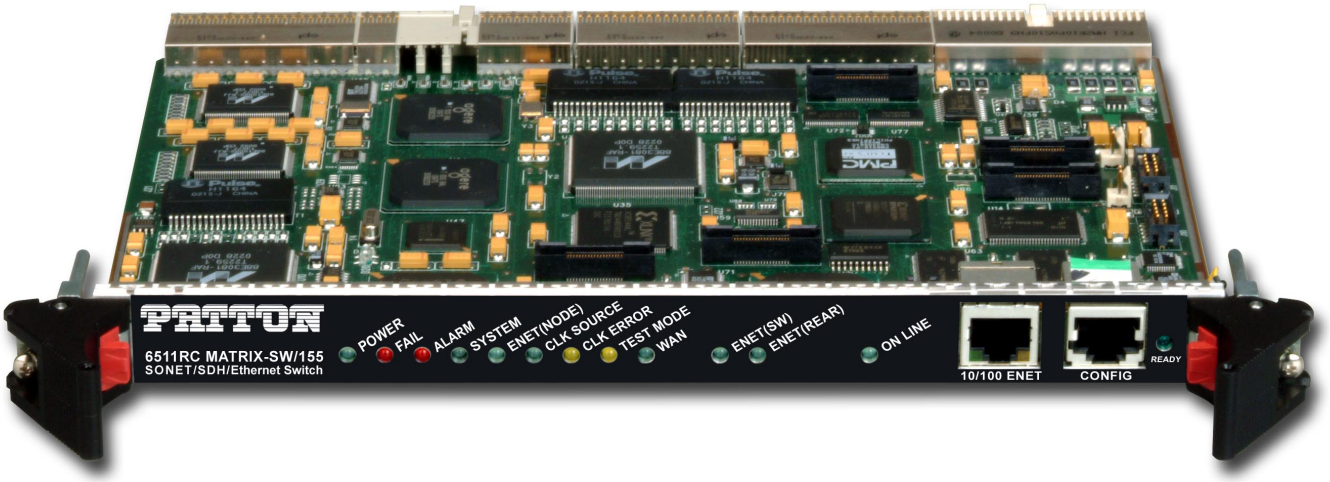
PATTON Electronics Co.

Model 6511RC
Matrix Switch

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: **11501U3-001 Rev. B**
Part Number: **07MD6511RC-ARG**
Revised: **April 6, 2005**

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

Notices

The information contained in this document is not designed or intended for use as critical components in human life-support systems, equipment used in hazardous environments, or nuclear control systems. Patton Electronics Company disclaims any express or implied warranty of fitness for such uses.

The information in this document is subject to change without notice. Patton Electronics assumes no liability for errors that may appear in this document.

Any software described in this document is furnished under license and may be used or copied only in accordance with the terms of such license.

Summary Table of Contents

Table of Contents

List of Figures

List of Tables

About this guide

This guide describes configuring a Patton Electronics Matrix Switch (6511RC). 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 "Conventions used in this document" on page 4)

Audience

This guide is intended for the following users:

- System administrators
- Operators

Structure

This guide contains the following chapters:

- Chapter 1 (on page 7) on describes using the Administration Page window
- Chapter 2 (on page 11) describes using the Home window
- Chapter 3 (on page 17) describes using the Import/Export window
- Chapter 4 (on page 21) describes using the Alarms window
- Chapter 5 (on page 29) describes using the DS0 Mapping window
- Chapter 6 (on page 41) describes using the Clocking window
- Chapter 7 (on page 47) describes using the Ethernet window
- Chapter 8 (on page 53) describes using the IP window
- Chapter 9 (on page 71) describes using the Filter IP window
- Chapter 10 (on page 79) describes using the RIP Version 2 window
- Chapter 11 (on page 87) describes using the SNMP window
- Chapter 12 (on page 93) describes using the System window
- Chapter 13 (on page 111) describes using the System Log window
- Chapter 14 (on page 123) describes using the E1 Link window

- Chapter 15 (on page 133) describes using the SDH window
- Chapter 16 (on page 149) describes the contents of the About window
- Chapter 17 (on page 151) describes the contents of the License window

Precautions

The following are used in this guide to help you become aware of potential problems:

Note A note presents additional information or interesting sidelights.

The alert symbol and IMPORTANT heading calls attention to important information.

Conventions used in this document

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

General conventions

The procedures described in this guide use the text conventions listed in table 1.

Table 1. Text conventions

Convention	Meaning
Garamond blue type	Indicates a cross-reference hyperlink that points to a figure, graphic, table, or section heading. Clicking on the hyperlink jumps you to the reference. When you finish reviewing the reference, click on the **Go to Previous View** button in the Adobe® Acrobat® Reader toolbar to return to your starting point.
Italicized Garamond type	Indicates the names of items.
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

Table 2 lists conventions this guide uses to describe 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 6511RC Matrix Switch by using its internal HTTP/HTML Web Management windows. However, to access the HTTP/HTML windows, you must first define:

- The 6511RC system's LAN IP method to obtain address
- LAN IP address
- LAN IP subnet mask for the 6511RC

If you have not defined the above parameters, refer to the procedures in the Getting Started Guide that came with your 6511RC

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 6511RC will ask for your user name and password as shown in figure 1.

Figure 1. 6511RC login window

Your 6511RC will accept the following default administrative username: **superuser**

Your 6511RC will accept the following default administrative passwords:

- **superuser**—this password carries full permission to change and view any parameters in the 6511RC
- **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.

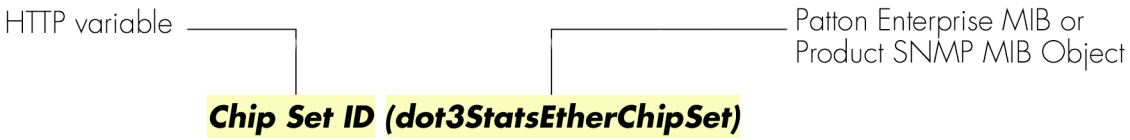


Figure 2. HTTP/HTML and SNMP object format

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 6511RC is power-cycled.

Chapter 2 Home

Chapter contents

Introduction

The 6511RC Web Management *HOME* window is the first management window that you see after logging into the 6511RC (see figure 3).

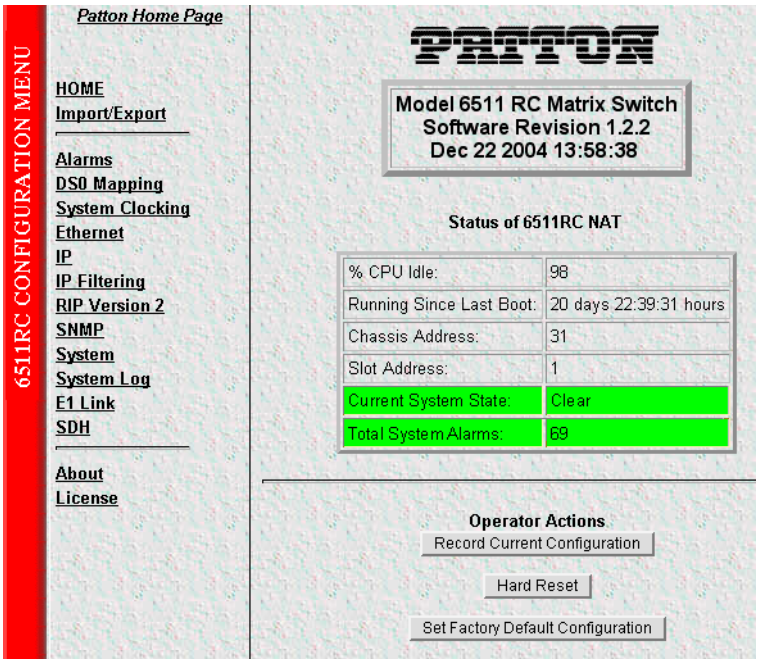


Figure 3. HOME window

The *HOME* window consists of sections that enable you to:

- View general product information about the 6511RC, such as the current software version (see section "Product information box" on page 14)
- 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 6511RC (front blade/rear blade) alarm status, which displays the highest-level alarm currently detected in the 6511RC—listed as *Major*, *Minor*, or *Clear* (for none)
  - Total alarms active in the 6511RC

  See section "Operating status variables" on page 14 for more information.
- Initiate the following *immediate actions*:
  - Save any changes you have made to the 6511RC's system configuration

– Perform a hard reset (*cold restart*) of the system without power-cycling the 6511RC.

– Set factory default configuation. Reset all the 6511RC's configurable parameters to their factory-default values.

See section "Operator Actions" on page 15 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 6511RC 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.

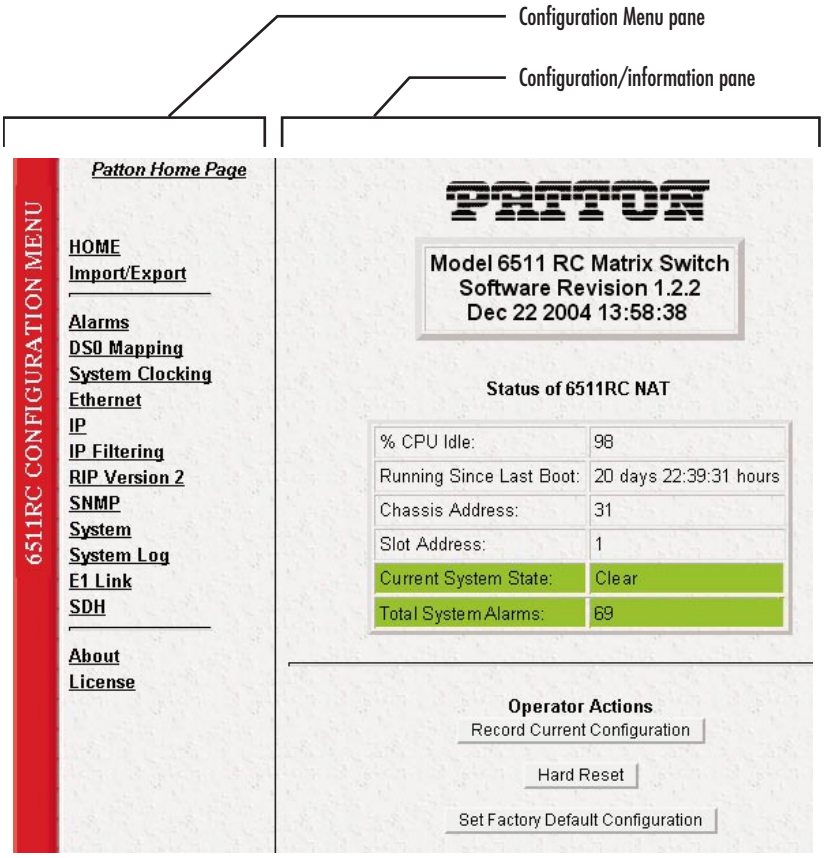


Figure 4. HOME window panes

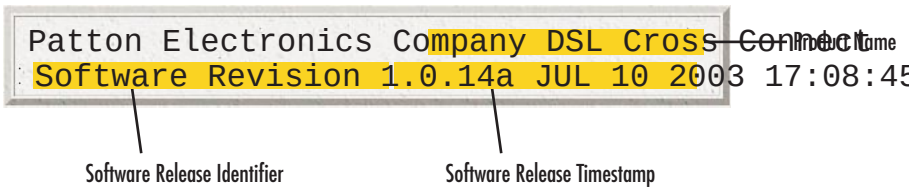


Figure 5. Product information section of HOME window

Product information box

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

- Product name: *Matrix Switch*
- Software release identifier: The current software version running on the 6511RC. 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 6511RC are shown in figure 6 and described in the following sections.

% CPU Idle:	87
Running Since Last Boot:	3 days 06:45:10 hours
Chassis Address:	31
Slot Address:	2
Current System State:	Clear
Total System Alarms:	69

Figure 6. Status menu

Shelf Address (cPCIShelfAddr)

Indicates the address of the ForeFront chassis in which the 6511RC resides. The address is set via DIP switches located on the 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 6511RC. 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 6511RC.

Running Since Last Boot (sysUpTime)
The time (in hundredths of a second) since the 6511RC was last power-cycled.

Current Box State (alarmBoxState)
The highest level alarm currently active in the 6511RC 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.

Operator Actions
In superuser mode you can initiate several operator actions (see figure 7) which will cause the 6511RC to operate according to the descriptions in the following sections.

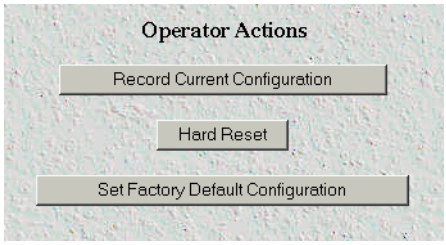


Figure 7. Operator Actions buttons

Record Current Configuration (storeConfig(1))
Clicking the button labeled **Record Current Configuration** causes the 6511RC 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** and the current configuration of the 6511RC will be saved when the 6511RC is powered down.

Configuration changes in the 6511RC are made by clicking a button labeled **Submit Query** on any of the subsystem window. When you click **Submit Query**, the 6511RC 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.

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))

The **Hard Reset** button causes the 6511RC to perform a cold restart. When you click **Hard Reset**, the 6511RC requests confirmation before executing the command, after which, the 6511RC will disconnect all current sessions, re-initialize the interfaces, and re-load configuration parameters from Flash memory.

Set Factory Default Configuration (forceDefaultConfig(3))

The **Set Factory Default Configuration** 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 6511RC until it has been re-booted, for example by doing a **Hard Reset**.

Note **Set Factory Default Configuration** will delete the 6511RC's Ethernet IP address, reset the password to the default administrative passwords (see section "Logging into the HTTP/HTML Web Management windows" on page 8), 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 6511RC's Ethernet IP address and netmask using the 6511RC'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 6511RC's configuration parameters. By exporting the configurations, the saved files can quickly be loaded, or *imported*, into a replacement 6511RC—greatly speeding up the installation process should a 6511RC 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).

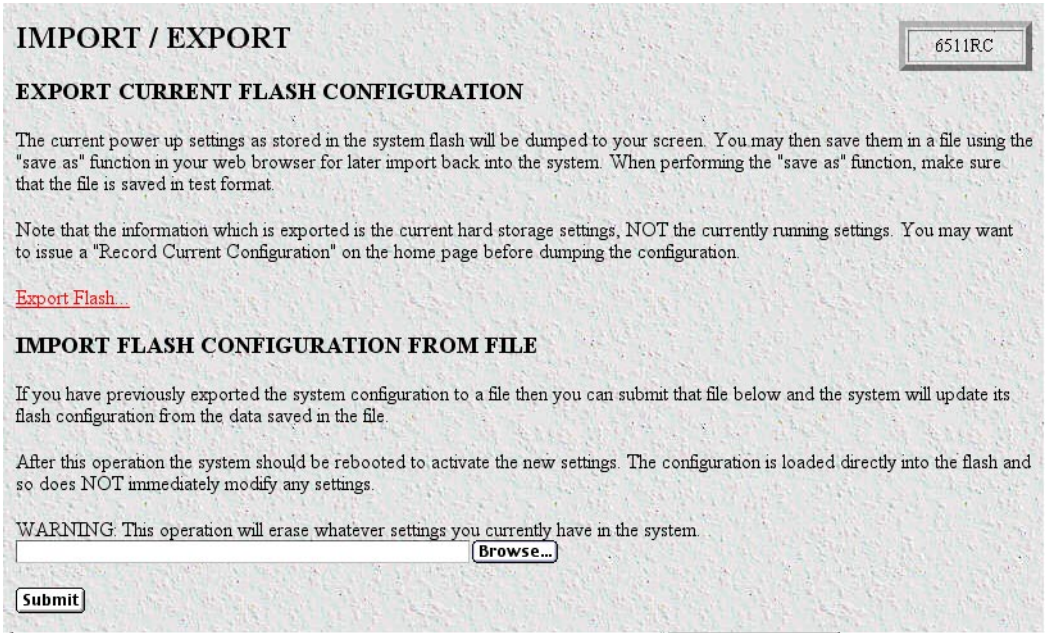


Figure 8. IMPORT/EXPORT main window

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 *Operator Actions*.

To export the Flash configuration, click on the *Export Flash* link on the *IMPORT/EXPORT* main window. The 6511RC will display text configuration information resembling that shown in figure 9.

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

Flash configuration data for: 6511RC

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.2 = "0x07:C8:A8:C0:72:61:6D:2E:6D:6B:69:00:78:5C:72:61:6D:2E:6D:6B:69:00:00:00
:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:22:79"


fconfigData.13 = "0x01:00:00:00:22:0C:0A:0A:00:00:FF:FF:00:00:00:00:00:00:00:00:00:00:00:00
:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:5D:DB"
```

Figure 9. Typical 6511RC 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**.

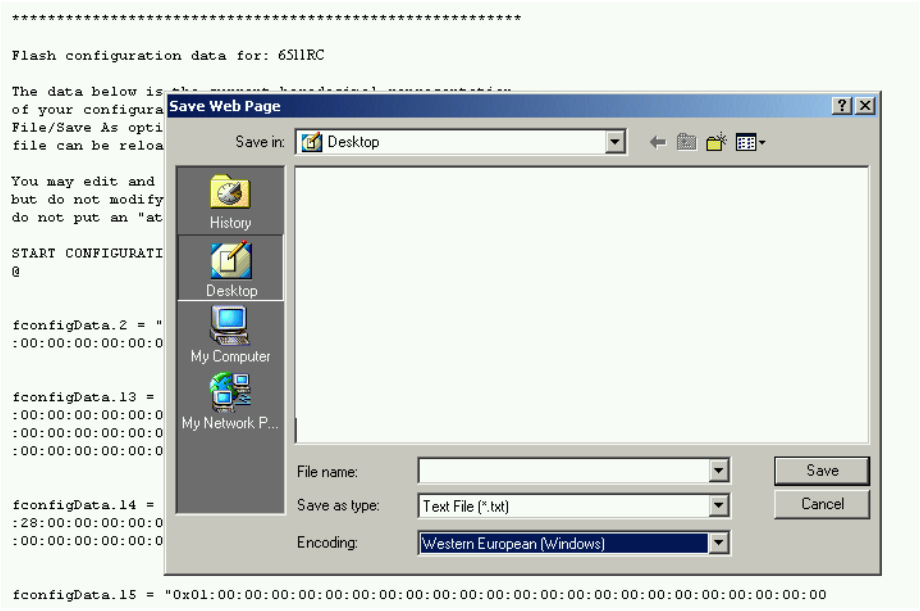


Figure 10. Saving the 6511RC flash memory configuration data as a text file

Import Flash Configuration From File

To import a configuration file into the 6511RC, 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 18).

Upon successfully importing the file, the 6511RC 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 *Operator Actions*.

Chapter 4 Alarms

Chapter contents

Introduction

The 6511RC provides alarm facilities that monitor the operating status of the 6511RC's SDH port, path, H.110 WAN ports, clock synchronization and fallback, and ambient temperature. The 6511RC provides three alarm signaling methods to indicate that an alarm condition has been detected:

- Visual indication via the 6511RC front panel ALARM and rear blade ALARM status LED indicators
- Operator console indication via the 6511RC management windows
- External alarms management host indication delivered via SNMP traps or Syslog messages that the 6511RC can send to an external alarms management host

By default, all 6511RC alarms are set to display as major (orange-colored) severity 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 11) and related windows enable you to manage the 6511RC's alarm system. Click on the *Alarms* hyperlink in the 6511RC's *Configuration Menu* to display the *Alarm System Overview* window.

Note From the *Alarm System Overview* window, the system administrator can force the 6511RC to generate alarms for testing purposes as well as clear selected alarms.

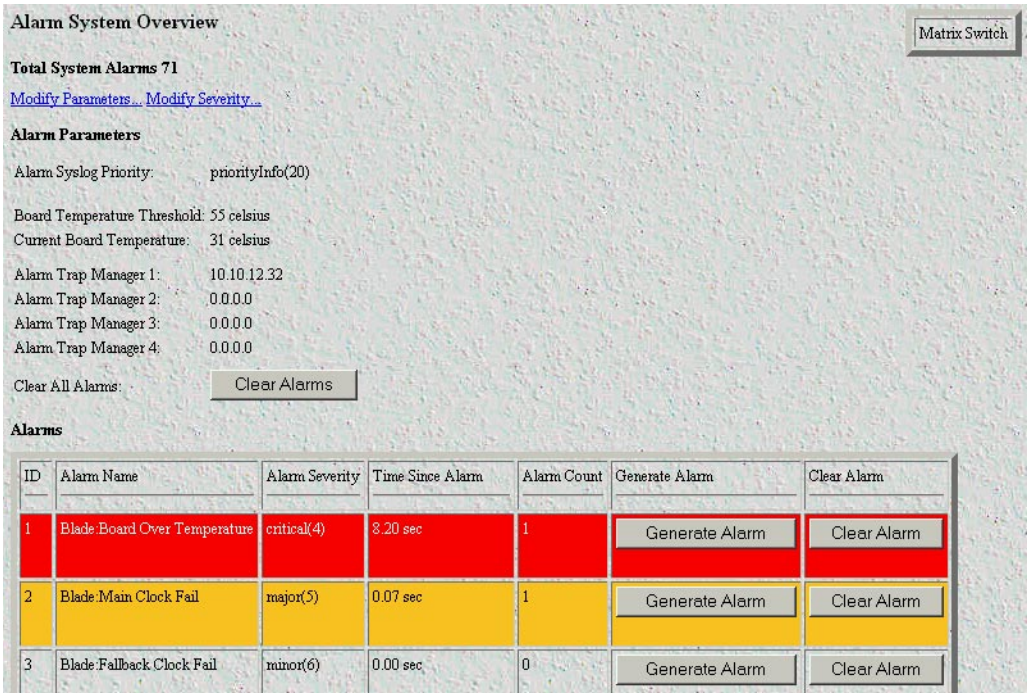


Figure 11. Alarm System Overview window

The 6511RC 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 6511RC'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 26), 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.

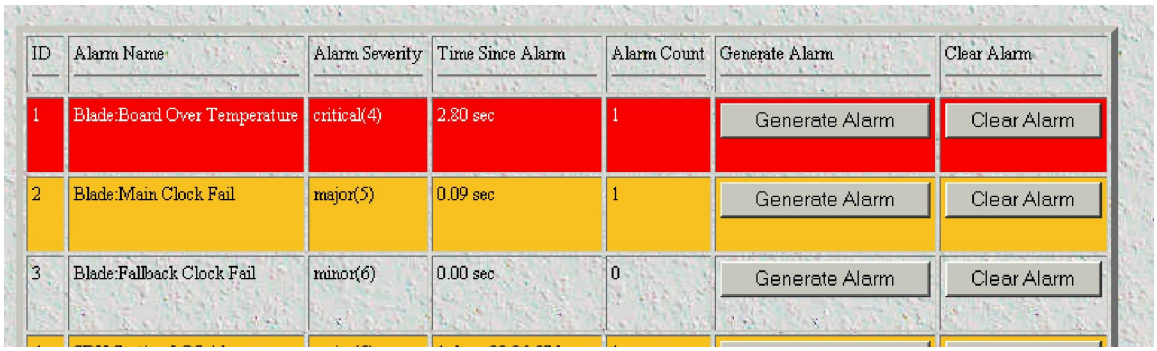


Figure 12. Sample alarm indications

- Management web page indication—The *Alarms* section (see figure 12) of the *Alarm System Overview* window (see figure 11 on page 22) 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 6 on page 14) and as a flashing red star (see figure 49 on page 98) on the *System Status* window (see figure 48 on page 98).
  - **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 6 on page 14) and as an orange exclamation mark (see figure 49 on page 98) on the *System Status* window (see figure 48 on page 98).
  - **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 6 on page 14) and as a yellow triangle (see figure 49 on page 98) on the *System Status* window (see figure 48 on page 98).

- **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.

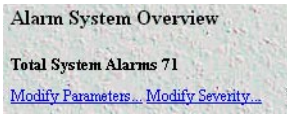


Figure 13. Modify Parameters and Modify Severity hyperlinks

- External host indication—For external notification, the 6511RC 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 6511RC to send SNMP traps or Syslog messages in response to alarm conditions, click on the *Modify Parameters* hyperlink (see figure 13) to open the *Alarm System Configurations—Alarm Response Outputs* window (refer to section "Alarm System Configurations window" on page 25).

In addition to viewing current alarm status, you can force the 6511RC to generate an alarm as a test by clicking on the **Generate Alarm** button (see figure 12 on page 23) for the desired alarm. Click on the **Clear Alarm** button (see figure 12 on page 23) to clear the alarm when the test is concluded.

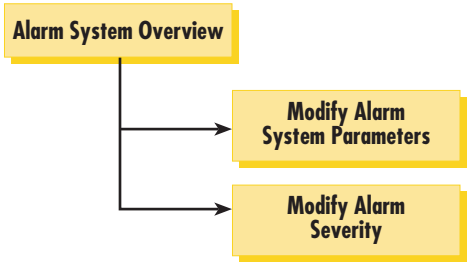


Figure 14. Alarms management diagram

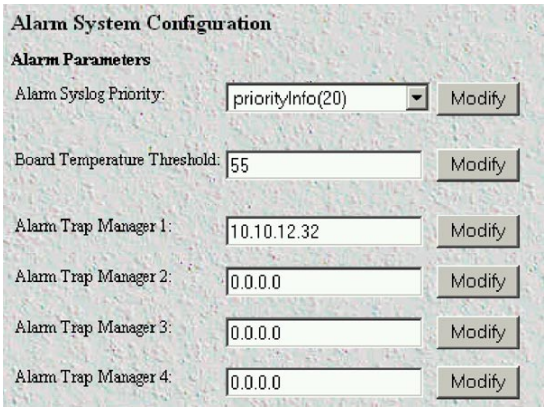


Figure 15. Alarm System Configurations window

Alarms management windows

As shown in figure 11 on page 22 and figure 14, 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 15) 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 16 on page 26) 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 26)

Alarm System Configurations window

When an alarm condition occurs, by default the 6511RC does the following to notify administrators of the alarm:

- Activates the front and rear panel Alarm LEDs
- Activates the alarm indications on the 6511RC 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 6511RC 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 11 on page 22) to open the *Alarm System Configurations* window (see figure 15). 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 6511RC 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 6511RC 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 13, "System Log" on page 111.

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 6511RC. Upon the occurrence of an alarm, the 6511RC 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 6511RC 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 11 on page 22) displays the *Alarm Severity Configuration* window (see figure 16) listing of 6511RC alarms. From this window you can assign the severity for each alarm (*critical*, *major*, *minor*, *informational*, or *ignore*).

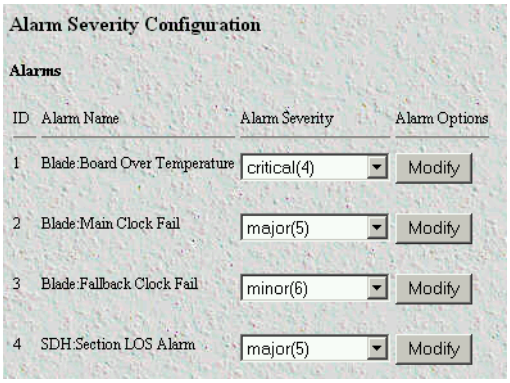


Figure 16. Alarm Severity Configuration window

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 6 on page 14) and as a flashing red star (see figure 49 on page 98) on the *System Status* window (see figure 48 on page 98).
- **major**(5)—When active, *major* alarm notifications appear as orange highlighting on the *Home* window (see figure 6 on page 14) and as an orange exclamation mark (see figure 49 on page 98) on the *System Status* window (see figure 48 on page 98).

- **minor(6)**—When active, *minor* alarm notifications appear as yellow highlighting on the *Home* window (see figure 6 on page 14) and as a yellow triangle (see figure 49 on page 98) on the *System Status* window (see figure 48 on page 98).
- **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 6511RC will not generate an alarm.

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

Note The 6511RC'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 5 DS0 Mapping

Chapter contents

Introduction

The Model 6511RC Matrix Switch concentrates the traffic capacity of up to 63 E1 lines for delivery over a 155.52 Mbps optical or electrical STM-1interface. The Matrix Switch provides an interface to the TDM midplane bus within the ForeFront chassis. The total capacity of the TDM midplane bus is 4096 simplex DS0s, the equivalent of 64 E1s. Each DS0 channel can be mapped in either direction, transmitting to the TDM midplane bus or receiving from the TDM midplane bus. The 6511RC places the DS0 traffic into the STM-1 multiplexer for transport over the SDH network. To place DS0 traffic from the TDM midplane bus to the STM-1 you must define a *DS0 mapping* (also called an *internal connection* or *cross-connection*). The source is DS0 traffic on the H.110 side, and the destination are STM-1 virtual containers. The 6511RC's *DS0 Mapping Overview* window (see figure 17) provides the means for managing (mapping) internal connections.

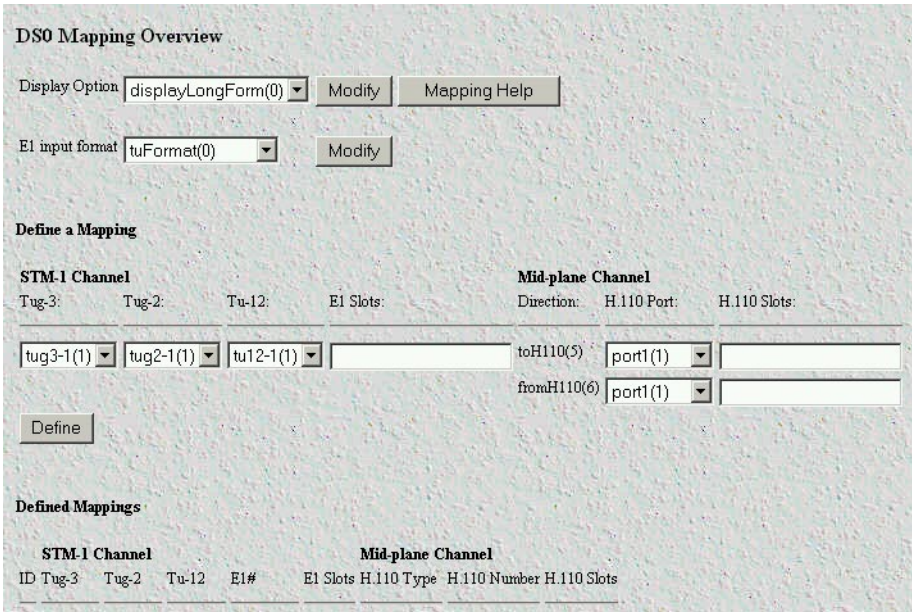


Figure 17. DS0 Mapping Overview window

Devices connect to the 6511RC via the STM-1 optical or electrical interface, and H.110 ports. (A device will connect to an H.110 port via the 6511RC's interface to the TDM midplane bus in the cPCI chassis midplane). Each DS0 mapping defines a one-to-one connection between a selected number of timeslots on one H.110 port and an E1 port or a TU-12. Use the *DS0 Mapping* management web page to define these DS0 mappings (internal connections) and to view previously defined mappings.

DS0 Mapping Overview main window

The *DS0 Mapping Configuration* window and related windows provide the means for you to manage the 6511RC DS0 mapping subsystem. To display the *DS0 Mapping Configuration* window (see figure 17), on the 6511RC Configuration Menu, click the *DS0 Mapping* link.

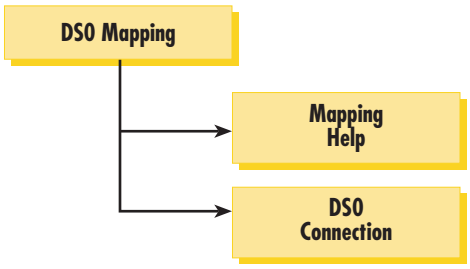


Figure 18. DS0 Mapping diagram

The DS0 mapping window contains the following:

- *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 32)
- E1 input format menu used to select Tug format (*tuFormat)* or the E1 Format (*E1PortFormat*)
- *Configure Static Connections* section in Tu or E1 format where you can create the cross-connections (see section "Defining a DS0 map using the Long Form" on page 32 or section "Defining DS0 mappings using the command line interface (CLI)" on page 36)
- Static Connection section where you can view the previously defined DS0 mappings (cross-connections) in the 6511RC (see section "Defined Mappings table (static connections)" on page 38)

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 "Defining a DS0 map using the Long Form" on page 32 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 36 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 18). The *DS0 Mapping Help* page provides a convenient online tutorial on how to use the 6511RC'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.

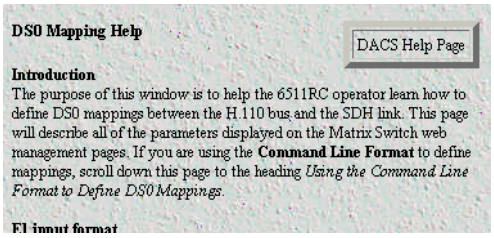


Figure 19. DACS Help Information window

Defining a DS0 map using the Long Form

DS0 connections can be entered using one of two E1 input formats:

- TU (Tributary Unit) format—DS0s from the TDM midplane bus are mapped into E1 timeslots which in turn are placed into TU-12 containers with a max capacity for 32 E1 DS0s each (see figure 20).
- E1 port format—DS0s from the H.110 are placed into E1 timeslots corresponding to one of 63 E1 ports.

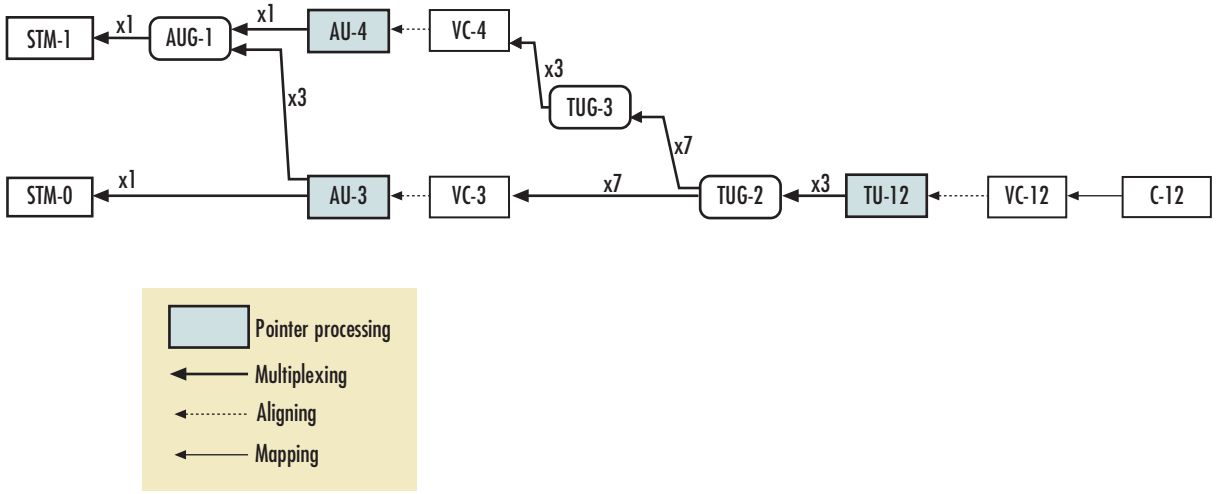


Figure 20. SDH multiplexing diagram

TuFormat static connections

To create a DS0 map (cross-connection) between the DS0s from the H.110 and the STM-1 containers using the *TuFormat* follow the instructions below.

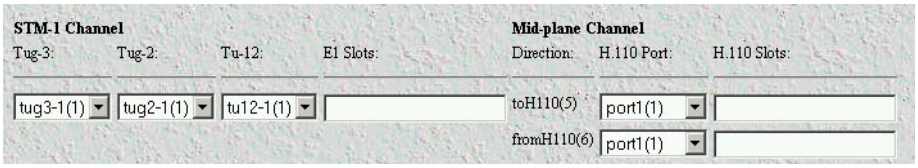


Figure 21. Configure Static Connections section of DS0 Mapping Configuration window

The drop-down menus in the Defining a Mapping section of the DS0 Mapping Configuration window (see figure 21) are organized into *tug-3, tug-2, Tu12* and *H.110* fields, the *Tu* designators follow standard SDH/ STM-1 terminology. In *displayLongForm* mode, you will use drop-down menus and text boxes to define the DS0 mapping parameters. The following parameters define each channel mapped connection (see figure 21).

- TUG level 3 (*tug3*)
- TUG Level 2 (*tug2*)
- TU-12 Level (*tu12*)
- E1 Slots *(Slots)*
- H.110 Direction (*toH110, fromH110)*
- H.110 port number
- H.110 Slots

TUG-3 (Tributary Unit Group 3) (tug3)

There are three TUG-3 multiplexers in a STM-1. Each TUG-3 accepts up to 7 TUG-2 (21 E1 capacity). The options are:

- tug3-1(1)
- tug3-2(2)
- tug3-3(3)

TUG-2 (Tributary Unit 2) (tug2)

Each TUG-2 container carries up to 3 E1s. Up to 7 TUG-2 are carried in a TUG-3 container. The options are:

- tug2-1(1)
- tug2-2(2)
- tug2-3(3)
- tug2-4(4)
- tug2-5(5)
- tug2-6(6)

- tug2-7(7)

TU-12 (Tributary Unit 12) (tu12)

Each TU-12 container takes one E1 (32 DS0 Slots). Groups of 3 TU-12s are placed into TUG2 containers. The options are:

- tu12-1(1)
- tu12-2(2)
- tu12-3(3)

E1 Slots

The field labeled *E1 Slots* accepts values from 1 to 32, these correspond to DS0s mapped from and two the H.110 bus.

H.110 Direction

Display indicating the direction of traffic to and from the TDM midplane bus.

H.110 Port Number

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 define the transmit port (to the TDM midplane bus) and parameters in the second row define the receive port (from the TDM midplane bus). There are up to 32 configurable H.110 ports.

H.110 Slot

H.110 ports can support up to 128 slots (DS0s).

> **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 the H.110 ports in either direction must be the same.

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.

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

E1 port format static connections

The E1 port long format allows an STM-1 multiplexer to be defined in E1 Port terms. Instead of representing STM-1 multiplexing in terms of TUG-2 or TUG-3, the E1 Port format simply shows all 63 E1 ports carried by the STM-1 interfaces, enabling direct DS0 mapping from the TDM midplane bus onto any of the 63 E1s.

The drop-down menus for the E1 format screens are organized as follows:

- Port Type
- E1 Number
- E1 Slots
- H.110 Direction (*toH110, fromH110)*
- H.110 port number
- H.110 Slots

Port Type

This is a fixed E1 port.

E1 Number

Selects the E1 number. Options are from 1 to 63.

Slots

The field labeled *Slots* accepts values anywhere from 1–32, these correspond to DS0s within any of the 63 E1s.

H.110 Port Number

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 define the transmit port (to the TDM midplane bus) and parameters in the second row define the receive port (from the TDM midplane bus). There are up to 32 configurable H.110 ports.

H.110 Slot

Each H.110 port can support up to 128 slots (DS0s).

> **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 the H.110 ports in either direction must be the same.

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.

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:

t1-e1:Port#:Slots/toH110:Port#:Slots/fromH110:Port#:Slots

- *t1-e1*—The fixed format for E1 ports in the STM-1 hierarchy.
- *Port# (1–63)*—Any of the 63 E1s available.
- *Slots (1–32)*—E1 timeslots range from 1 through 32.
- *to H110:Port#*—Indicates the H.110 port number and transmission from 6511RC to TDM midplane bus

> **Note** There are a maximum of 32 ports available for the TDM midplane bus. If the port number selected is not within the range supported an error will be generated.

- *Slots:*—Number of H.110 slots (1–128). The range should have a maximum of 32 slots, this corresponds to the maximum capacity of 32 slots per E1.
- *FromH.110: Port #*–Indicates the H.110 port number and transmission from TDM midplane bus to 6511RC.
- *Slots*—Number of H.110 slots (1–128). The range should have a maximum of 32 slots, this corresponds to the maximum capacity of 32 slots per E1.

> **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 *toH.110* must be the same as the number of time slots defined for *fromH.110*.

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.
- 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:

To define a DS0 mapping between a E1 line, Port 1, timeslots 1–32, sent to H.110 port 1, timeslots 1–32 and from H.110 port 2, timeslots 1–32 type the following text:

t1-e1:1:1-32/H.110:1:1-32/H.110:2:1-32

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 6511RC'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 *Define a Mapping* (static connections) section of the *DS0 Mapping Configuration* window (see figure 22) displays all previously defined DS0 mappings (cross-connections) in the 6511RC. The parameter details are described in the following paragraphs.

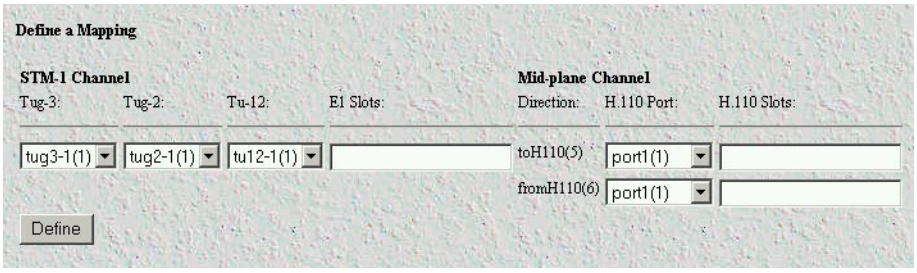


Figure 22. Configure Static Connections section of DS0 Mapping Configuration window

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 6511RC assigns connection IDs automatically. When the user enters DS0 mapping parameters and clicks the **Submit Query** button, the 6511RC automatically assigns the next available ID number in sequence to that connection.

Tug-3

Displays the type of STM-1 multiplexed TUG-3 group.

Tug-2

Displays the type of STM-1 multiplexed TUG-2 group.

Tu-12

Displays the type of STM-1 multiplexed TU-12 group.

E1

Displays the E1 port number.

E1 Slots

Displays which 64-kbps time slots (also referred to as the *DS0 data communications channels*) are used for the corresponding E1 port.

H.110 Type

Displays the direction of timeslots in reference to the TDM midplane bus.

H.110 Number

Displays the H.110 port number.

H.110 Timeslots
Displays the H.110 timeslots.

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).

Chapter 6 System Clocking

Chapter contents

Introduction

During operation, the T-DAC synchronizes data transmission on all DS0 channels with a clock pulse, called the reference clock. This reference clock synchronizes all the cards in the ForeFront chassis, or all the cards in a chassis segment in the Model 6676 ForeFront chassis. The configuration of the system clocking parameters select the source for that clock pulse. (The T-DAC generates the synchronizing clock from this source). In the following discussion, the clock sources are called Main Reference and Fallback Reference on the web management pages.

The clocking subsystem includes a fallback auto-recovery mechanism by which the T-DAC monitors a Main clock Reference (source) and switches to a Fallback Reference (source) if the main reference becomes unavailable. Once the main reference clock is re-established, the auto-recover feature switches the clocking back to the main reference. By default, the clocking fallback mechanism is disabled at the factory prior to the T-DAC's shipment. To activate the T-DAC's fallback system, you must enable it.

The following parameters control the T-DAC's clocking subsystem: *Module Clocking Mode*, *Module Clocking Source*, and *Module Clocking Fallback*.

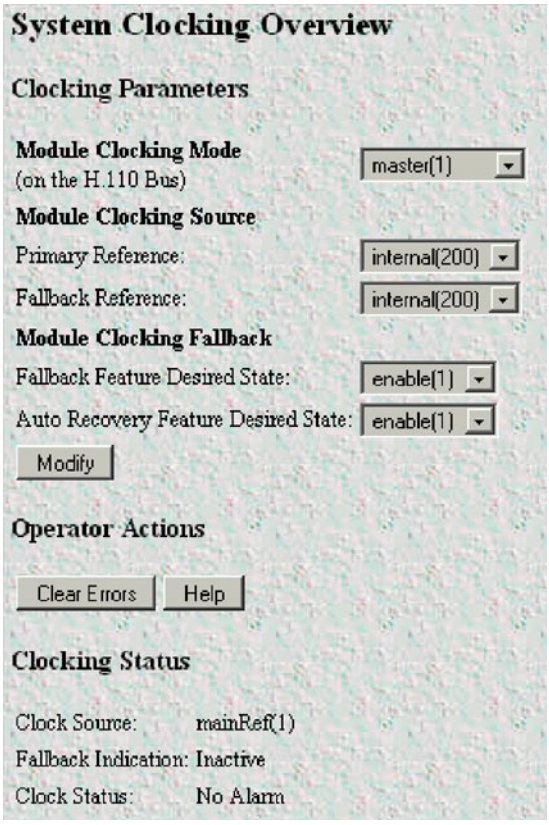


Figure 23. System Clocking Overview window

System Clocking Overview window

The *System Clocking Overview* window enables you to define the system clocking parameters and view certain clocking status information. To display the *System Clocking Overview* window (see figure 23), click the *System Clocking* link on the *Configuration Menu* pane.

The *System Clocking Overview* window includes the following items:

- *Clocking Parameters* section—Displays the configurable system clocking parameters and non-configurable (display-only) parameters (see section "Clocking Parameters section" on page 43).
- *Operator Actions* buttons section—Provides buttons for clearing the system fallback state, forcing the 6511RC into fallback clocking state, clearing error conditions, and displaying the clocking help window (see section "Operator Actions buttons" on page 44).
- *Clocking Status Information* table—Displays a set of display-only parameters intended for use by software engineers during field debugging. Therefore, most 6511RC end-users will not use this information. (See section "" on page 45.)

Clocking Parameters section

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 46).

Module Clocking Fallback (sysGSClockMode)

The *Fallback Feature Desired State* and the *Auto Recovery Feature Desired State* parameters define the 6511RC's clocking fallback and fallback auto recovery mechanism as enabled or disabled.

The fallback feature, when enabled, allows the 6511RC to switch to a secondary clock as follows:

- Master or secondary mode—The 6511RC, upon failure of the primary reference clock source, will switch to the selected fallback reference clock source.
- Slave Mode—The 6511RC defaults (fallback feature options are not accessible to user) to system for both main reference and fallback reference—since the slave cards do not provide clock to the chassis, they receive clock from the system clocking bus provided by a master or secondary card.

By default, the clocking fallback mechanism is disabled at the factory before the 6511RC is shipped. To activate the 6511RC's fallback system you must enable it. When disabled, the 6511RC will not use the fallback reference clocking source, even if the primary reference becomes unavailable. To define the enable or disable the fallback system parameter, select one of the following values from the drop-down menu.

- disable(0)
- enable(1)

Once you have defined the desired value for the *Enable/Disable Fallback System* parameter, you must click the **Modify** button below the auto recovery feature menu to save your selection into volatile DRAM.

The *Auto Recovery Feature Desired State*, when enabled, will cause a 6511RC (in master or secondary mode), which is operating on fallback reference clock due to a failure of the primary reference clock, to switch back to primary reference clock when it becomes available.

By default, *Auto Recovery Feature Desired State* is disabled at the factory before the 6511RC is shipped. To activate the 6511RC's clock auto recovery system you must enable it. When disabled, the 6511RC, operating on fallback reference clock, will not switch back to primary reference clock, even if the primary reference becomes available. To define the enable or disable the fallback system parameter, select one of the following values from the drop-down menu.

- disable(0)
- enable(1)

Once you have defined the desired value for the *Enable/Disable Auto Recovery System* parameter, you must click the Modify button below the auto recovery feature menu to save your selection into volatile DRAM.

Module Clocking Source (daxClockMainRef and daxClockFallbackRef)

The *Primary Reference* and *Fallback Reference* parameters define a primary and secondary (fallback) reference for the 6511RC system clock source (and for all blades in the chassis when the 6511RC's clocking mode is defined as master). The 6511RC 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 6511RC is shipped. To activate the 6511RC's fallback system you must enable it (see section "Module Clocking Fallback").

When defining the main and fallback clocking sources, you can select the STM-1 WAN port, the 6511RC internal clock pulse oscillator, or a system clock provided by another blade in the same chassis. The 6511RC will use the main reference as its system clocking source unless the main reference fails or is disconnected. When the primary reference becomes unavailable 6511RC 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 6511RC's fallback mechanism (see Enable/Disable Fallback System). For the 6511RC's primary and secondary clocking references, you can choose:

- WAN(602)—Clocking derived from the SDH network clock received at the STM-1 interface.
- internal(200)—Uses the 6511RC internal free-running oscillator for the clock source.
- system(500)—Uses the system clock reference provided by another blade in the chassis for the clock source. Automatically selected when the card is operating in slave mode.

Module Clocking Fallback

This parameter defines the 6511RC's clocking fallback mechanism as enabled or disabled. By default, the clocking fallback mechanism is disabled at the factory before the 6511RC is shipped. To activate the 6511RC's fallback system you must enable it. When disabled, the 6511RC will not use the fallback reference clocking source, even if the primary reference becomes unavailable. To define the enable or disable the fallback system parameter, select one of the following values from the drop-down menu.

- disable(0)
- enable(1)

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

Operator 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 6511RC 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 6511RC into the fallback clocking state by setting the value of FallBack State to fallback(1). The 6511RC will switch to the defined fallback reference as its clocking source.
- Clear Errors—Clicking the **Clear Errors** button clears the 6511RC's error condition for all clock signals. For all clock signals, the 6511RC 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 24).

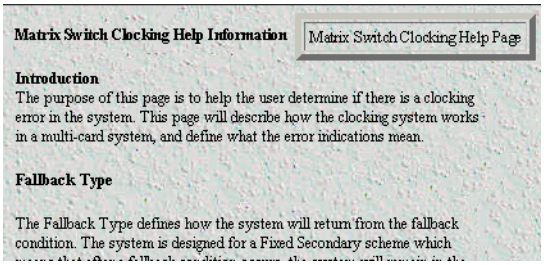


Figure 24. System Clocking help window

Clocking Status section

The *Clocking Status* displays status information for *Clock Source, Fallback Indication*, and *Clock Status*.

Clock Source

Indicates the clock source in use, possible values are:

- unknown(0)
- mainRef(1)
- fallbackRef(2),
- masterClk(3),
- secondaryClk(4),
- internal(5)

Fallback Indication

Displays status of fallback system:

- Inactive—The 6511RC clock is derived from the main reference clock.
- Active—The 6511RC has switched its clocking source to the fallback reference clock.

Clock Status

Displays the presence of clock alarms since last time unit was rebooted or last time alarms were cleared.

- No Alarm
- Alarms

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.

Chapter 7 Ethernet

Chapter contents

Introduction

The access server provides management and statistical information in the *Ethernet Overview* window (see figure 25). Detailed information regarding the SNMP MIB II variables may be downloaded from *RFC 1643, Definitions of Managed Objects for the Ethernet-like Interface Types*.

Click on *Ethernet* under the *Configuration Menu* to display the *Ethernet Overview* main window.

The *Ethernet Overview* main window displays information about the configuration of the Ethernet interface including IP addresses, subnet masks, and state of the Ethernet link.

The Ethernet interface contains the following links:

- *Ethernet Statistics* link—Clicking on the *Statistics* link takes you to the page where you can see the statistics on the ethernet interface. For more information about the *Statistics* page, refer to "Ethernet Statistics window" on page 51.
- *Modify Parameters…* link—Clicking on the *Modify* link takes you to the page where you can change the configuration of your ethernet interface. For more information about modifying Ethernet settings, refer to "Ethernet Configuration window" on page 50.

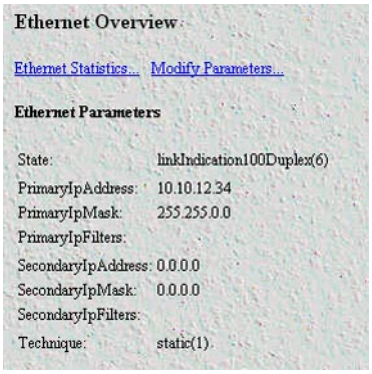


Figure 25. Ethernet Overview main window

Ethernet main window

The *Ethernet* main window shows the current configuration of the Ethernet interface. The following sections describe each parameter.

State (boxEtherAState)

Indicates the state of the ethernet interface. The following states are valid:

- notInstalled(0)—Ethernet interface is not physically present
- noLinkIndication(1)—no cable is connected to the Ethernet interface. Hub is not seen.
- adminOff(2)—Ethernet interface has been turned off by setting technique to disable
- linkIndication10M(3)—Ethernet is 10M
- linkIndication10Duplex(4)—Ethernet is 10M full duplex

- linkIndication100M(5)—Ethernet is 100M
- linkIndication100Duplex(6)—Ethernet is 100M full duplex

PrimaryIPAddress (boxEtherAPrimaryIpAddress)
The primary Ethernet IP address.

PrimaryIpMask (boxEtherAPrimaryIpMask)
The primary Ethernet IP subnet mask.

PrimaryIpFilters (boxEtherAPrimaryIpFilters)
Filters packets based on the filters assigned to the Primary IP address of the Ethernet port. Enter the filter ID of a filter configured under *Filter IP*. Use a comma (,) to separate multiple filters.

SecondaryIpAddress (boxEtherASecondaryIpAddress)
The secondary Ethernet IP address.

> **Note** This address is not propagated via RIP.

SecondaryIpMask (boxEtherASecondaryIpMask)
The secondary IP Ethernet IP subnet mask.

SecondaryIpFilters (boxEtherASecondaryIpFilters)
Filters packets based on the filters assigned to the secondary IP address of the Ethernet port. Enter the filter ID of a filter configured under *Filter IP*. Use a comma (,) to separate multiple filters.

> **Note** Only outbound filters can be applied to the secondary Ethernet. Inbound filters for the secondary Ethernet must be entered in the *Primary IP Filter* field.

Technique (boxEtherATechnique)
Turns ethernet port off and on. The remote access server must be reset for this setting to take effect.

- disable(0)—Ethernet port is disabled
- static(1)—Ethernet port is turned on. IP address(es) and mask(s) are obtained from data entered under the *Ethernet* link.

Ethernet Configuration window

The Ethernet Configuration window (see figure 26) allows you to make changes to the Ethernet configuration.

To reach this window, select *Modify Parameters…* from the *Ethernet Overview* main window.

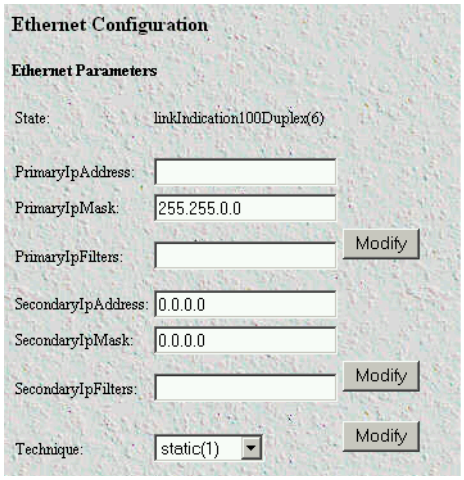


Figure 26. Ethernet Configuration window

State (boxEtherAState)

Indicates the state of the Ethernet interface. The following states are valid:

- notInstalled(0)—Ethernet interface is not physically present
- noLinkIndication(1)—no cable is connected to Ethernet interface. Hub is not seen.
- adminOff(2)—Ethernet interface has been turned off by setting technique to disable
- linkIndication10M(3)—Ethernet is 10M
- linkIndication10Duplex(4)—Ethernet is 10M full duplex
- linkIndication100M(5)—Ethernet is 100M
- linkIndication100Duplex(6)—Ethernet is 100M full duplex

PrimaryIPAddress (boxEtherAPrimaryIpAddress)

The primary Ethernet IP address.

PrimaryIpMask (boxEtherAPrimaryIpMask)

The primary Ethernet IP subnet mask.

PrimaryIpFilters (boxEtherAPrimaryIpFilters)

Filters packets based on the filters assigned to the Primary IP address of the Ethernet port. Enter the Filter ID of a filter configured under Filter IP. Use a comma (,) to separate multiple filters.

SecondaryIpAddress (boxEtherASecondaryIpAddress)
The secondary Ethernet IP address.

Note This address is not propagated via RIP.

SecondaryIpMask (boxEtherASecondaryIpMask)
The secondary IP Ethernet IP subnet mask.

SecondaryIpFilters (boxEtherASecondaryIpFilters)
Filters packets based on the filters assigned to the Secondary IP address of the Ethernet port. Enter the Filter ID of a filter configured under Filter IP. Use a comma (,) to separate multiple filters.

Technique (boxEtherATechnique)
Turns Ethernet port off and on. The remote access server must be reset for this setting to take effect.

- disable(0)—Ethernet port is disabled
- static(1)—Ethernet port is turned on. IP address(es) and mask(s) are obtained from data entered under the *Ethernet* link.

Ethernet Statistics window

The Ethernet Statistics window (see figure 27) shows statistics about the Ethernet interface. To reach this window select *Ethernet Statistics…* from the *Ethernet Overview* main window.

Alignment Errors (dot3StatsAlignmentErrors)
The number of frames received that are not an integral number of octets in length and do not pass the FCS check.

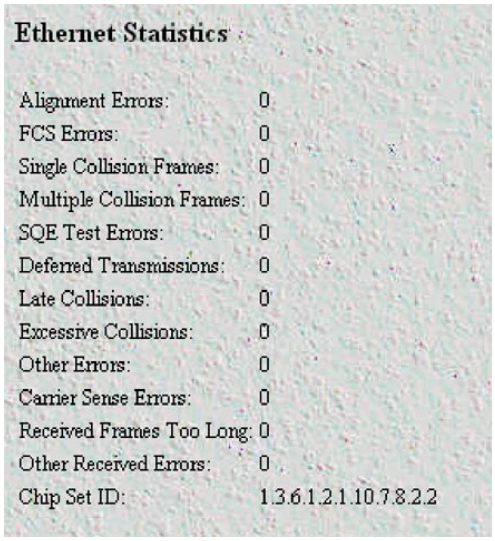


Figure 27. Ethernet Statistics window

FCS Errors (dot3StatsFCSErrors)
The number of frames received that are an integral number of octets in length but do not pass the FCS check.

Single Collision Frames (dot3StatsSingleCollision Frames)
The number of successfully transmitted frames in which there was exactly one collision.

Multiple Collision Frames (dot3StatsMultipleCollisionFrames)
The number of successfully transmitted frames in which there was more than one collision.

SQE Test Errors (dot3StatsSQETestErrors)
The number of times that the SQE TEST ERROR message is generated by the PLS sublayer.

Deferred Transmissions (dot3StatsDeferredTransmissions)
The number of times in 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.

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

Other Errors (dot3StatsInternalMacTransmitErrors)
The number of frames transmission on a fails due to an internal MAC sublayer transmit error.

Carrier Sense Errors (dot3StatsCarrierSenseErrors)
The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame on a particular interface.

Received Frames Too Long (dot3StatsFrameTooLongs)
The number of frames received that exceed the maximum permitted frame size.

Other Received Errors (dot3StatsInternalMacReceiveErrors)
The number of frames in which reception fails due to an internal MAC sublayer receive error.

Chip Set ID (dot3StatsEtherChipSet)
Ethernet-like interfaces are typically built out of several different chips. This value identifies the chip set that gathers the transmit and receive statistics and error indications.

Chapter 8 IP

Chapter contents

Introduction

The 6511RC's IP subsystem manages addressing and routing parameters and statistics pertaining to IP protocol operation on the 6511RC. 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 6511RC's configuration menu pane, to display the *IP Overview* main window (see figure 28).

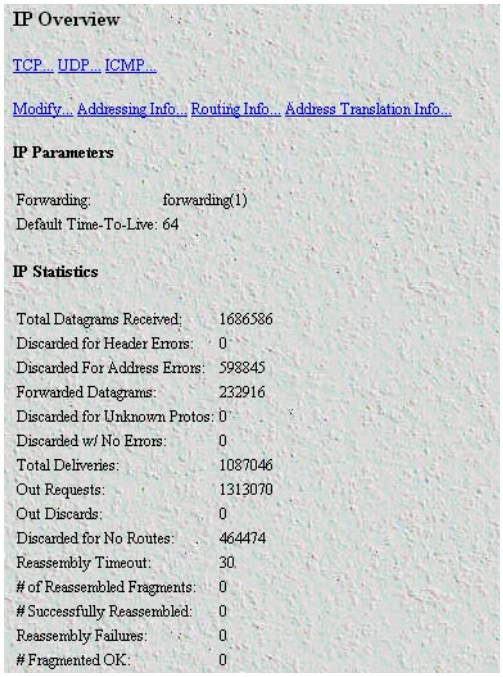


Figure 28. IP Overview main window

IP main window

The *IP Overview* main window provides hyperlinks to the windows shown in figure 29.

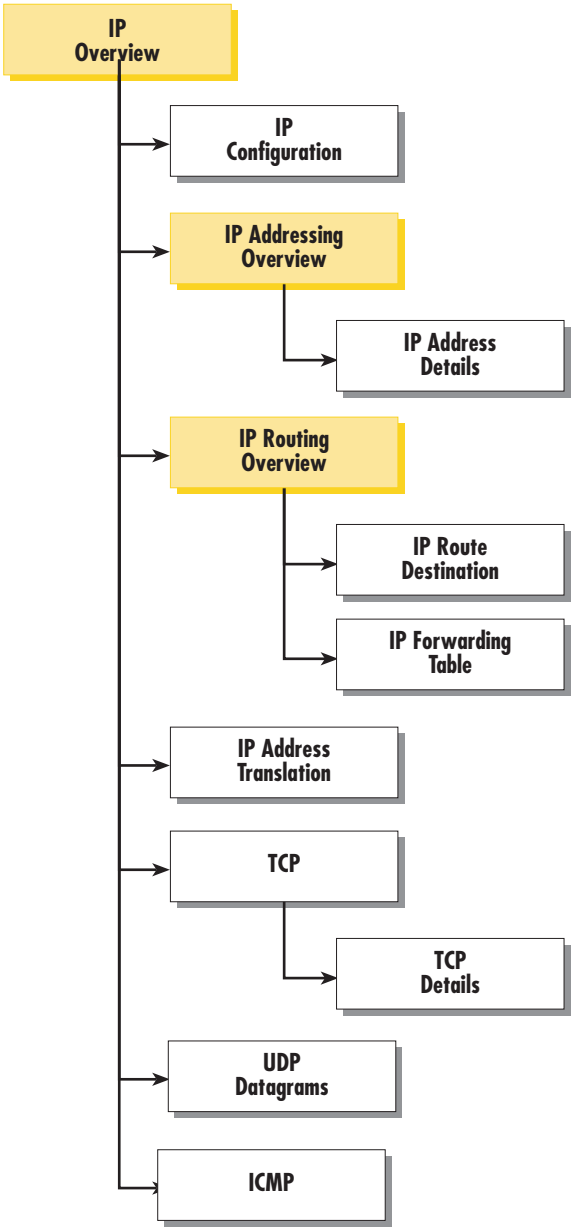


Figure 29. *IP Overview* main window and related windows

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 29. 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 Overview main window" on page 114).
- **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 59).
- **Addressing Info**—Clicking the Addressing hyperlink displays the IP Addressing Overview sub-window. This window (see "IP Addressing Information window" on page 61) displays each IP address and its associated 6511RC 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 6511RC 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 6511RC's routing table by defining IP routing parameters (see "IP Routing Information window" on page 62).
- **Address Translation Info**—Clicking the Address Translation hyperlink displays the IP address translation sub-window where you can view and define the 6511RCs physical to logical (MAC to IP) address correlations (mappings) (see "Address Translation Information window" on page 68).

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 6511RC acts as an IP gateway in respect to the forwarding of datagrams received by, but not addressed to the 6511RC. 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 6511RC, 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 6511RC. 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 6511RC 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 6511RC, 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 6511RC.

of Reassembled Fragments
The number of IP fragments received which needed to be reassembled at the 6511RC.

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 6511RC.

Fragmented Failed
The number of IP datagrams that have been discarded because they required fragmenting at the 6511RC, 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 6511RC.

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 30) provides the means for you to view and modify the values of the IP Forwarding and Default Time-to-Live parameters for the 6511RC.

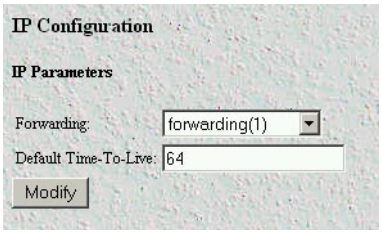


Figure 30. IP Configuration window

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

Forwarding (ipForwarding)

Determines whether the 6511RC is acting as an IP gateway that will forward datagrams received by-but not addressed to-the 6511RC. 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 6511RC, 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 subpage, you must click the **Submit Query** button to save the new values into volatile DRAM. Once you click the button, the 6511RC will implement the changes immediately.

> **Note** To save your changes permanently, you must visit the 6511RC HOME page, and click the Save Current Configuration button. When you click the Save Current Configuration button, the 6511RC 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 31) provides the means for you to view the default address for outgoing IP datagrams, the IP addresses defined for the 6511RC and the interface ID associated with each address.

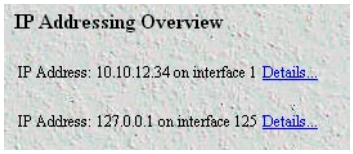


Figure 31. IP addressing Information window

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 32) displays the contents of the 6511RC'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.

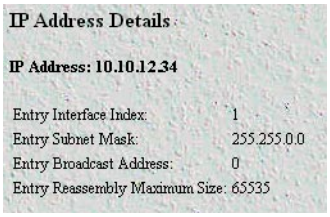


Figure 32. Address window

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 6511RC can re-assemble from incoming IP fragmented datagrams received on this interface.

IP Routing Information window

The IP Routing Information window (see figure 33) 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.

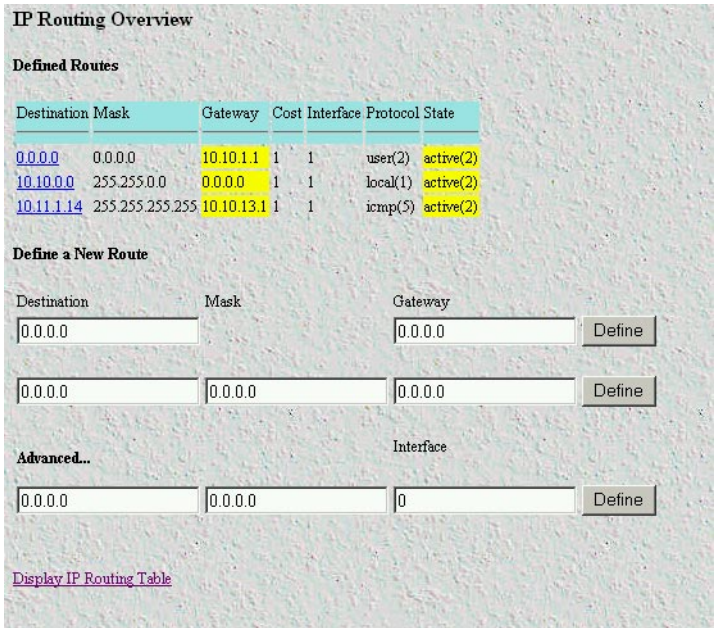


Figure 33. IP Routing Information sub-page

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 6511RC's operating system uses to make IP forwarding decisions. (see "Forwarding Table" on page 66).

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 64.

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 3.

Table 3. 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 **Define**.

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 3 on page 63.

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 **Define**.

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 3 on page 63.

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

Route Destination window

The Route Destination sub-page (see figure 34) 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.

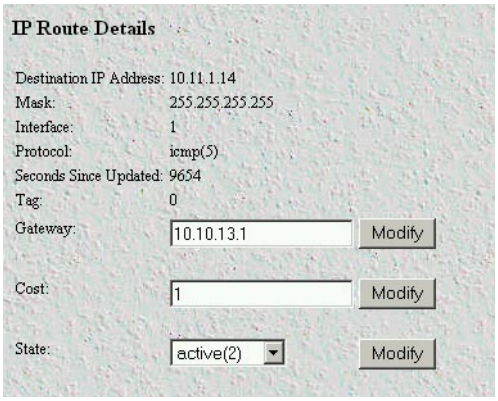


Figure 34. Routing Destination window

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 3 on page 63.

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 its higher cost.

Forwarding Table

The Forwarding Table window (see figure 35) displays the IP forwarding parameters for all routes in the 6511RC's forwarding table. To display the Forwarding Table window, on the IP Routing Information subpage, click the O/S forwarding table link.

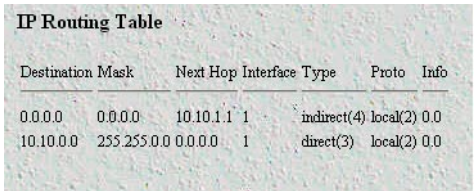


Figure 35. Forwarding Table window

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 3 on page 63.

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 36) displays the contents of the 6511RC's logical-to-physical address translation table. The 6511RC 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 6511RC's interfaces are using an address translation table.

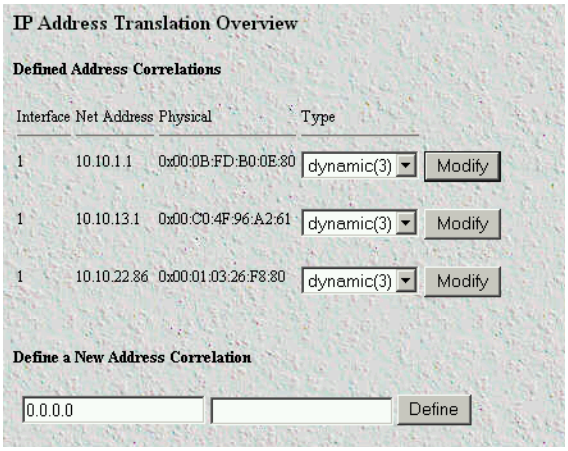


Figure 36. Address Translation Information window

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 9 IP Filtering

Chapter contents

Introduction

The access server software provides an IP filtering system that enables you to set up security as well as to provision services for selected customers. While IP filters are typically thought of as a security measure, many providers wish to limit some services a customer may have access to. These could include such things as limited access only to an e-mail server or proxy server. IP filters also include the ability to encapsulate all packets received on the specified dialup link in an extra IP header using RFC 2003. This would allow packets on a dialup link to be tunneled to a specific host.

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 access server enables 20 separate filters to be defined, of which up to 10 can be used on a single user connection. A single filter can be assigned to a user via the Static Users Authentication. Multiple filters can be assigned by using the RADIUS Filter-Id attribute.

Filters can be configured with default settings that are used for all dial-in sessions. If any filters are applied through either RADIUS or the Static User filter parameter, then all of the dial-in defaults will be disabled and only the specified filters will be applied.

Click on *Filter* IP under the *Configuration Menu* to display the *IP Filtering Overview* main window (see figure 37). The following sections describe each of the parameters found in the *IP Filtering Overview* main window.

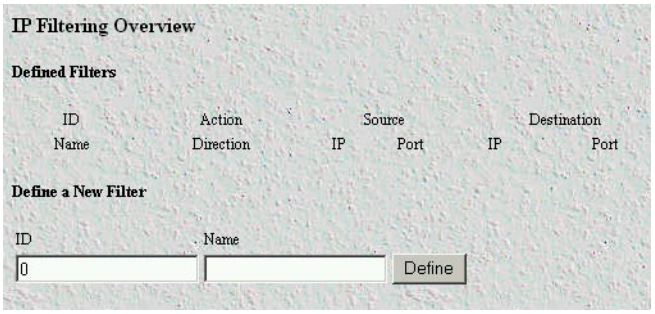


Figure 37. IP Filtering Overview main window

Defining a filter

To define a new filter, select a number and a name, then click on the **Define** button to submit the request. The number and name must not already exist in the IP FILTER list, and the number must be an integer between 1 and 20. To delete a filter, enter just the ID number without a name and click on the **Define** button.

Modify Filter

After entering a number and name, click on the name of the filter to display the filter parameters window (see figure 38).

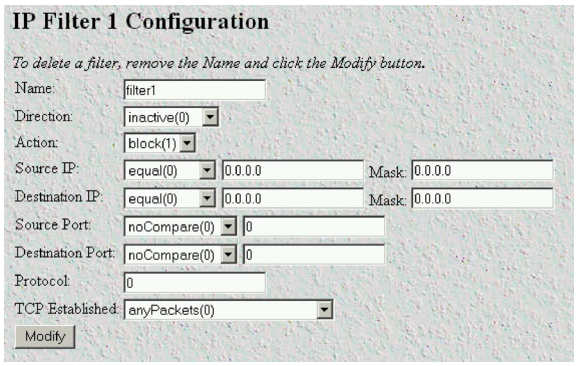


Figure 38. Filter IP parameters window

The following parameters can be configured for IP Filtering:

Note Any changes to a filter take place immediately. This can aid in troubleshooting a filter profile while the user is online.

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 access server). The filter only applies to dial in users, users on other interfaces (that is, Ethernet, Frame Relay, and so on) are not affected. The following options are available:

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

Note Enabling or disabling filters that are applied to dial-in users who are currently online will immediately change those users' ability to send or receive packets, depending on the changes that are made to the filters.

Action (filterIpAction)

Specifies the action to take on a packet 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 dialup 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 remote access server.

  All wrap filters are inbound only.

  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.

Source IP

Applies the filter action based on the results of the stated comparison to the IP address and subnet mask.

Comparison (filterIpSourceAddressCmp)

- equal(0)—apply the action of the filter if the Source IP equals the IP address/subnet mask combination supplied
- notEqual(1)—apply the action of the filter if the Source IP does not equal the IP address/subnet mask combination supplied

Address (filterIpSourceIp)

The IP address to which the filter will compare the source IP address.

Mask (filterIpSourceMask)

The subnet mask the filter will apply to the source IP address to make the comparison.

Note These fields are ignored unless either the IP address or Mask have been entered. Bit positions that are set to 1 will be compared and 0s will be ignored. Thus, a setting of 0.0.0. will have the effect of disabling source IP address comparison.

Destination IP

Applies the action based on the results of the stated comparison to the IP address and subnet mask.

Comparison (filterIpDestinationAddressCmp)

- equal(0) – apply the action of the filter if the destination IP equals the IP address/subnet mask combination supplied
- notEqual(1) – apply the action of the filter if the destination IP does not equal the IP address/subnet mask combination supplied

Address (filterIpDestinationIp)

The IP address the filter will apply to the destination IP address to make the comparison.

Mask (filterIpDestinationMask)

The subnet mask the filter will apply to the destination IP address to make the comparison.

Note These fields are ignored unless either the IP address or Mask have been entered. Bit positions that are set to 1 will be compared and 0s will be ignored. Thus, a setting of 0.0.0. will have the effect of disabling destination IP address comparison.

Source Port

Applies the filter action based on the stated comparison to the source port number (TCP or UDP)

Comparison (filterIpSourcePortCmp)

- noCompare(0) – no comparison to the source port in the IP packet
- equal(1) – the source port in the IP action must be the same for the filter to be applied
- lessThan(2) – the source port in the IP packet must be less than the source port specified for the filter to be applied
- greaterThan(3) – the source port in the IP packet must be greater than the source port specified for the filter to be applied

Port (filterIpSourcePort)

The port number to be compared to the source port in the IP packet

Destination Port

Applies the filter action based on the stated comparison to the destination port number

Comparison (filterIpDestinationPortCmp)

- noCompare(0) – no comparison to the destination port in the IP packet
- equal(1) – the destination port in the IP action must be the same for the filter to be applied
- lessThan(2) – the destination port in the IP packet must be less than the source port specified for the filter to be applied

- greaterThan(3) – the destination port in the IP packet must be greater than the source port specified for the filter to be applied

Port (filterIpDestinationPort)
The port number to be compared to the destination port in the IP packet

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

Default for dialin (filterIpDefaultDialin)
This option applies the filter to as a default filter for all dial-in users. If another filter is specified, either in RADIUS or in the static user profiles, then all dial-in defaults are disabled and only the specified filters are applied. The following choices are available:

- no(0)
- applyToDialin(1)

An example of using a filter
All customers are limited to the local mail server (mail.internal.com) and an internal website (www.internal.com).

- The IP address for mail.internal.com is: 192.10.10.1
- for: www.internal.com is: 192.10.10.2
- DNS server for name resolution is 192.10.10.1.

The filters needed:

- ID:1
  - Name: Mail Server
  - Direction: inbound
  - Action: pass
  - Source IP and mask: not set
  - Destination IP: 192.10.10.1 mask: 255.255.255.255
  - Source Port: no compare

  - Destination Port: equal 110 for POP3 or 25 for SMTP
  - Protocol: not set
  - TCP Established: anyPackets
  - Default for dial-in: apply to Dial-in
- ID:2
  - Name: WebSite
  - Direction: inbound
  - Action: pass
  - Source IP and mask: not set
  - Destination IP: 192.10.10.2 mask: 255.255.255.255
  - Source Port: no compare
  - Destination Port: equal 80
  - Protocol: not set
  - TCP Established: anyPackets
  - Default for dial-in: apply to Dial-in
- ID:3
  - Name: DNS
  - Direction: inbound
  - Action: pass
  - Source IP and mask: not set
  - Destination IP: 192.10.10.1 mask: 255.255.255.255
  - Source Port: no compare
  - Destination Port: equal 53
  - Protocol: not set
  - TCP Established anyPackets
  - Default for dial-in: apply to Dial-in

Note If the DNS filter was not created, then users would have to use IP addresses to access the web server and the mail server.

Now if you wanted to add the ability to ping to test the dial-in users connectivity to the network, the following filter would be created:

- ID:4
- Name: PING

- Direction: both
- Action: pass
- Source IP and mask: not set
- Destination IP and mask: not set
- Source Port: no compare
- Destination Port: no compare
- Protocol: 1
- TCP Established: anyPackets
- Default for dial-in: apply to Dial-in

Note This would also allow traceroute to work.

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 37 on page 72).
2. Leaving the *Name* field blank, click on the **Define** button to delete the filter.

Chapter 10 RIP Version 2

Chapter contents

Introduction

The 6511RC provides support for Routing Information Protocol (RIP) Version 2. The 6511RC 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 Overview main window

The *RIP Version 2 Overview* main window (see figure 39) provides the means for you to manage the 6511RC'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 6511RC'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.

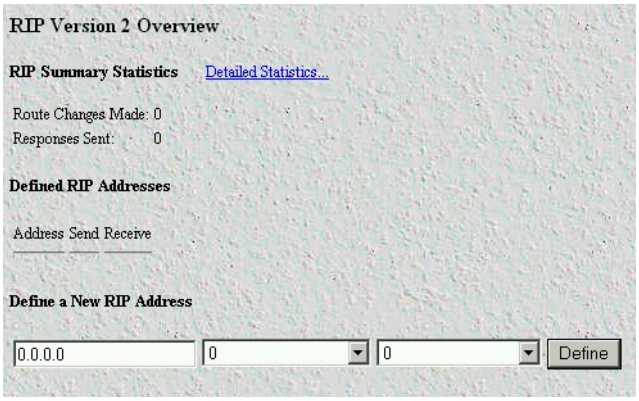


Figure 39. RIP Version 2 Overview window

To display the *RIP Version 2 Overview* main window, on the 6511RC *Configuration Menu* pane, click on the *RIP Version 2* link.

The *RIP Version 2 Overview* main window provides links to the RIP Version 2 Statistics and Parameters windows, as shown in figure 40.

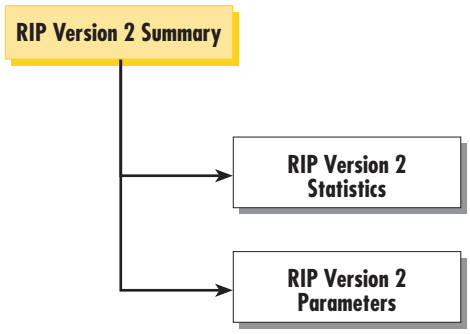


Figure 40. RIP Version 2 windows map

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 83). For each subnet IP address in the 6511RC'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 6511RC—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 83). You can use the RIP Version 2 Parameters window to view and modify the parameters for a single address.

  Initially, because the 6511RC 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 6511RC 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 83).
- **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 6511RC's RIP Version 2 table, do the following:

1. Enter the IP network address of the interface on the 6511RC that you want to enable RIP. This will be the LAN IP address, in other words, the IP address of the 6511RC. 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 **Define**.

   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 **Define**.

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 6511RC's RIP Version 2 table, the RIP Version 2 (Status) window (see figure 42) 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.

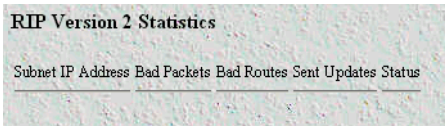


Figure 41. RIP Version 2 (Status) window

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 42) 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.

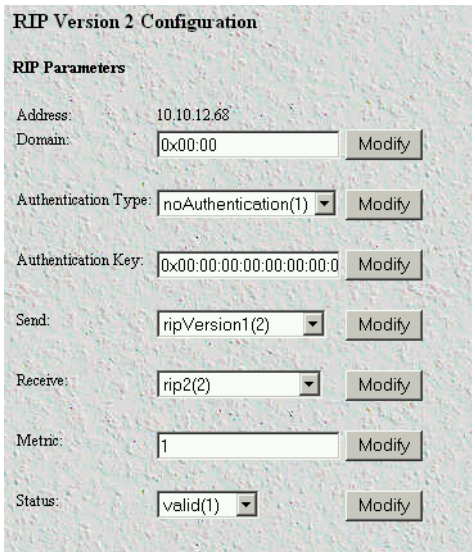


Figure 42. RIP Version 2 (Configuration) window

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 Authen-

tication 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 11 SNMP

Chapter contents

Introduction

The 6511RC SNMP subsystem provides management and statistical information about the operation of the SNMP protocol on the 6511RC.

RFC 3418: Management Information Base (MIB) for the Simple Network Management Protocol (SNMP) provides detailed information about the SNMP MIB variables that the 6511RC SNMP subsystem utilizes.

SNMP window

The *SNMP Overview* window (see figure 43), contains three sections that provide the following functions::

- **MIB Links**—Three hyperlinks to the SNMP sub-windows shown in the diagram below to display the MIB diagrams for the Corporate, Enterprise and Products MIBs. When you click one of the MIB hyperlinks, your browser will download and display the document containing the diagram for that MIB.
- **SNMP Parameters**—By selecting a value for this configurable parameter, you can enable or disable sending SNMP traps to report SNMP authentication failures.
- **SNMP Statistics**—displays statistics about the operation of the SNMP protocol on the 6511RC.Two columns display the statistical counts for incoming and outgoing SNMP messages.

To display the *SNMP Overview* window on the 6511RC configuration menu pane, click the *SNMP* hyperlink.

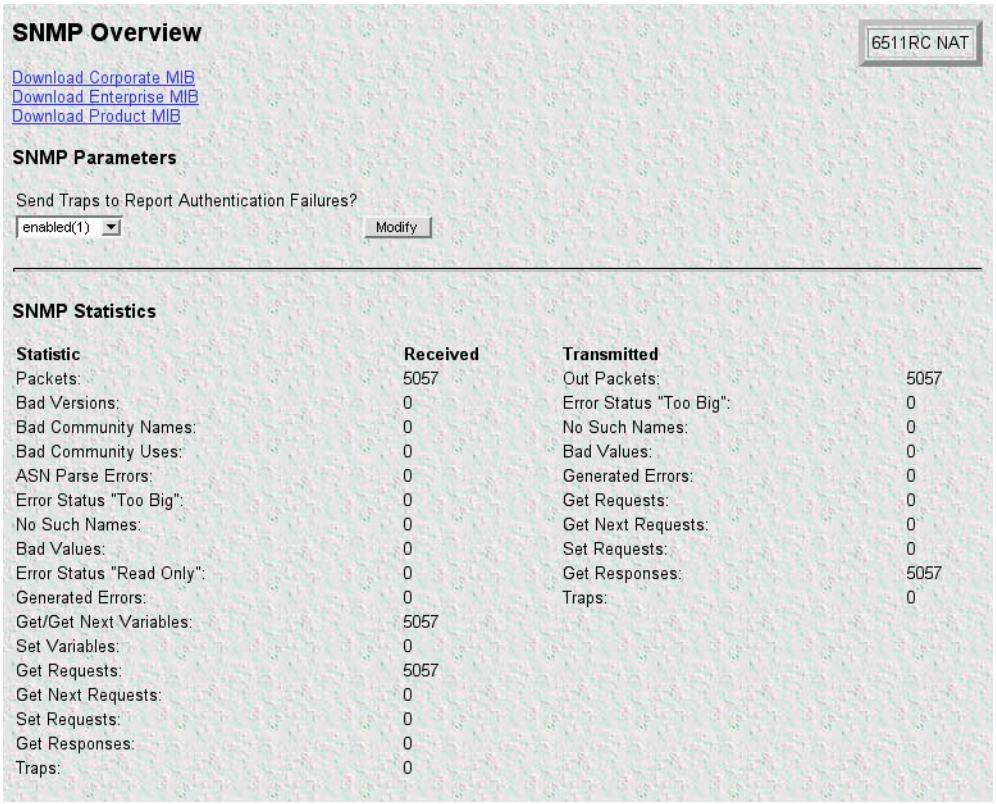


Figure 43. SNMP Overview window

MIB Links

Three hyperlinks provide access to the MIB diagrams for the Corporate, Enterprise and Products MIBs by which the Matrix Switch SNMP protocol operates. When you click one of the MIB hyperlinks, the web browser will request a location to save the MIB, then download and display the text file describing that MIB.

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 **Modify** button to save your settings into volatile DRAM. Once you click the button, the 6511RC will implement the changes immediately.

> **Note** To save your changes persistently, (i.e. through a 6511RC power cycle) you must visit the 6511RC HOME page, and click the **Record Current Configuration** button. When you click the **Record Current Configuration** button, the 6511RC will copy the configuration currently stored in volatile DRAM into non-volatile Flash memory for persistent storage.

SNMP Statistics table

The following sections describe the statistical counts displayed in the In and Out columns on the SNMP Statistics table.

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.

Chapter 12 System

Chapter contents

Introduction

The *System Status Overview* window provides an overall summary of the 6511RC Matrix Switch's current operating status. The page displays the currently operating software release and timestamp, along with such information as system temperature, power-supply and clocking status, as well as the link status of all Ethernet conections (see figure 44).

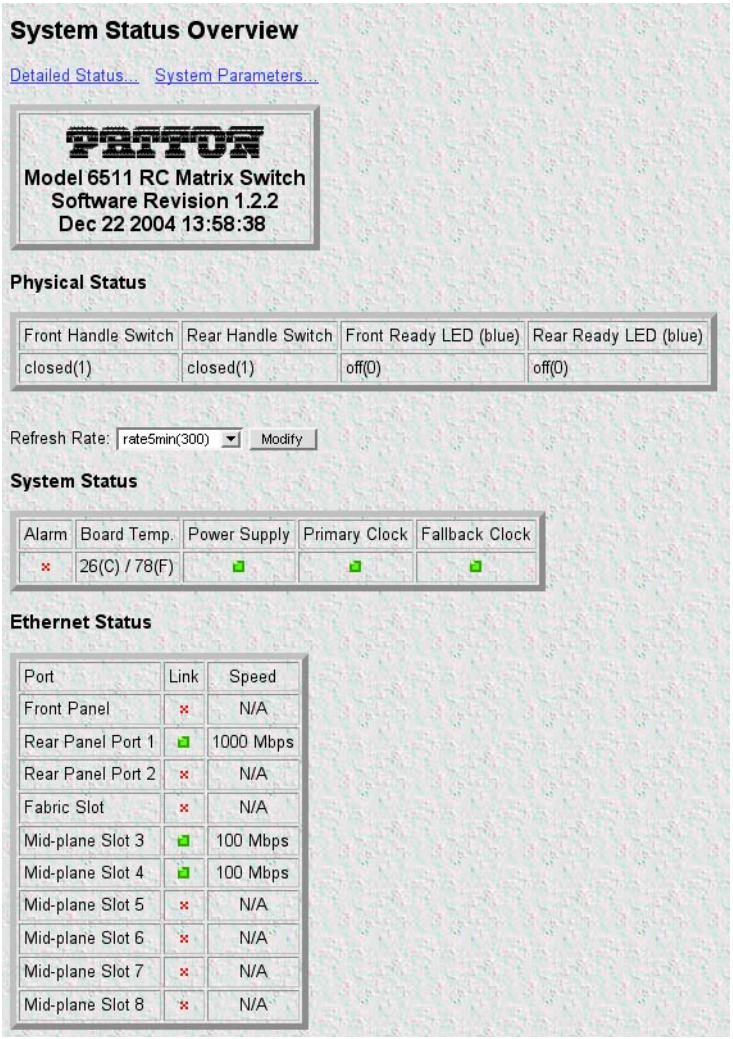


Figure 44. System Status Overview window

The *System Status Overview* page provides links to the *System Status Details, System Message Block Statistics, System Parameters*, and *System Parameters Configuration* subpages (see figure 45) where you can view more detailed status information..

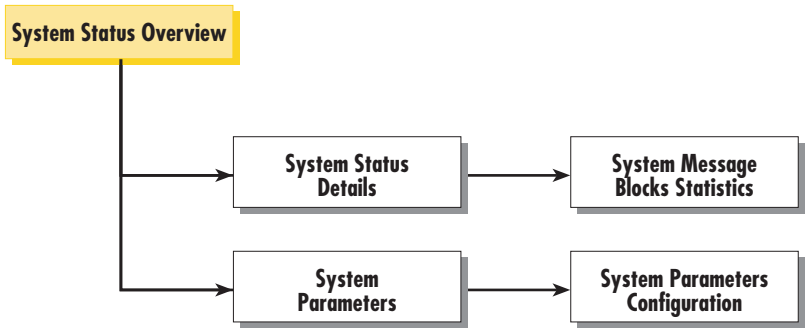


Figure 45. System Status Overview page and related subpages

System Status Overview window

The information the *System Status Overview* window displays is organized into four sections as described below:

- **General product information box**—Displays the product name, software release identifier, and software release timestamp (see figure 44 on page 95).
- **Physical status table**—Displays current state of certain physical components of the Matrix Switch, including the front handle switch, rear handle switch, front *READY* LED (blue), and rear *READY* LED (blue).
- **Refresh rate parameter**—Determines how often the Matrix Switch will refresh the information that the *System Status Overview* window displays.
- **System Status table**—Displays the state of alarms, the internal temperature of the Matrix Switch—displayed in Celsius (C)/Fahrenheit (F), the current operating status of the two power supplies and the pro-mary and fallback clock signals that the Matrix Switch uses.
- **Ethernet Status table**—Displays the link status and speed for each of the Matrix Switch's three Ethernet ports, as well as the status of all Ethernet links to modules residing in other slots within the same chassis where the 6511 is installed.

Hyperlinks

As shown in figure 45, the *System Status Overview* window also provides hyperlinks to the four subordinate windows within the System Status subsytem. The subordinate windows include the *System Status Details* window (see section "System Status Details window" on page 101), *System Message Block* Statistics window (see section "System Message Block Statistics window" on page 103), *System Parameters* window (see section "System Parameters window" on page 104) and the *System Parameters Configuration* window (see section "System Parameters Configuration window" on page 107).

Figure 46. General product information box

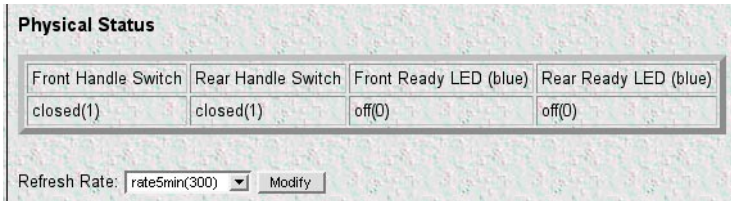


Figure 47. Physical status table and Refresh Rate menu

Physical status table

The *Physical Status* section of the *System Status Overview* window (see figure 47) lists the possible conditions of the Matrix Switch components (see table 4).

Table 4. 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 Matrix Switch's front panel will light, indicating that the Matrix Switch front blade is ready for removal. The Matrix Switch can then be removed from the CPCI chassis.
	Closed	Both front handle switches are closed, indicating that the handles are locked and the Matrix Switch 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 Matrix Switch'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 Matrix Switch's front panel is lit, indicating the switches on both front handles are open and the handles are unlocked, so the Matrix Switch is ready to be removed from the CPCI chassis.
	Off	The blue READY LED status indicator on the Matrix Switch'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 Matrix Switch is ***not*** ready for removal, and therefore ***cannot*** be removed from the CPCI chassis.

Table 4. Physical states (Continued)

Item	Setting	Description
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 47 on page 97) selects how often the 6511 will refresh the statistics display on the various *web management* windows.

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 **Modify** after selecting the desired refresh rate.

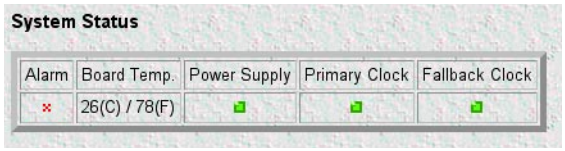


Figure 48. System Status table

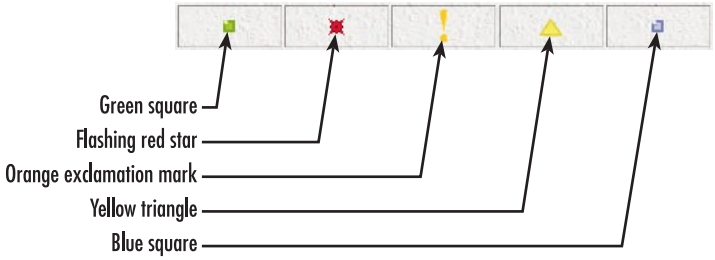


Figure 49. Alarm symbols

System Status table

The *System Status* table (see figure 48) displays the following parameters:

- **Alarm**—A flashing red star (see figure 49) 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 chapte table 5 on page 99.

- **Board Temp.**—Displays the internal temperature in Celsius (C)/Fahrenheit (F).
- **Power supply.** A flashing red star (see figure 49) indicates there is an alarm condition in the power supply. A green square denotes that the power supply is functioning properly.
- **Primary clock.** A flashing red star (see figure 49) indicates there is an alarm condition in the primary clock. A green square denotes that the primary clock is functioning properly.
- **Fallback clock**. A flashing red star (see figure 49) indicates there is an alarm condition in the fallback clock. A green square denotes that the fallback clock is functioning properly.

Table 5. System status/subsystem reference

Item	Recommended
Alarm	Chapter 4, "Alarms" on page 21
Board Temp.	Chapter 4, "Alarms" on page 21
Power Supply	Chapter 4, "Alarms" on page 21
Primary Clock	Chapter 4, "Alarms" on page 21 and chapter 6, "System Clocking" on page 41
Fallback Clock	

Ethernet Status table

The *Ethernet Status* table on the *System Status Overview* window (see figure 50) displays the speed and alarm/no-alarm condition for each of the Matrix Switch's three Ethernet ports as well as the 6511's Ethernet links to modules residing in other slots within the same chassis..

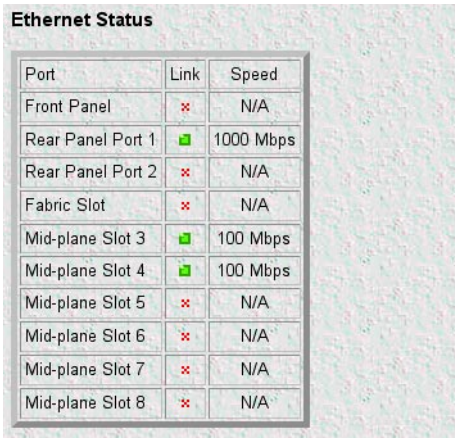


Figure 50. Ethernet status

The three Ethernet ports include one front panel Ethernet port and 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 49 on page 98) 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 51. System Status Details window

System Status Details window

- The *System Status Details* window (see figure 51) displays the following information:
- CPU Statistics
- Manufacture Information
- Message Block Statistics (includes a Detailed Message Block Statistics hyperlink to the System Message Block Statistics window)
- Operating System Heap Memory Statistics
- Enclosure System Temperature

To display the *System Status Details* window, on the *System Status Overview* window, click the *Detailed Status* hyperlink.

CPU Statistics

This portion of the *System Status Details* window, shown in figure 51, contains information described in the following sections.

Percentage CPU Idle (boxIdletime)

This indicates what percentage of the 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.

Manufacturer Information

This portion of the *System Status Details* window, shown in figure 51 on page 100, contains manufacturing information described in the following sections.

Serial Number (boxManufactureDatecode)

The serial number.

PCB Revision (boxManufacturePcbRevision)

The revision of the printed circuit board.

General Information (boxManufactureGeneralInfo)

Notes from Patton manufacturing, if any.

Message Block Statistics

This portion of the *System Status Details* window, shown in figure 51 on page 100, 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.

Note Click on the *Detailed Message Blocks Statistics…* hyperlink to display the System Message Blocks Statistics window and view the statistics (see section "System Message Blocks Statistics window" on page 127 for more information).

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.

Operating System Heap Memory Statistics

This portion of the *System Status Details* window, shown in figure 51 on page 100, 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.

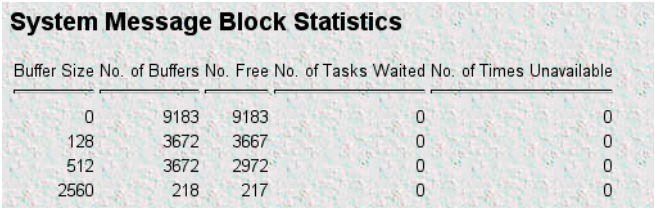
Largest (boxHeapLargestSpace)
The largest contiguous memory block in octets in the memory heap.

Enclosure System Temperature

This portion of the *System Status Details* window, shown in figure 51 on page 100, contains information about the internal temperature of the Matrix Switch.

Internal Temperature (boxTemperature)
Displays the current temperature in Celsius (centigrade).

Highest Temperature (boxMaxTemperature)
The highest temperature registered in Celsius (centigrade) since the Matrix Switch was last re-booted.



System Message Block Statistics

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 52. System Message Block Statistics window

System Message Block Statistics window

The 6511RC Matrix Switch system manages the i960 processor utilization by allocating message blocks for packet management. The *System Message Block Statistics* window (see figure 52) displays statistics about the Matrix Switch's buffer usage for messages according to the size of the message block size required. To display the *System Message Block Statistics* window, at the *System Status Details* window, click the *Detailed Message Block Statistics...* hyperlink

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.

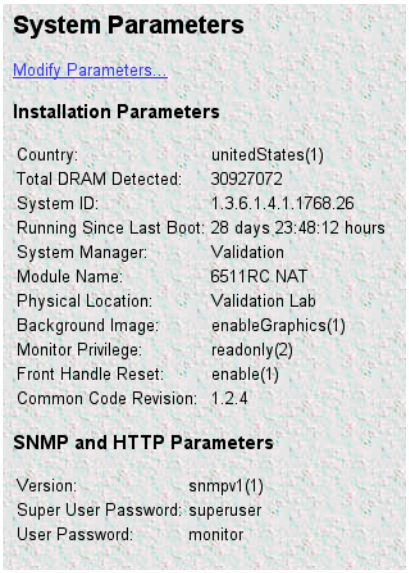


Figure 53. System Parameters window

System Parameters window

The System Parameters window (see figure 53) displays in read-only format the configurable system parameters that govern Matrix Switch operation. The window displays the parameters in two tables:

- *Installation Parameters* table
- *SNMP and HTTP Parameters* table

The System Paramters window also displays the *Modify Parameters…* hyperlink, which opens the *System Parameters Configuration window.* You can use the *System Parameters Configuration window to* modify configurable installation, SNMP, and HTTP parameters.

To display the *System Status Parameters* window, on the *System Status Overview* window, click the *System Parameters* hyperlink.

Installation Parameters

This portion of the *System Parameters* window, shown in figure 53 on page 104, displays the following parameters:

Country (installCountry)

Specifies the country that the Matrix Switch is installed in so it can be configured in accordance with local laws.

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 Matrix Switch 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.

Module 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 Matrix Switch.

Front Handle Reset (TBD)
This parameter determines how the 6511 will behave when you unlock the topmost front handle.

- **enable(1)**—When someone opens (unlocks) the top front handle the Model 6511 module will reboot as follows:
  - When the switch is opened, the blue LED begins flashing ON/OFF every 2 seconds.
  - After 13 seconds, the unit will reboot.

    Note Opening the front handle triggers the reboot process described above. Once you open the handle, you should immediately close it again before the module actual reset occurs.

- **disable(0)**—The 6511 will NOT restart when someone unlocks the topmost front handle.

SNMP and HTTP Parameters

This portion of the *System Parameters* window, shown in figure 53 on page 104, provides the following 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 parameter defines the password that provides superuser access via SNMP and HTTP to the Matrix Switch web management interface. Logging on as Superuser gives you read access to all management information and modify access to all Matrix Switch configurable parameters. The password may not exceed 64 octets (characters).

User Password (boxSnmpMonitorPassword)

This parameter defines the password that provides monitor access to the Matrix Switch web management interface. Logging on with monitor access gives you read-only access to a limited selection of management information. Certain parameters displayed for superuser access are hidden to user (monitor) access.

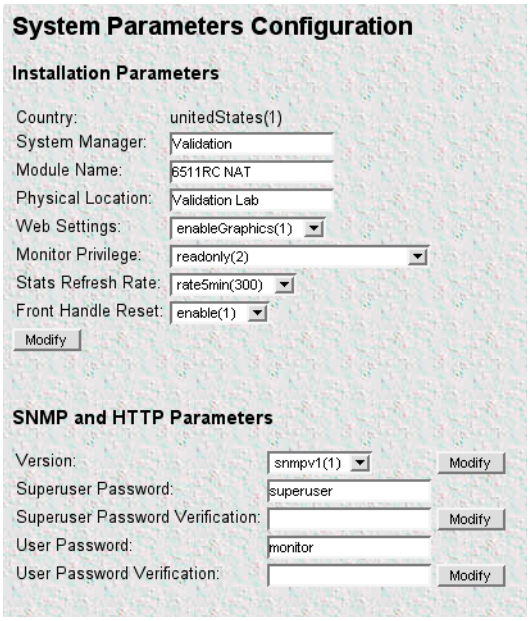


Figure 54. System Parameters Configuration window

System Parameters Configuration window

The *System Parameters Configuration* window (see figure 54) provides the means for you to modify the values for Matrix Switch System configurable parameters in the SNMP and HTTP, and Installation tables. To display the System (configurable parameters) window, on the System Parameters window, click the *Modify Parameters…* link (see figure 53 on page 104).

The following sections describe the configurable parameters displayed on the *System Parameters Configuration* window.

Installation Parameters

The Installation Parameters table displays the configurable parameters described in the following section:

Country (installCountry)

Specifies the country that the Matrix Switch 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)

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.

Module 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.
- writeUserlp(50)—The monitor user can change all parameters—except passwords— under authentication, drop-and-insert, dial-in, and IP links.
- writeUserlpWan(114)—The monitor user can change all parameters—except passwords— under authentication, drop-and-insert, dial-in, IP, T1/E1, and Frame Relay links.
- writeUserlpWanSystem(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.
- writeUserlpWanSystemUpload(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.

Stats Refresh Rate (TBD)

This parameter (see figure 47 on page 97) selects how often the 6511 will refresh the statistics display on the various *web management* windows.

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 **Modify** after selecting the desired refresh rate.

Front Handle Reset (TBD)

This parameter determines how the 6511 will behave when you unlock the topmost front handle.

- **enable(1)**—The 6511 will automatically restart when someone unlocks the topmost front handle.
- **diable(0)**—The 6511 will **NOT** restart when someone unlocks the topmost front handle.

SNMP and HTTP

The SNMP and HTTP parameters table (figure 54 on page 107) displays the selectable SNMP version, together with the configurable usernames and passwords that govern operator read-only and modify access to the Matrix switch web management interface via HTTP.

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 parameter defines the password that provides superuser access via SNMP and HTTP to the Matrix Switch web management interface. Logging on as Superuser gives you read access to all management information and modify access to all Matrix Switch configurable parameters. The password may not exceed 64 octets (characters).

Superuser Password Verification (boxSnmpVerifyMasterPassword)

Re-enter the superuser password to verify it was entered correctly. The contents of both fields must match for the Matrix Switch to accept your changes.

User Password (boxSnmpMonitorPassword)
This parameter defines the password that provides monitor access to the Matrix Switch web management interface. Logging on with monitor access gives you read-only access to a limited selection of management information. Certain parameters displayed for superuser access are hidden to user (monitor) access.

User Password Verification (boxSnmpVerifyMonitorPassword)
Re-enter the user (monitor) password to verify it was entered correctly. The contents of both fields must match for the Matrix Switch to accept your changes.

Chapter 13 System Log

Chapter contents

Introduction

The 6511RC software provides a system log utility. The system log subsystem generates an event message for certain errors and significant occurrences within the 6511RC system. The 6511RC 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 6511RC where to send system log messages based on the priority of the message. The 6511RC can send system log messages to the following destinations:

- Flash memory—The 6511RC's Non-volatile Read-only Memory (NVRAM)
- RAM—The 6511RC's Random Access Memory (RAM)
- Config port—The 6511RC's RS-232 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 6511RC's System Log parameters.

SYSTEM LOG main window

The *SYSTEM LOG* main window (see figure 55) provides the means for you to manage the 6511RC's system log subsystem. To display the *SYSTEM LOG* main window, on the 6511RC's *Configuration Menu* pane, click the *System Log* link.

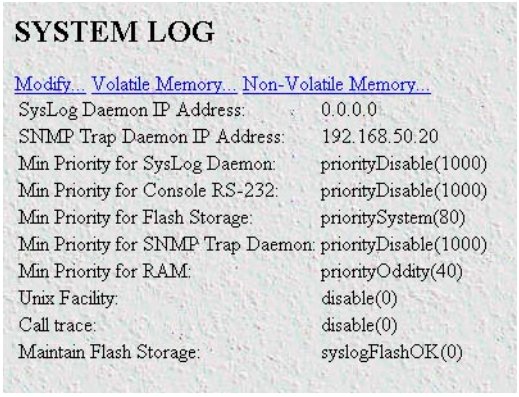


Figure 55. SYSTEM LOG main window

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 56.

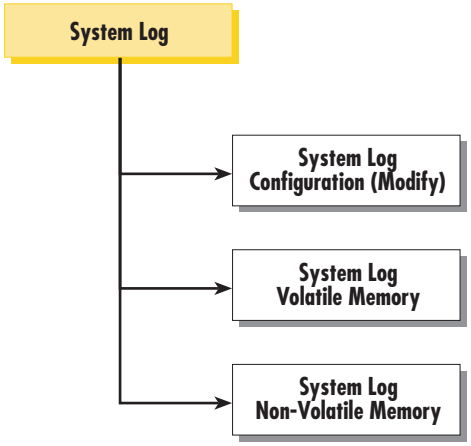


Figure 56. System Log windows map

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 6511RC currently stores in
  - Volatile memory
  - Non-volatile memory

The following sections describe the contents of the *SYSTEM LOG* main window.

Figure 57. Hyperlinks section of the SYSTEM LOG main window

Hyperlinks

The *SYSTEM LOG* main window displays the following hyperlinks (see figure 57):

- 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 117
- 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 6511RC'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 120
- 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 6511RC

NVRAM. The System Log (Non-Volatile Memory window is described later in this chapter "System Log—Non-Volatile Memory window" on page 120

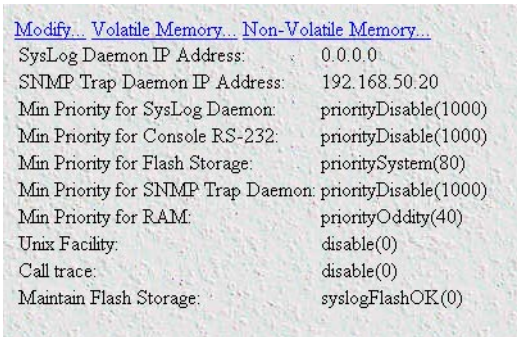


Figure 58. Parameters section of the System Log main window

System Log parameters

The following sections describe the System Log parameters (see figure 58).

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 117).

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 6511RC. 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.

SYSTEM LOG (configuration) window

The System Log (configuration) window (see figure 59) 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.

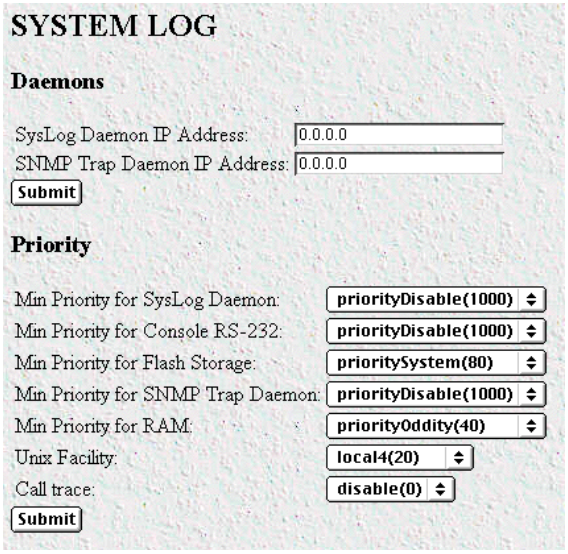


Figure 59. System Log—Modify window

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 117).

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 6511RC. 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.

System Log—Volatile Memory window

The System Log—Volatile Memory window (see figure 60) displays the time-stamped system log messages currently stored in the 6511RC's volatile memory. To display the System Log (Volatile Memory) window, on the System Log main window, click the Volatile Memory… hyperlink.

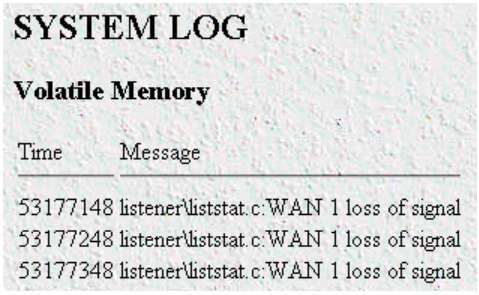


Figure 60. System Log—Volatile Memory window

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 6511RC 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 61) displays the time-stamped system log messages currently stored in the 6511RC'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.

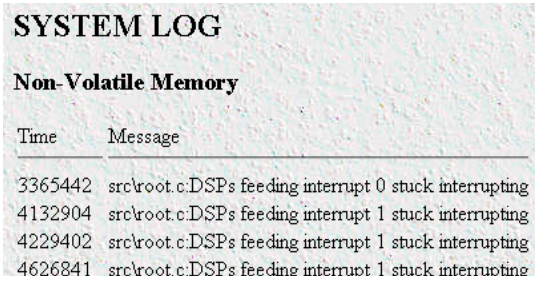


Figure 61. System Log—Non-Volatile Memory window

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 6511RC loses power, the messages stored in non-volatile flash memory will ***not*** be lost.

Chapter 14 E1 Link

Chapter contents

Introduction

The *E1 Link* window (see figure 62) provides the means for you to configure, test, and manage individual or group of E1s in the STM Matrix Switch. The *E1 Link* provides quick access to a single or groups of E1s in any TUG3/TUG2 or TU12 groups.

To display the *E1 Link* window on the 6511RC's *Configuration Menu* pane, click the *E1 Link* hyperlink.

Figure 62. E1 Link—E1selection window

From the *E1 Link* page, select the group (TUG3 and TUG2) containing the E1 or E1s of interest. Once you have selected a TUG2 and TUG3 group, click the **Submit Query** button to view the E1 configuration and information page (see figure 63).

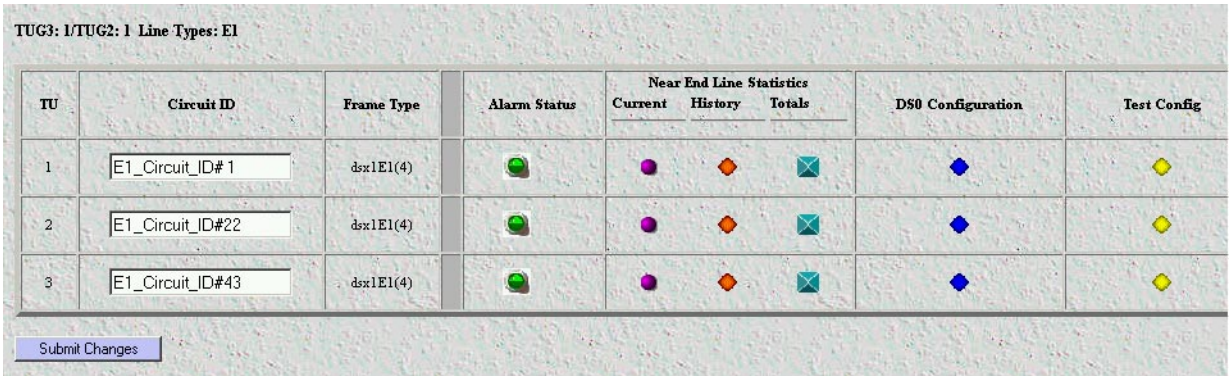


Figure 63. E1 Link page

The E1 screen offers configuration and status fields for *Circuit ID, Frame Type, Alarm Status, Near End Line Statistics, DS0 Configuration*, and *Test Configuration*.

- **Circuit ID**—Text label identifying the E1 circuit
- **Frame Type**—Fixed for dsx1 (Framed E1) format
- **Alarm Status**—Display-only field with detailed information of current E1 link alarms
- **Near End Line Statistics**—Displays E1 link statistics for current, history, and totals

Near End Line Statistics—Current

Click on *Near End Line Statistics—Current* (see figure 63 on page 125) (purple circle) to display line statistics for the current 15-minute interval (see figure 64).

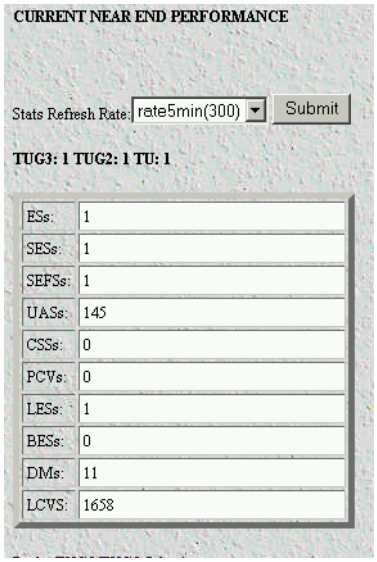


Figure 64. Current Near End Performance window

ESs (errored seconds) (dsx1CurrentESs)

The number of errored seconds, encountered by a DS1 interface in the current 15-minute interval.

SES (severely errored seconds) (dsx1CurrentSESs)

The number of severely errored seconds encountered by a DS1 interface in the current 15-minute interval.

SEFS (severely errored frame seconds) (dsx1CurrentSEFSs)

The number of severely errored framing seconds encountered by a DS1 interface in the current 15-minute interval.

UASs (unavailable seconds) (dsx1CurrentUASs)

The number of unavailable seconds encountered by a DS1 interface in the current 15-minute interval.

CSSs (controlled slip seconds) (dsx1CurrentCSSs)

The number of Controlled Slip Seconds encountered by a DS1 interface in the current 15-minute interval.

PCVs (path code violations) (dsx1CurrentPCVs)

The number of path coding violations encountered by a DS1 interface in the current 15-minute interval.

LESs (line errored seconds) (dsx1CurrentLESs)

The number of line errored seconds encountered by a DS1 interface in the current 15-minute interval.

BESs (bursty errored seconds) (dsx1CurrentBESs)

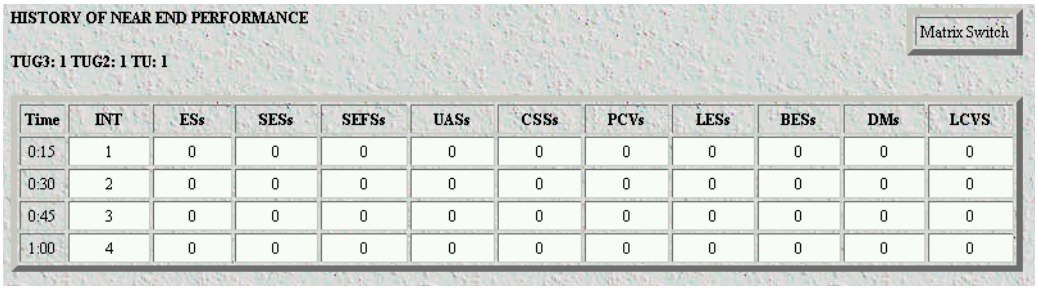
The number of bursty errored seconds (BESs) encountered by a DS1 interface in the current 15-minute interval.

DMs (degraded minutes) (dsx1CurrentDMs)
The number of degraded minutes (DMs) encountered by a DS1 interface in the current 15-minute interval.

LCVs (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* (see figure 63 on page 125) (orange diamond) to display line statistics for prior completed 15-minute intervals within the last 24 hours (see figure 65). This does not include the current 15-minute interval.


HISTORY OF NEAR END PERFORMANCE

Matrix Switch

TUG3: 1 TUG2: 1 TU: 1

Time	INT	ESs	SESs	SEFSs	UASs	CSSs	PCVs	LESs	BESs	DMs	LCVS
0:15	1	0	0	0	0	0	0	0	0	0	0
0:30	2	0	0	0	0	0	0	0	0	0	0
0:45	3	0	0	0	0	0	0	0	0	0	0
1:00	4	0	0	0	0	0	0	0	0	0	0

Figure 65. History of Near End Performance window

INT (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 6511RC 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 6511RC was powered up.

ESs (errored seconds) (dsx1intervaless)
The number of errored seconds encountered by a DS1 interface in one of the previous 96, 15-minute intervals.

SESs (severely errored seconds) (dsx1IntervalSESs)
The number of severely errored seconds encountered by a DS1 interface in one of the previous 96, 15-minute intervals.

SEFSs (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.

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

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

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

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

BESs (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.

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

LCVs (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* (see figure 63 on page 125) (teal square) to display the total statistics of errors that occurred during the previous 24-hour period, the previous 96, 15-minute intervals (see figure 66).

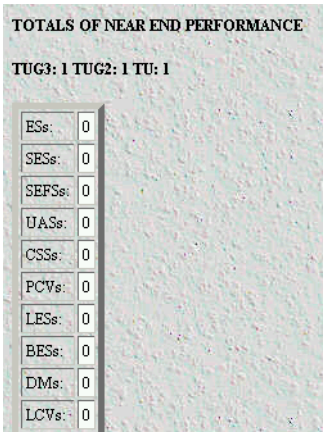


Figure 66. Totals of Near End Performance window

ESs (errored seconds) (dsx1TotalESs)
The number of errored seconds encountered by a DS1 interface in the previous 24-hour interval.

SESs (severely errored seconds) (dsx1TotalSESs)
The number of severely errored seconds encountered by a DS1 interface in the previous 24-hour interval.

SEFSs (severely errored frame seconds) (dsx1TotalSEFSs)
The number of severely errored framing seconds encountered by a DS1 interface in the previous 24-hour interval.

UASs (unavailable seconds) (dsx1TotalUASs)
The number of unavailable seconds encountered by a DS1 interface in the previous 24-hour interval.

CSSs (controlled slip seconds) (dsx1TotalCSSs)
The number of controlled slip seconds encountered by a DS1 interface in the previous 24-hour interval.

PCVs (path code violations) (dsx1TotalPCVs)
The number of path coding violations encountered by a DS1 interface in the previous 24-hour interval.

LESs (line errored seconds) (dsx1TotalLESs)
The number of line errored seconds encountered by a DS1 interface in the previous 24-hour interval.

BESs (bursty errored seconds) (dsx1TotalBESs)
The number of bursty errored seconds (BESs) encountered by a DS1 interface in the previous 24-hour interval.

DMs (degraded minutes) (dsx1TotalDMs)
The number of degraded minutes (DMs) encountered by a DS1 interface in the previous 24-hour interval.

LCVs (line code violations) (dsx1TotalLCVs)
The number of line code violations (LCVs) encountered by a DS1 interface in the previous 24-hour interval.

DS0 idle code configuration
Click on the DS0 configuration icon (see figure 63 on page 125) (blue diamond) corresponding to the E1 under configuration. The selected DS0s will carry standard idle code (7E Hex).

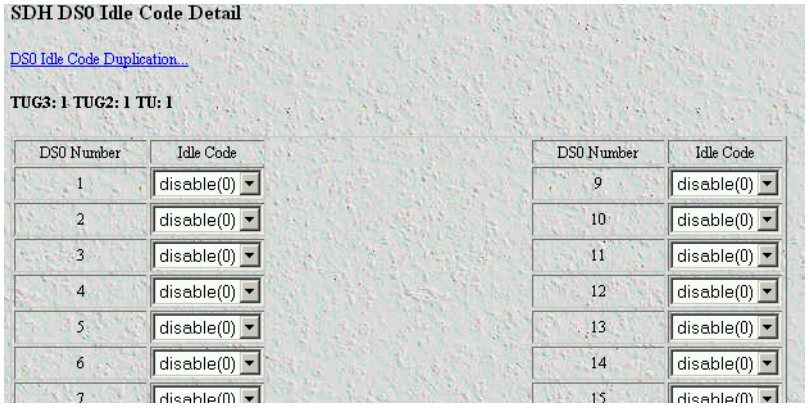


Figure 67. Idle Code Detail page

Idle code (7E H) is entered by selecting *enabled* for DS0s not carrying user data. Once all DS0s have been configured, use the *Modify* button to activate the configuration.

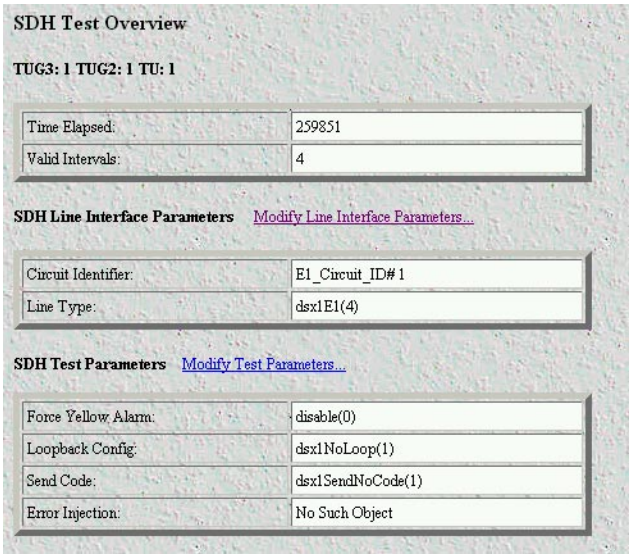


Figure 68. SDH Test Overview

Test Configuration—Allows access to E1 *SDH Test Overview* page (see figure 68) that displays the following:

- ***E1 Circuit Statistics***—displays time elapsed and valid intervals information.
- ***Line Interface Options***:—Displays E1 circuit ID, and E1 line format information.

SDH/E1 test parameters

To access the SDH/E1 Test Details page, click on the *Modify Test Parameters* link.

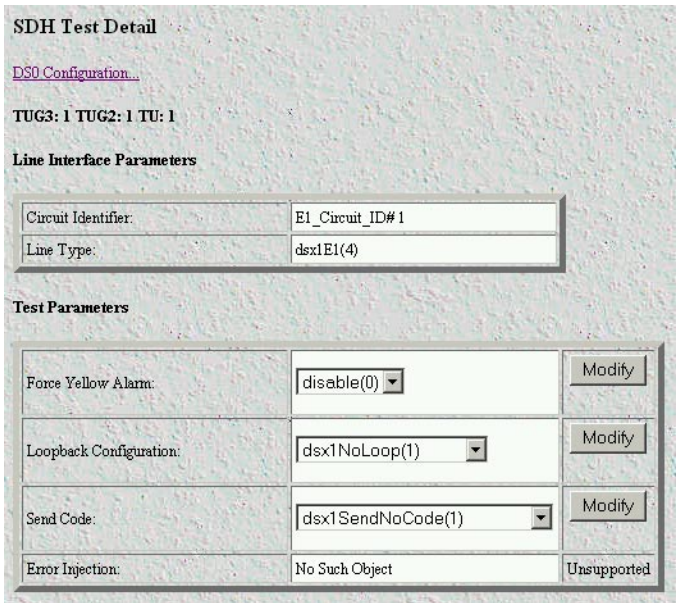


Figure 69. SDH Test Detail

Line Interface Parameters

This portion of the Test Details page displays *Circuit Identifier* and *Line Type* information

Test Parameters

This portion of the Test Details page contains *Test Parameters* options described in the following sections.

Force Yellow Alarm (linkYellowForce)

This variable identifies which standard will be used to transmit and identify the yellow alarm.

- enable(1)—Force the transmission of a yellow alarm even if the received signal is in frame.
- disable(0)—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 its 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
- dsx1SendQRSSCode(5)—Sending QRSS test pattern
- dsx1Send511Code(6)—Sending 511 test pattern
- dsx1Send3in24Code(7)—Sending 3 in 24 test pattern
- dsx1SendOtherTestPattern(8)—Not defined

Chapter 15 SDH

Chapter contents

Introduction

The *SDH Overview* page provides the means for you to manage the configuration, alarm status, and to view near-end and far-end statistics for the model 6511RC. The *SDH Overview* page—which provides at-a-glance visual display of the alarm status—contains the following items:

- *Link to SDH configuration page.*
- *Alarm Status for SDH Section, Line, and Path.*
- *SDH statistics for Near and Far end.*
  - Near End section, line, and path statistics
  - Far End line and path

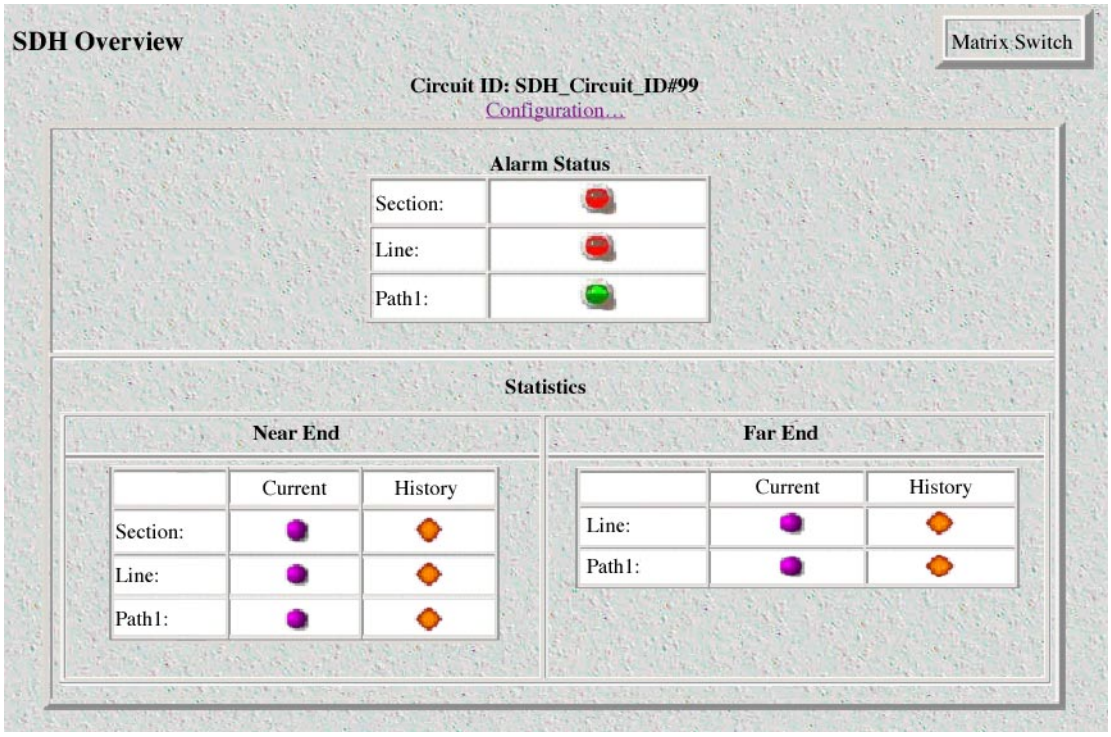


Figure 70. SDH Overview window

Alarm Status

The Alarm Status section allows at-a-glance indication of the condition of *Section, Line,* and *Path* (where a green symbol indicates normal status and a red symbol indicates that there is an alarm condition). If an alarm condition exists, the red icon becomes a hyperlink that the user can click to get information about the alarm. When the SDH mapping is set to AU-4, the window will display the condition for Path1 only, when the SDH mapping is set to AU-3, this window will display condition of Path1, Path2, and Path3.

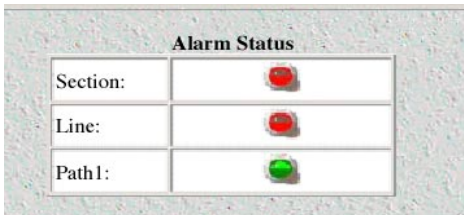


Figure 71. SDH Overview window—Alarm Status section

Sections, Lines, and Paths. Between a pair of SDH multiplexers, an SDH circuit may comprise multiple cable segments connected by intermediate devices such as signal repeaters and add-drop multiplexers (See figure 61). A cable segment with a regenerator at one or both endpoints is called a Section. A set of cable segments with an add-drop multiplexer at one or both endpoints is called a Line.An SDH circuit with full-service multiplexers at both endpoints is called a Path.

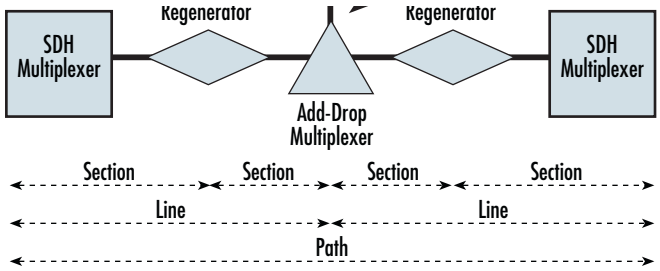


Figure 72. Section, path, and line within an SDH circuit

Section alarm

If an alarm is present in the SDH section, the indicator will change from green to red. Clicking on the icon will take the user to the *SDH Section STATUS ALARMS* page (see figure 73). A section alarm is activated if LOS (loss of signal), LOF (loss of framing), or both are detected by the SDH interface.

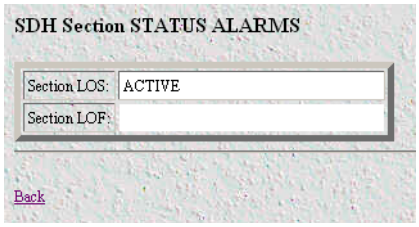


Figure 73. SDH Section STATUS ALARMS window

Section LOS

The LOS alarm is activated when no transitions are detected on the incoming signal (before descrambling). The LOS condition is detected upon observing 2.3 to 100 microseconds of no transitions. The LOS alarm is cleared after a 125 microsecond interval (one frame) during which no LOS defect is detected.

Section LOF

A section LOF failure is declared when the LOF defect persists for a period of 2.5 seconds, except when an LOS defect or failure is present. The LOF failure is cleared when the LOS failure is declared, or when the LOF defect is absent for 10 seconds. To display SDH Configuration and status page on the 6511RC s Configuration Menu pane, click the SDH Link hyperlink.

Line status alarm

When an alarm is present in the SDH Line, the icon will change from green to red. Clicking on the icon takes the user to the *SDH Line STATUS ALARMS* page (see figure 74). A Line alarm is activated upon detection of a *Line AIS* (alarm indication signal), *Line RDI* (remote defect indication), or a *Section Trace Mismatch*.

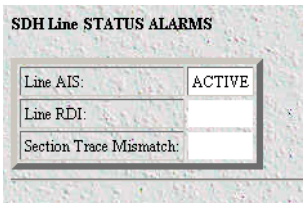


Figure 74. SDH Line STATUS ALARMS window

Line AIS

Line AIS defect is detected as a "111" pattern in bits 6, 7, and 8 of the K2 byte in five consecutive frames. Line AIS defect is terminated when bits 6, 7, and 8 of the K2 byte do not contain the code "111" for five consecutive frames. A Line AIS failure is declared when the Line AIS defect persists for a period of 20.5 seconds. A Line AIS failure is cleared when the Line AIS defect is absent for 10 seconds.

Line RDI

Line RDI defect is a "110" code in bits 6, 7, and 8 of the K2 byte of in STS-1 #1 in five consecutive frames. Line RDI defect is terminated when any code other than "110" is detected in bits 6, 7, and 8 of the K2 byte in five consecutive frames. A alarm is declared when the incoming Line RDI defects lasts for 2.5 seconds. The alarm failure is cleared when no Line RDI defects are detected for 10 seconds.

Section Trace Mismatch

The Section Trace Mismatch alarm is activated when the section trace message received does not match the configured message.

Path status alarm

When a Path alarm is present in the SDH Line, the icon will change from green to red. Clicking on the icon takes the user to the *SDH Path STATUS ALARMS* page. A Path alarm is activated upon detection of *Path LOP, Path AIS, Path RDI, Path Unequipped, Path Signal Label Mismatch,* or *Path Trace Mismatch,* in addition, it displays the *Received Path Signal Label* and the *Received Path Trap*.

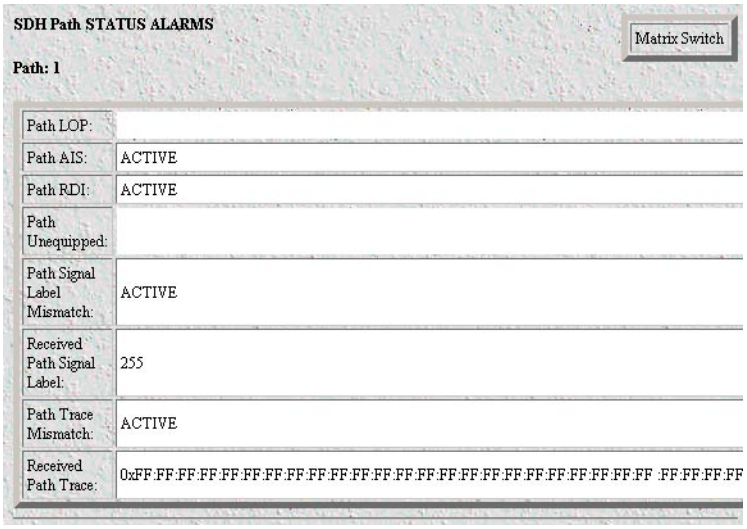


Figure 75. SDH Path STATUS ALARMS window

Path LOP

A Loss of Pointer (LOP) is declared when either a valid pointer is not detected in eight consecutive frames, or when eight consecutive frames are detected with the New Data Flag (NDF) set to *1001* without a valid concatenation indicator. LOP state is cleared when either a valid pointer with a normal NDF set to *0110*, or a valid concatenator indicator is detected for three contiguous frames.

Path AIS

Path AIS is defined as all-ones in the TU or AU pointers. SOH is not affected. Path AIS is generated to replace the normal traffic signal when it contains a defect condition in order to prevent cascaded downstream failures being declared or alarms being raised.

Path RDI

Path RDI formerly called path-FERF (Far End Remote Fail). This signal is returned to the transmitting TE when the far end detects a Loss of Signal, Loss of Frame, AIS, Trace Identifier Mismatch, or Path Unequipped.

Path Unequipped

The *Path Unequipped* alarm is initiated when the path signal label byte C2 is set to all zeroes for at least five consecutive frames.

Path Signal Label Mismatch

A Path or VT connection is not correctly provisioned if a received Path or VT Signal Label mismatch occurs. A received Signal Label is considered mismatched if it does not equal either the locally provisioned value or the value 'equipped non-specific' (1 hex).

Note Any received non-zero Signal Label is considered a locally provisioned value of 'equipped non-specific'. Only in-service, provisioned Path Terminating equipment can detect mismatched Signal labels. It is considered provisioned if it has been configured for a mapping and has been assigned signals to and from which the mapping takes place.

Received Path Signal Label

Displays the received path signal label.

Path Trace Mismatch

Activated upon detection of mismatch in the path trace.

Received Path Trace

Displays received path trace message string (in Hex format).

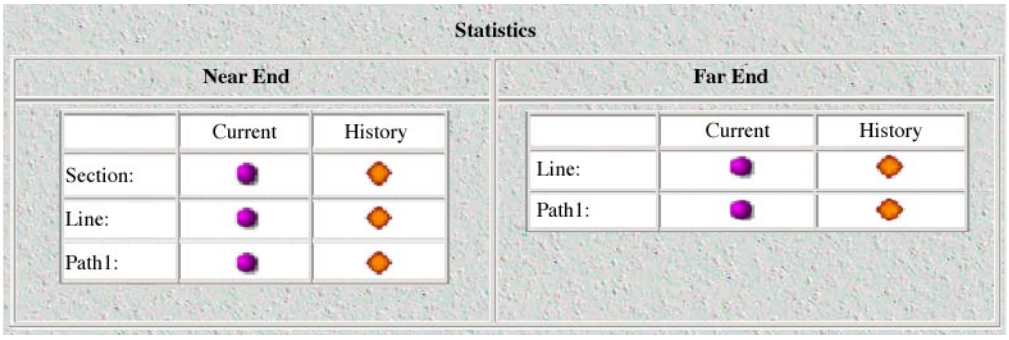


Figure 76. SDH Near and Far end Statistics section

Statistics

The statistics windows shows current and historical statistics for near and far end interfaces (see figure 76).

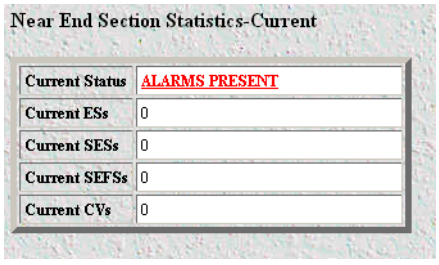


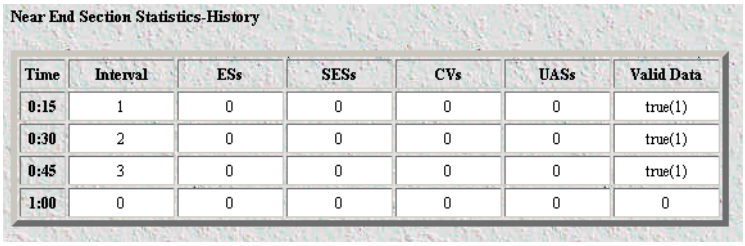
Figure 77. Near End Section Statistics—Current

Near End statistics

The Near End statistics window include current and historical data for the local STM-1 interface. Click on an icon (purple circle for *Current*, orange diamond for *History*) to get detailed information.

Near End Section Statistics—Current

The *Near End Section Statistics—Current* window (see figure 77) displays five fields corresponding to *Current Status*, *Current ESs* (errored seconds), *Current SESs* (severe errored seconds), *Current SEFSs* (severe errored frame seconds), and *Current CVs* (code violation—line code).



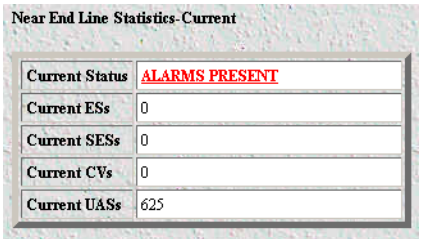
Near End Section Statistics-History

Time	Interval	ESs	SESs	CVs	UASs	Valid Data
0:15	1	0	0	0	0	true(1)
0:30	2	0	0	0	0	true(1)
0:45	3	0	0	0	0	true(1)
1:00	0	0	0	0	0	0

Figure 78. Near End Section Statistics—History

Near End Section Statistics—History

The *Near End Section Statistics—History* window (see figure 78) displays historical information on the condition of the local STM-1 interface. Statistics are presented in fifteen minute intervals, and present data for *ESs* (errored seconds), *SESs* (severe errored seconds), *CVs* (code violations), *UASs* (unavailable seconds), and *Valid Data*.



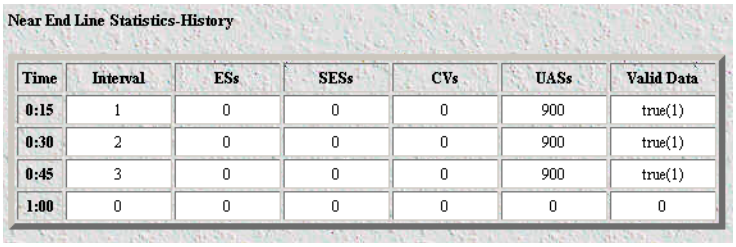
Near End Line Statistics-Current

Current Status	ALARMS PRESENT
Current ESs	0
Current SESs	0
Current CVs	0
Current UASs	625

Figure 79. Near End Line Statistics—Current

Near End Line Statistics—Current

This window presents current status and statistics information about the local STM-1 interface. Information fields include: *Current Status*, *Current ESs* (Errored Seconds), *Current SESs* (severe errored seconds), *Current CVs* (code violations), and *Current UASs* (unavailable seconds).



Near End Line Statistics-History

Time	Interval	ESs	SESs	CVs	UASs	Valid Data
0:15	1	0	0	0	900	true(1)
0:30	2	0	0	0	900	true(1)
0:45	3	0	0	0	900	true(1)
1:00	0	0	0	0	0	0

Figure 80. Near End Line Statistics—History

Near End Line Statistics—History

The *Near End Line Statistics—History* window displays historical information on the condition of the local STM-1 interface. Statistics are presented in fifteen minute intervals, and present data for *ESs* (errored seconds), *SESs* (severe errored seconds), *CVs* (code violations), *UASs* (unavailable seconds), and *Valid Data*.

Near End Path1 Statistics—Current

The *Near End Path Statistics—Current* displays path statistics for the 6511RC. The information fields include *Current Width*, *Current Status*, *Current ESs* (errored seconds), *Current SESs* (severe errored seconds), *Current CVs* (code violations), and *Current UASs* (unavailable seconds).

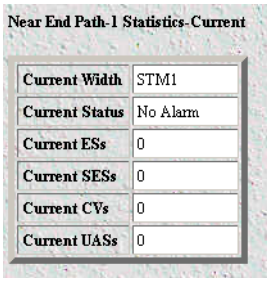


Figure 81. Near End Path-1 Statistics Current

Near End Path1 Statistics—History

The *Near End Path Statistics—History* window displays historical information on the condition of the local STM-1 interface. Statistics are presented in fifteen minute intervals, and display data for *ESs* (errored seconds), *SESs* (severe errored seconds), *CVs* (code violations), *UASs* (unavailable seconds), and *Valid Data*.

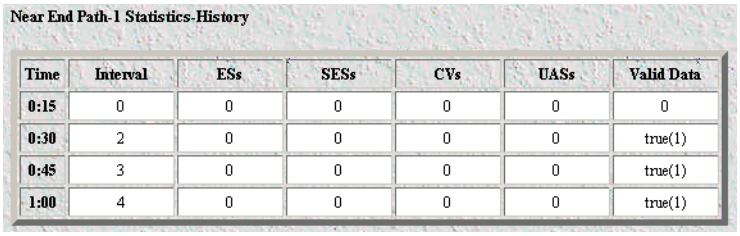


Figure 82. Near End Path 1 Statistics—History

Far End statistics

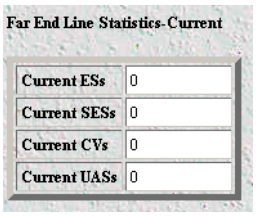


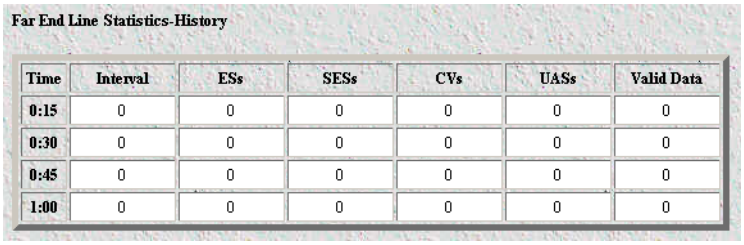
Figure 83. Far end Line Statistics—Current

Far End Line Statistics—Current

This window presents current status and statistics information about the local STM-1 interface. Information fields include: *Current Status*, *Current ESs* (errored seconds), *Current SESs* (severe errored seconds), *Current CVs* (code violations), and *Current UASs* (unavailable seconds).

Far End Line Statistics—History

The *Far End Line Statistics—History* window displays historical information on the condition of remote STM-1 interface. Statistics are presented in fifteen minute intervals, and present data for *ESs* (errored seconds), *SESs* (severe errored seconds), *CVs* (code violations), *UASs* (unavailable seconds), and *Valid Data*.

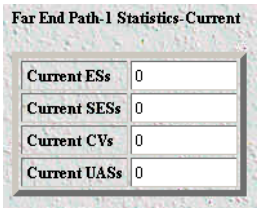

Far End Line Statistics-History

Time	Interval	ESs	SESs	CVs	UASs	Valid Data
0:15	0	0	0	0	0	0
0:30	0	0	0	0	0	0
0:45	0	0	0	0	0	0
1:00	0	0	0	0	0	0

Figure 84. Far End Line Statistics—History

Far End Path-1 Statistics—Current

The *Far End Path Statistics—Current* displays path statistics for the far end interface. The information fields include *Current ESs* (errored seconds), *Current SESs* (severed errored seconds), *Current CVs* (code violations), and *Current UASs* (unavailable seconds).

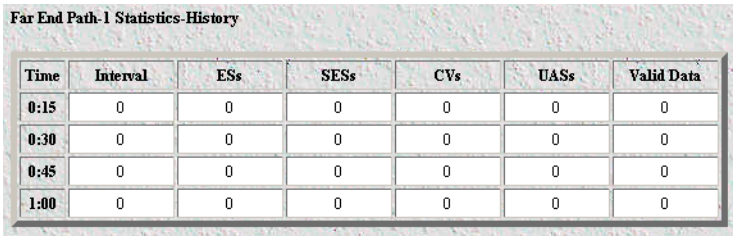

Far End Path-1 Statistics-Current

Current ESs	0
Current SESs	0
Current CVs	0
Current UASs	0

Figure 85. Far End Path-1 Statistics—Current

Far End Path-1 Statistics—History

The *Near End Path Statistics—History* window displays historical information on the condition of the far end STM-1 interface. Statistics are presented in fifteen minute intervals, and display data for *ESs* (errored seconds), *SESs* (severe errored seconds), *CVs* (code violations), *UASs* (unavailable seconds), and *Valid Data*.


Far End Path-1 Statistics-History

Time	Interval	ESs	SESs	CVs	UASs	Valid Data
0:15	0	0	0	0	0	0
0:30	0	0	0	0	0	0
0:45	0	0	0	0	0	0
1:00	0	0	0	0	0	0

Figure 86. Far End Path-1 Statistics—History

SDH Configuration link

Click on the *Configuration* link in the SDH window display the *Modify* window (see figure 87). The *Modify* window is divided into sections that display the following SDH parameters

- *SDH Physical Configuration*—Selects between an electrical or optical interface.
- *SDH Interface Configuration*—Configurable parameters for the STM-1 port.
- *Path Trace Configuration*—Configurable parameters for Path trace.
- *SDH Mapper*—configures E1 mapping for either Async or Bytesync payload timing.

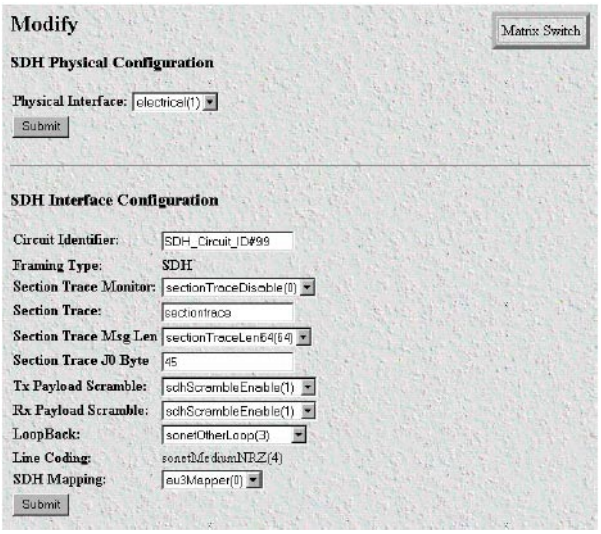


Figure 87. SDH Configuration page

Physical Interface

This variable indicates the type of physical interface the 6511RC will be using for the STM-1 link. The options are:

- optical(0)—The 6511RC will use the Single Mode SC optical interface.
- electrical(1)—The 6511RC will use the 75-Ohm dual BNC interface.

SDH Interface Configuration

SDH configuration page fields include:

Circuit Identifier

The *Circuit Identifier* provides a way for the user to define a free-text name (character string) that identifies the circuit (link) attached to the 6511RC. Although the table display is limited to 20 characters at a time, the 6511RC 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.

Framing Type

The framing type field is informational only, there are no options to configure. Framing type is set to SDH at the factory.

Section Trace Monitor

For Section Trace Message Monitor, the user provides a message and the SONET/SDH Receiver `will locate the message in the received bitstream`. Options for Section Trace Monitor are:

- sectionTraceDisable(0)—Disables Section Trace Monitor.
- sectionTraceEnable(1)—Enables Section trace Monitor.

Section Trace (`sdhSectionTrace`)

This is a character string with the maximum length based on the section trace msg len setting. This field is not used with 1 byte message length. If the length is set to 16, this field is 15 bytes maximum length. A 1 byte crc-7 check is appended to the string to make 16 bytes. If the length is set to 64, this field can hold 64 up to characters.

Section Trace Msg Len (`sdhSectionTraceLength`)

The Section Trace Message Length determines length of the trace message in bytes. There are three options:

- sectionTraceLen1(1)—Section Trace Message one byte length
- sectionTraceLenght16(16)—Section Trace Message is 16 bytes.
- sectionTraceLenght64(64)—Section Trace Message in groups of 64 bytes.

Section Trace J0 Byte(`sdhSectionTraceJ0Byte`)

If the message length is set to 1 byte, this field is used for the message. It holds a decimal value from 0-255. This field is ignored for 16 and 64 byte message lengths.

Tx Payload Scramble

The current Scramble state of the SONET/SDH interface, options are:

- sdhScrambleDisable(0)—Transmit payload is not scrambled
- sdhScrambleEnable(1)—Transmit payload is scrambled

Rx Payload Scramble

The current Scramble state of the receiver SONET/SDH interface, options are:

- sdhScrambleDisable(0)—Received payload is not descrambled.
- sdhScrambleEnable(1)—Received payload is descrambled.

LoopBack
The 6511RC WAN interface can initiate the following diagnostics loops:

- sonetNoLoop(0)—Not in the loopback state. The 6511RC WAN interface has not initiated or is not under a diagnostic loop.
- sonetFacilityLoop(1)—The received signal at this interface is looped back out through the transmitter section in the return direction.
- sonetTerminalLoop(2)—The signal that is about to be transmitted is connected to the associated incoming receiver.
- sonetOtherLoop(3)—Data arriving at the 6511RC H.110 interface is looped back to the originating device.

Line Coding
This is a fixed parameter. The 6511RC comes configured for NRZ (sonetMediumNRZ(4)).

SDH Mapping
The 6511RC Matrix Switch supports the two SDH mapping schemes ANSI and ETSI. ANSI mapping adds an AU pointer to the VC-3 to create an AU-3 (Administrative Unit 3). In ETSI Mapping, a pointer is added to VC-4 to create an AU-4.

- au3Mapper(0)—When the AU mapping is set to AU-3, `each VC-3 High Order Path can be cor ured to carry up to 21 E1s mapped into TU-12.`
- au4Mapper(1)—`When the AU mapping is set to AU-4, the VC-4 High Order Pat three TUG-3s. Each TUG-3 can be configured to carry up to 21 E1s mapp`

Path Trace Configuration
The Path Trace function verifies path connectivity between the two path-terminating nodes.The two SDH path-terminating devices perform the trace over the STM-1 media segment between them. When Path Trace is enabled, the SDH frame carries the Path Trace message in either the J1 byte or the *path trace string*. The value you define for *Path Trace Message Length* determines which field will carry the Path Trace message, as specified below:

1-byte Trace Message Length
Use the J1 byte for trace messaging, and ignore the contents of path trace string. The value of J0 may be any positive integer in the range of 0 to 255.

16-byte Trace Message Length
Use the path trace string for path trace messaging, and ignore the contents of J1. The value of path trace string may be any alphanumeric text string up to 15 characters long. The 16-byte field includes CRC-7 in the 16th byte.

64-byte Trace Message Length
Use the section trace string for section trace messaging, and ignore the contents of J1. The value of section trace string may be any alphanumeric text string up to 64 characters long. The 64-byte field does not include any CRC.

Number of Paths per Frame
The STM-1 frame can support one path or three paths, depending on how the STM-1 signal is mapped.

AU-4 Mapping
Using AU-4 mapping the STM-1 frame supports a single path. When you select AU-4 mapping for the value of the SDH Mapping parameter, the Matrix Switch displays only the Path-1 Trace parameters.

AU-3 Mapping
Using AU-3 mapping the STM-1 frame supports three paths. Each of the three AU-3s in the STM-1 frame represents a separate path. When you select AU-3 mapping for the value of the SDH Mapping parameter, the Matrix Switch displays the Path Trace parameters for each of the three paths. Path-1, Path-2, and Path-3 (one path trace for each AU-3 in the STM-1 frame).

Path Trace Monitor

Options for path trace are:

- pathTraceDisable(0)—Path Trace function disabled.
- pathTraceEnable(1)—Path Trace function enabled.

Path Trace (sdhPathTrace)
This is a character string with the maximum length based on the path trace msg len setting. This field is not used with 1 byte message length. If the length is set to 16, this field is 15 bytes maximum length. A 1-byte crc-7 check is appended to the string to make 16 bytes. If the length is set to 64, this field can hold up to 64 characters.

Path Trace Msg Len `(sdhPathTraceLength)`
Options below determine the path-1 trace message length:

- pathTraceLen1(1)—Path Trace Message is one byte in length.
- pathTraceLen16(16)—Section Trace Message is 16 bytes.
- pathTraceLen64(64)—Section Trace Message is 16 bytes.

Path Trace J1 Byte
If the message length field, is set to 1 byte, this field is used for the message. It holds a decimal value from 0-255. This field is ignored for 16 and 64 byte message length.

Path Signal Label
Enter the value your connected SDH network uses for the path signal label in the SDH frame

SDH Mapper

The SDH Mapper allows configuration of the E1 payload timing with regard to SDH timing.

Note When using AU-3 mapping/multiplexing, the SDH mapper window shows configuration options for TUG3-1, TUG3-2, and TUG3-3. When using AU-4 mapping/multiplexing, only one configuration field with the heading Payload Type is shown.

Payload Type (sdhPayloadType1)

The payload type 1 (DS1 Level) heading is common to all three TUGs in AU-3 mapping mode, and to the single configuration field in AU-4 mapping. The payload type indicates whether the E1 signals are asynchronous or synchronous with respect to SDH.

- stm1MappedAsyncE1(0)—The E1 2 Mbits signals are not synchronized to the SDH signal.

  Note Async mapping imposes no signal structure requirements, therefore a 2 Mbit signal using this mapping doesn't need to be framed. This mapping allows easy interface with existing PDH systems because variable bit justification (bits/bytes used for timing compensations) occurs as part of this mapping, however direct access to 64kbps timeslots is not possible.

- stm1MappedBytesincE1(1)—Byte synchronous mapping means that rate and framing of E1 signals are synchronized to the SDH signal.

  Note Byte synchronous mapping requires G.704 framing on the E1 signals. Since bit justification is not used, the E1 signal must be already synchronized to the SDH network. This type of mapping allows direct access to 64kbps timeslots, therefore it should be used for nx64kbps services.

Chapter 16 About

Chapter contents

Introduction

The *About* link displays Patton Electronics Company contact information (see "Patton Electronics Company contact information"). Click on *About* under the 6511RC's *Configuration Menu* to display the *ABOUT* main window (see figure 88).

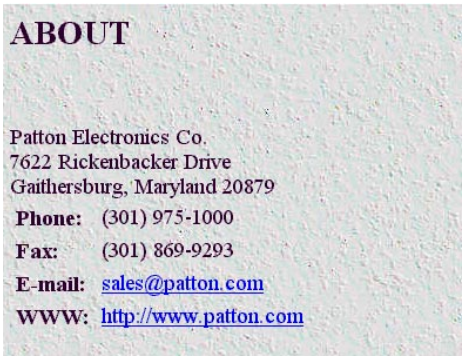


Figure 88. ABOUT window

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 17 License

Chapter contents

Introduction

The *License* link presents the *End User License Agreement* for the 6511RC software. Click on *License* under the *Configuration Menu* to display the *END USER LICENSE AGREEMENT* main window (see figure 89).

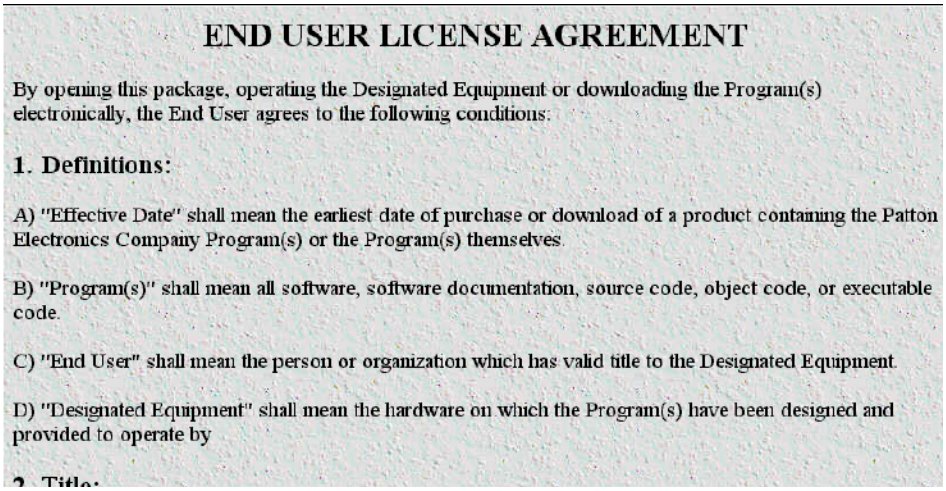


Figure 89. END USER LICENSE AGREEMENT window

Note By opening the 6511RC, operating the Designated Equipment or downloading the Program(s) electronically, the End User agrees to the conditions in the End User License Agreement (section "End User License Agreement" provides a copy of the agreement).

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 the End User.

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:" on page 153.

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 section "4. Grant of License:".

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)

Appendix A **Updating the operating software**

Chapter contents

Introduction

From time to time, Patton may provide online software upgrades for the Model 6511 Matrix Switch. As a Matrix Switch owner, you can obtain such software updates from Patton's web site at **upgrades.patton.com**.

To obtain an updated software release you will need:

- A computer workstations such as a PC or laptop with a standard browser (such as Internet explorer or Nestcape Navigaotr)
- An Internet connection to your workstation

Software upgrade procedures

Do the following to update the software for your Model 6511 Matrix Switch:

1. Open a standard browser on your computer workstation
2. Enter the URL **upgrades.patton.com** in the *Address* field. The *UPGRADES.patton.com* web page displays (see figure 90).

Figure 90. UPGRADES.patton.com web page

3. Click the *Model 6511RC (SDH/Ethernet Matrix Switch)* hyperlink. The Software Updates page displays (see figure 91). The page lists all Model 6511RC software releases and the release date for each.

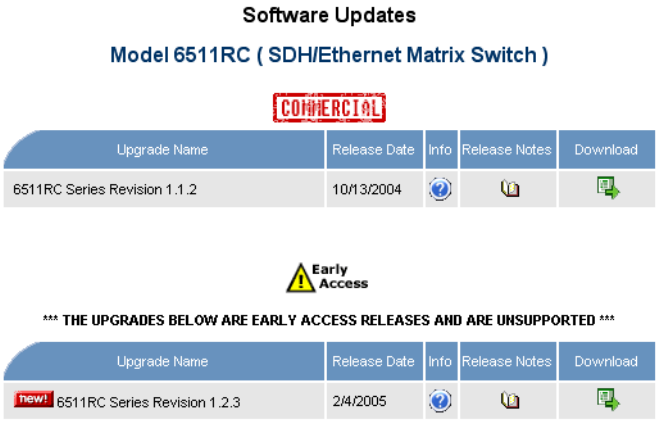


Figure 91. Model 6511RC Software Updates window

4. Determine which software release you need, then click the icon in the *Download* column for the desired software release.
5. The *End-user License Agreement* displays (see figure 92). Read it carefully, then click the **I agree** button to begin downloading the software release.

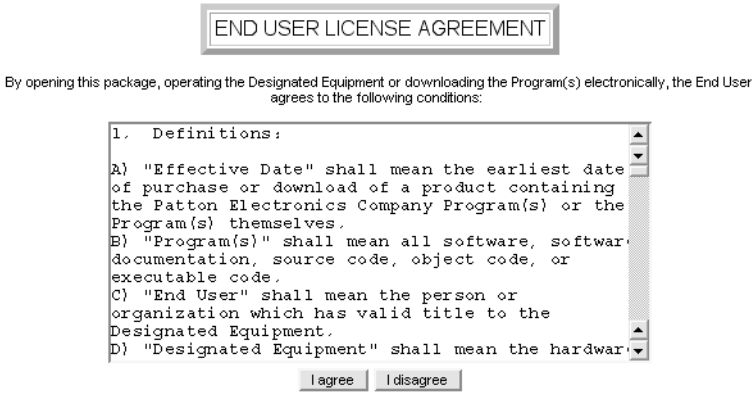


Figure 92. End-user license agreement window

Figure 93. Software Upgrades Authentication login window

6. The authentication login page displays (see figure 93). If you have already registered and have a user name and password, then go to step 8. Otherwise, click the *click here* link to register.
7. The *Patton Upgrades Registration* page appears (see figure 94). Complete the registration form and click the **Register** button at the bottom of the page.

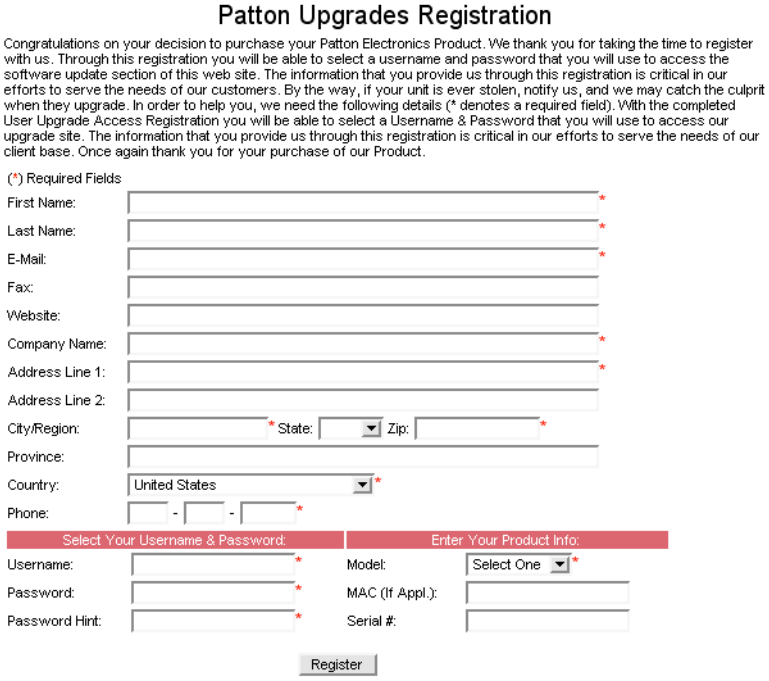


Figure 94. Patton Upgrades Registration window

8. Enter your username and password in the authentication page and click the **Login** button.
9. When the pop-up window appears, select *SAVE*. Save the zip file to a location on your computer where you will be able to easily find it.
10. Unzip the contents of the zip file into a folder as follows:
    - Right-click the file icon.
    - Select **Open with WinZip.**

– Click **Next.**

– Select a folder on your computer.

– Click **Unzip now.**

– Click **close.**

11. Go to the folder where you saved the unzipped contents. Double click the filename *6511Download Procedure.txt t*o open the file.

12. Read and follow the intructions contained in 6511Download Procedure.txt. A sample copy of one such set of instructions is provided below for your reference.

```
###############6511Download Procedure.txt########
Model 6511RC
                  Software Installation Procedures

REQUIREMENTS
The following must be true of your 6511RC before loading new operational
software:

1. You must have a valid IP address assigned to the 6511RC
2. You must have an FTP client on a machine which can communicate with
   the LAN


PROCEDURES

To load new software into the 6511RC, execute the following steps:

1. Boot the 6511RC
2. Open a DOS window on your Windows platform
3. After the 6511RC has fully booted, type the following command at the
   DOS prompt: "ftp <the IP address of the 6511RC>"
4. At the Username prompt, type: "KillImage"
5. At the Password prompt, type: <your superuser password> (the default
   is "superuser")
6. At the ftp prompt, type: "bin"
7. At the ftp prompt, type: "put flash.img" (if the flash.img file is
   not in the current path, be sure to specify the path of the file)
8. When the transfer process has completed, the 6511RC will reboot.
   DO NOT DO ANYTHING TO THE 6511RC UNTIL THE DOWNLOAD PROCESS HAS COM-
PLETED!

This has been done using the Windows command line FTP client. Other FTP
clients may work fine as well. Be sure to select a binary (or image)
transfer.

Other FTP clients may be annoyed that the 6511RC FTP server does not provide
a directory.  Normally, this is permissible if you bypass the messages for
your FTP client.
```