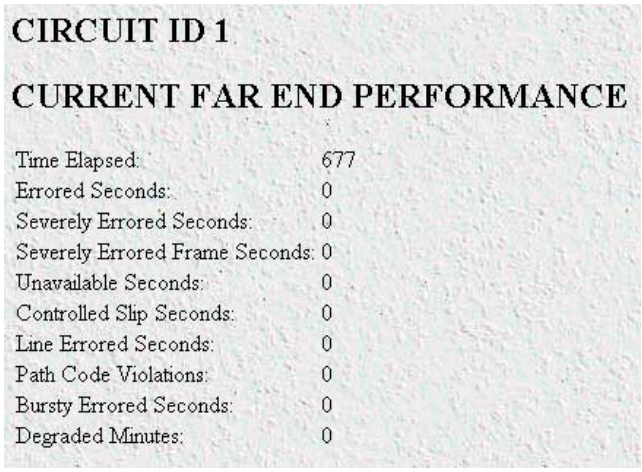


Figure 122. Current Far End Performance window

Time Elapsed (dsx1FarEndTimeElapsed)
The number of seconds that have elapsed since the beginning of the far-end current error-measurement period.

Errored Seconds (dsx1FarEndCurrentESs)
The number of far-end errored seconds encountered by a DS1 interface in the current 15-minute interval.

Severely Errored Seconds (dsx1FarEnd CurrentSESs)
The number of far-end severely errored seconds encountered by a DS1 interface in the current 15-minute interval.

Severely Errored Frame Seconds (dsx1FarEndCurrentSEFSs)
The number of far-end severely errored framing seconds encountered by a DS1 interface in the current 15-minute interval.

Unavailable Seconds (dsx1FarEndCurrentUASs)
The number of far-end unavailable seconds encountered by a DS1 interface in the current 15-minute interval.

Controlled Slip Seconds (dsx1FarEndCurrentCSSs)
The number of far-end controlled slip seconds encountered by a DS1 interface in the current 15-minute interval.

Line Errored Seconds (dsx1FarEndCurrentLESs)
The number of far-end line errored seconds encountered by a DS1 interface in the current 15-minute interval

Path Code Violations (dsx1FarEndCurrentPCVs)
The number of far-end path coding violations reported via the far-end block error count encountered by a DS1 interface in the current 15-minute interval.

Bursty Errored Seconds (dsx1FarEndCurrentBESs)
The number of far-end bursty errored seconds (BESs) encountered by a DS1 interface in the current 15-minute interval.

Degraded Minutes (dsx1FarEndCurrentDMs)
The number of far-end degraded minutes (DMs) encountered by a DS1 interface in the current 15-minute interval.

Far End Line Statistics—History
Click on Far End Line Statistics—History to display far-end statistics for previously completed 15-minute intervals (see figure 123).

CIRCUIT ID 1

DACS

HISTORY OF FAR END PERFORMANCE

Interval	Errored Seconds	Severely Errored Seconds	Severely Errored Frame Seconds	Unavailable Seconds	Controlled Slip Seconds	Line Errored Seconds	Path Code Violations	Bursty Errored Seconds	Degraded Minutes
1	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0

Figure 123. History of Far End Performance window

Interval (dsx1FarEndIntervalNumber)
A number between 1 and 96, where 1 is the most recently completed 15-minute interval and 96 is the least recently completed 15-minutes interval (assuming that all 96 intervals are valid).

Errored Seconds (dsx1FarEndIntervalESs)
The number of far-end errored seconds encountered by a DS1 interface in one of the previous 96, individual 15-minute, intervals.

Severely Errored Seconds (dsx1FarEndIntervalSESs)
The number of far-end severely errored seconds encountered by a DS1 interface in one of the previous 96, individual 15-minute, intervals.

Severely Errored Frame Seconds (dsx1FarEndIntervalSEFSs)
The number of far-end severely errored framing seconds encountered by a DS1 interface in one of the previous 96, individual 15-minute, intervals.

Unavailable Seconds (dsx1FarEndIntervalUASs)
The number of far-end unavailable seconds encountered by a DS1 interface in one of the previous 96, individual 15-minute, intervals.

Controlled Slip Seconds (dsx1FarEndIntervalCSSs)
The number of far-end controlled slip seconds encountered by a DS1 interface in one of the previous 96, individual 15-minute, intervals.

Line Errored Seconds (dsx1FarEndIntervalLESs)
The number of far-end line errored seconds encountered by a DS1 interface in one of the previous 96, individual 15-minute, intervals.

Path Code Violations (dsx1FarEndIntervalPCVs)
The number of far-end path coding violations encountered by a DS1 interface in one of the previous 96, individual 15-minute, intervals.

Bursty Errored Seconds (dsx1FarEndIntervalBESs)
The number of far-end bursty errored seconds (BESs) encountered by a DS1 interface in one of the previous 96, individual 15-minute, intervals.

Degraded Minutes (dsx1FarEndIntervalDMs)
The number of far-end degraded minutes (DMs) encountered by a DS1 interface in one of the previous 96, individual 15-minute, intervals.

Far End Line Statistics—Totals

Click on Far End Line Statistics—Totals to display the total statistics of errors that occurred during the previous 24-hour period (see figure 124). This is the sum of the current 15-minute interval and all time prior intervals within the last 24 hours.

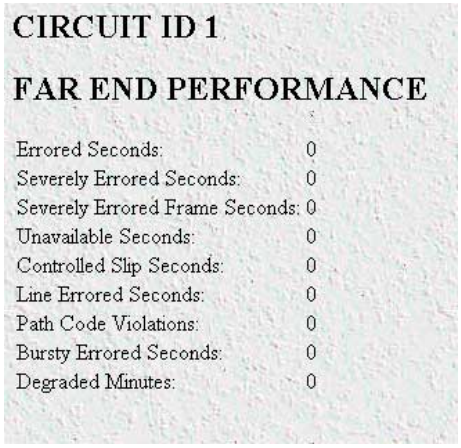


Figure 124. Far End Performance window

Errored Seconds (dsx1FarEndTotalESs)

The number of far-end errored seconds encountered by a DS1 interface in the previous 24-hour interval.

Severly Errored Seconds (dsx1FarEndTotalSESs)

The number of far-end severely errored seconds encountered by a DS1 interface in the previous 24-hour interval.

Severely Errored Frame Seconds (dsx1FarEndTotalSEFSs)

The number of far-end severely errored framing seconds encountered by a DS1 interface in the previous 24-hour interval.

Unavailable Seconds (dsx1FarEndTotalUASs)

The number of far-end unavailable seconds encountered by a DS1 interface in the previous 24-hour in-24-hour interval.

Controlled Slip Seconds (dsx1FarEndTotalCSSs)

The number of far-end controlled slip seconds encountered by a DS1 interface in the previous 24-hour interval.

Line Errored Seconds (dsx1FarEndTotalLESs)

The number of far-end line errored seconds encountered by a DS1 interface in the previous 24-hour interval.

Path Code Violations (dsx1FarEndTotalPCVs)

The number of far-end path coding violations reported via the far-end block error count encountered by a DS1 interface in the previous 24-hour interval.

Bursty Errored Seconds (dsx1FarEndTotalBESs)

The number of far-end bursty errored seconds (BESs) encountered by a DS1 interface in the previous 24-hour interval.

Degraded Minutes (dsx1FarEndTotalDMs)

The number of far-end degraded minutes (DMs) encountered by a DS1 interface in the previous 24-hour interval.

Chapter 23 About

Chapter contents

Introduction

The About link displays Patton Electronics Company contact information (see "Patton Electronics Company contact information"). Click on About under the T-DAC's Configuration Menu to display the About main window (see figure 125).

Figure 125. About window

Patton Electronics Company contact information

Patton Electronics Company
7622 Rickenbacker Drive
Gaithersburg, Maryland 20879
U.S.A.

Phone: **+1 (301) 975-1000**

Fax: **+1 (301) 869-9293**

E-mail: **sales@patton.com**
support@patton.com

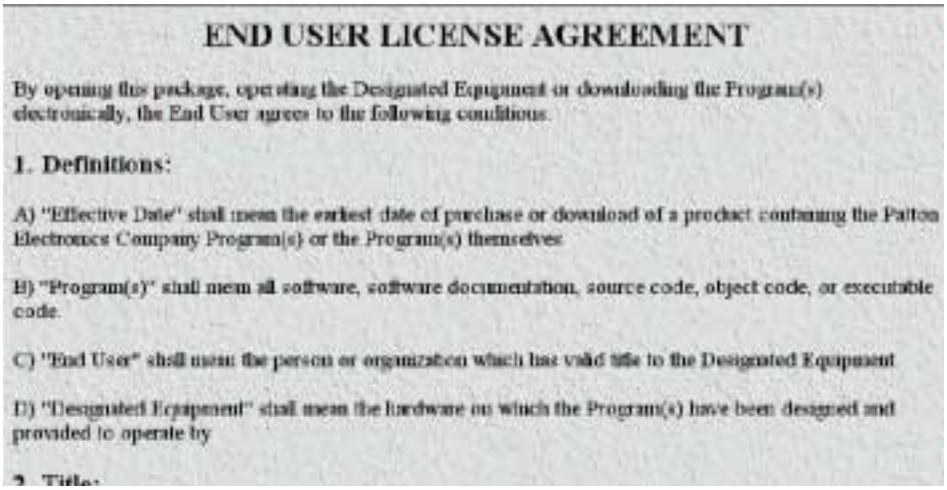
WWW: **www.patton.com**

Chapter 24 License

Chapter contents

Introduction

The License link presents the End User License Agreement for the T-DAC software. Click on License under the Configuration Menu to display the License main window (see figure 126).


END USER LICENSE AGREEMENT

By opening this package, operating the Designated Equipment or downloading the Program(s) electronically, the End User agrees to the following conditions:

1. Definitions:

A) "Effective Date" shall mean the earliest date of purchase or download of a product containing the Patton Electronics Company Program(s) or the Program(s) themselves

B) "Program(s)" shall mean all software, software documentation, source code, object code, or executable code.

C) "End User" shall mean the person or organization which has valid title to the Designated Equipment

D) "Designated Equipment" shall mean the hardware on which the Program(s) have been designed and provided to operate by

2. Title:

Figure 126. License window

By opening the T-DAC, operating the Designated Equipment or downloading the Program(s) electronically, the End User agrees to the conditions in the "End User License Agreement" below.

End User License Agreement

By opening this package, operating the Designated Equipment or downloading the Program(s) electronically, the End User agrees to the following conditions:

1. Definitions:

A) "Effective Date" shall mean the earliest date of purchase or download of a product containing the Patton Electronics Company Program(s) or the Program(s) themselves.

B) "Program(s)" shall mean all software, software documentation, source code, object code, or executable code.

C) "End User" shall mean the person or organization which has valid title to the Designated Equipment.

D) "Designated Equipment" shall mean the hardware on which the Program(s) have been designed and provided to operate by

2. Title:

Title to the Program(s), all copies of the Program(s), all patent rights, copyrights, trade secrets and proprietary information in the Program(s), worldwide, remains with Patton Electronics Company or its licensors.

3. Term:

The term of this Agreement is from the Effective Date until title of the Designated Equipment is transferred by End User or unless the license is terminated earlier as defined in "6. Termination:" below.

4. Grant of License:

A) During the term of this Agreement, Patton Electronics Company grants a personal, non-transferable, non-assignable and non-exclusive license to the End User to use the Program(s) only with the Designated Equipment at a site owned or leased by the End User.

B) The End User may copy licensed Program(s) as necessary for backup purposes only for use with the Designated Equipment that was first purchased or used or its temporary or permanent replacement.

C) The End User is prohibited from disassembling; decompiling, reverse-engineering or otherwise attempting to discover or disclose the Program(s), source code, methods or concepts embodied in the Program(s) or having the same done by another party.

D) Should End User transfer title of the Designated Equipment to a third party after entering into this license agreement, End User is obligated to inform the third party in writing that a separate End User License Agreement from Patton Electronics Company is required to operate the Designated Equipment.

5. Warranty:

The Program(s) are provided "as is" without warranty of any kind. Patton Electronics Company and its licensors disclaim all warranties, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose or non-infringement. In no event shall Patton Electronics Company or its licensors be liable for any damages whatsoever (including, without limitation, damages for loss of business profits, business interruption, loss of business information, or other pecuniary loss) arising out of the use of or inability to use the Program(s), even if Patton Electronics Company has been advised of the possibility of such damages. Because some states do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you.

If the Program(s) are acquired by or on behalf of a unit or agency of the United States Government, the Government agrees that such Program(s) are "commercial computer software" or "computer software documentation" and that, absent a written agreement to the contrary, the Government's rights with respect to such Program(s) are limited by the terms of this Agreement, pursuant to Federal Acquisition Regulations 12.212(a) and/or DEARS 227.7202-1(a) and/or sub-paragraphs (a) through (d) of the "Commercial Computer Software—Restricted Rights" clause at 48 C.F.R. 52.227-19 of the Federal Acquisition Regulations as applicable.

6. Termination:

A) The End User may terminate this agreement by returning the Designated Equipment and destroying all copies of the licensed Program(s).

B) Patton Electronics Company may terminate this Agreement should End User violate any of the provisions of "4. Grant of License:" above.

C) Upon termination for A or B above or the end of the Term, End User is required to destroy all copies of the licensed Program(s)