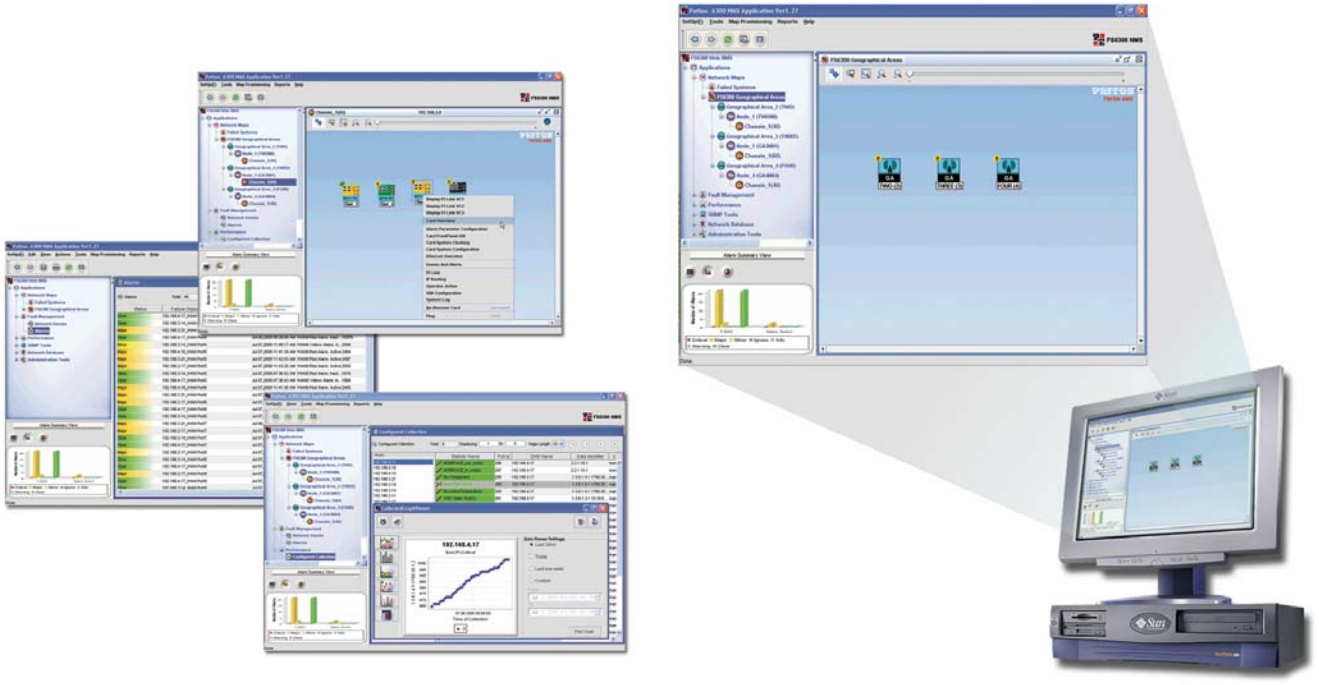
ForeSight 6300

Network Management System

User Manual



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

Part Number: **07MFS6300-GS, Rev. B**
Revised: **February 29, 2012**

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
Web: www.patton.com
E-mail: support@patton.com

Trademark Statement

The term *ForeSight* is a trademark of Patton Electronics Company. All other trademarks presented in this document are the property of their respective owners.

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

Warranty Information

The software described in this document is furnished under a license and may be used or copied only in accordance with the terms of such license. For information about the license, go to **www.patton.com**.

Patton Electronics warrants all NMS components to be free from defects, and will—at our option—repair or replace the product should it fail within one year from the first date of the shipment.

This warranty is limited to defects in workmanship or materials, and does not cover customer damage, abuse or unauthorized modification. If the product fails to perform as warranted, your sole recourse shall be repair or replacement as described above. Under no condition shall Patton Electronics be liable for any damages incurred by the use of this product. These damages include, but are not limited to, the following: lost profits, lost savings and incidental or consequential damages arising from the use of or inability to use this product. Patton Electronics specifically disclaims all other warranties, expressed or implied, and the installation or use of this product shall be deemed an acceptance of these terms by the user.

Summary Table of Contents

Table of Contents

List of Figures

List of Tables

About this guide

The Patton *ForeSight 6300 NMS User Manual* helps you configure basic operations for the FS6300 Network Management System (NMS). For more detailed information about configuring advanced features, see the *ForeSight 6300 NMS Administrator's Reference Guide*.

Audience

This guide is intended for the following users:

- Operators
- Installers

Structure

This guide contains the following chapters and appendices:

- Chapter 1 on page 15 provides basic information on NMS features and functions
- Chapter 2 on page 24 provides information on discovering your network
- Chapter 3 on page 46 provides information on configuring alarms and clocking
- Chapter 4 on page 57 provides information on configuring and managing individual devices
- Chapter 5 on page 67 provides basic information on configuring the 2616RC card
- Chapter 6 on page 83 provides basic information on configuring the 3096RC card
- Chapter 7 on page 105 provides basic information on configuring the 3196RC card
- Chapter 8 on page 126 provides basic information on configuring the 6511RC card
- Chapter 9 on page 139 provides information on configuring a chassis
- Chapter 10 on page 143 provides information on contacting Patton technical support for assistance

For best results, read the contents of this guide *before* you install the NMS.

Chapter 1 Introduction

Chapter contents

Overview

This chapter introduces you to the features and benefits of the FS6300 NMS. It also includes basic information about logging in and out of the system, and working with the main toolbars and menus.

FS6300 NMS Features

- Integrated FCAPS
- Scalable NMS
- Configuration Management
- Alarm Management
- Security Management
- Administration Management
- Performance Management

Common User Tasks

The following are user tasks you will encounter when working with the FS6300 NMS:

- Discover the network (See "Discovering Your Network" on page 24)
- Configure alarms and clocking (See "Configuring Alarms and Clocking" on page 46)
- Configure and manage individual devices in the network (See "Configuring and Managing Devices" on page 57)
- Manage network events (Refer to the *FS6300 NMS Administrator's Reference Guide*)
- Monitor performance data (Refer to the *FS6300 NMS Administrator's Reference Guide*)

Bringing up the NMS Server from Linux

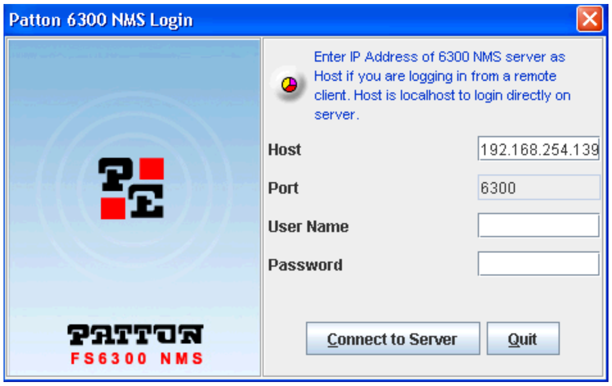
To start the server, from the */opt/FS6300/Server/<release #>* directory, double-click on the **WebNMSLauncher.sh** file to open the launcher. To start and stop the server, in the splash screen window, right-click on the **Start 6300 NMS Server** icon and select **Run**. To initialize the database, right-click on the **Reintialize 6300 NMS** icon and select **Run**, then acknowledge the confirmation request in the pop-up window.

Bringing up the NMS Client from Windows XP

The NMS Windows Remote Application Client (WRAC) is the primary client for the FS6300 NMS. It is recommended that you use the WRAC. You can launch the WRAC by double-clicking on the **WebNMSLauncher.bat** icon on the desktop. In the resulting splash screen window, right-click on the client icon and select **Run**. Then, enter the authentication information in the FS6300 NMS Authentication dialog box.

Logging into the Application Client

The FS6300 NMS Authentication box is displayed to provide an authenticated access to the FS6300 NMS. Enter a valid user name and password to access the Application Client.



Patton 6300 NMS Login

Enter IP Address of 6300 NMS server as Host if you are logging in from a remote client. Host is localhost to login directly on server.

Host 192.168.254.139

Port 6300

User Name

Password

Figure 1. Logging in to the application client

1. In the **Host** field, enter **localhost** for the server address if you are logging in directly to the server. If you are logging in from the WRAC, enter the **IP address** of the NMS server.
2. Enter the **User ID** assigned to you in the User ID field. If you do not have a User ID, contact your system administrator. For unconfigured systems, the default User ID is **superuser.**
3. Enter the password assigned to you in the **Password** field. To learn how to configure your password, see "Configuring Your Password" on page 18. For unconfigured systems, the default password is **superuser**.
4. Click **Connect**.

The splash screen with a progress bar is shown before the Application Client is completely opened.

Configuring Your Password

Configuring your password before connecting to the client

When you log on to the Application Client for the first time, a Password Confirmation dialog box is displayed (only if this has been enabled by your administrator). If you do not see this dialog box, then ignore this section and perform the steps explained in the next section, "Configuring your password from the client" on page 18 .

To configure your password before connecting to the client:

1. In the Password Confirmation dialog box, click **Reuse** to continue using the same password for the same period as previously configured. To enter a new password, click **Configure** and perform further steps.
2. Enter the new password in the **Type new password** field.
3. Re-enter the same password in the **Confirm new password** field.
4. Enter the number of days you want your password to be valid in **Password expiry duration.** If no value or zero is entered in this field, then the password never expires.
5. Click **Connect.**

The new password is assigned to you and you are connected to the Application Client. You need to use this new password from the subsequent login.

Configuring your password from the client

1. After logging into the client, select **Security Administration** from the Tools menu. Select the user from the users list, and click **Edit** in the Menu bar. Select **Change Password**. The Password Configurator window is displayed.
2. Enter the new password in the **New Password** field.
3. Re-enter the same password in the **Confirm Password** field.
4. Click **OK**. The new password is assigned to the user.

Troubleshooting

Table 1 lists the messages that are displayed in certain situations during the login process.

Table 1. Troubleshooting messages

Message	Why am I getting this?	What do I do?
You are logged in for the first time; would you like to reuse the existing password or configure a new password? (See "Configuring your password before connecting to the client" on page 18).	This pop-up message is displayed when you log on to the Application Client for the first time (only if this has been enabled by your administrator).	Refer to "Configuring your password before connecting to the client" on page 18 for the procedure.
Your password has expired. Would you like to reuse the old password or configure a New password?	Your password has expired.	• You can either set a new password or retain the old password. • Click Reuse to keep the same password and for the same expiration period configured before. • Click Configure to enter a new password. Refer to "Configuring your password before connecting to the client" on page 18 for the procedure. • If you do not have the permission to set your password, contact your system administrator.
This User account has Expired. Please contact the Administrator for further details	Your user account has expired. The user account is created by your system administrator.	Contact your system administrator to renew your user account.
This User account is Disabled. Please contact the Administrator for further details	• Your user account has been disabled by your system administrator. • Also, if your consecutive login attempts fail for a certain number of retries (number is configured by the administrator), the user account is automatically disabled.	Contact your system administrator to enable your user account.

Table 1. Troubleshooting messages

Message	Why am I getting this?	What do I do?
Connection lost to the FS6300 NMS server at <host>. Do you want to shutdown the client?	This message is displayed if the connection between the client and server is lost due to network problems or if the server is shut down abruptly.	• Click Yes to shut down the client or No to continue working. • If you decide not to close the client even after the connection is lost, the screens, views, and data of the client remain the same, but you cannot perform any further operations in the client and no updates occur. You need to reopen the client and reconnect to the FS6300 NMS Server.
[Lock Screen dialog box] Please enter your password to unlock the client	This dialog box is displayed when the Application Client is idle for more than a specific period, that is, when there is no interaction between the user and the Application Client (no mouse or keyboard events).	• Enter a valid password in the Password field and click Unlock to resume working on the Application Client. • To disable this prompt every time the Application Client is idle (only for that session), select Don't show this dialog for the current session any more • Only specific number of unsuccessful logins are allowed. When exceeded, the session with Application Client is forcefully terminated and you need to reopen the Application Client.
FS6300 NMS Application Client has been terminated	• This message is displayed when the Application Client is idle for more than a specified period, that is, when there is no interaction between the user and the Application Client. • The Application Client is terminated.	Bring up/reopen the client again.

Using the NMS Menus

The following menu items are always available at the top of the main window of the NMS:

- **SetUp(F):** Add Device | 6300 Container Definition | Back | Forward | Exit
- **Tools:** Schedule Tasks | Discovery Administration | View Exported Card Configuration | Firmware Upgrade | Multiple Card Configuration | Security Administration
- **Map Provisioning:** Create Inter-Chassis Links | Auto-Screen Maps and Channels | Create and Manage DS0 Maps | DS0 Availability by Ports | Chassis Diagnostics | InBand Channel Management
- **Reports:** Alarm Tracking | Chassis Checklist | Discovery Checklist | Device Checklist | NMS Summary
- **Help:** About FS6300 NMS

Additionally, some options in the menu tree have other toolbars at the top related to their function in the network:

- **Fault Management - Network Events - View:** Details | Alarms | Refresh
- **Fault Management - Network Events - Actions:** Save To File | Export Events | Print
- **Fault Management - Alarms - Custom Views:** Add | Remove | Modify
- **Fault Management - Alarms - Edit:** Delete | Pick Up/UnPick | Clear | Search
- **Fault Management - Alarms - View:** Delete | Details | Events | Refresh
- **Fault Management - Alarms - Actions:** Save To File | Export Events
- **Performance - Configured Collection - View:** Plot - Current Statistic | Plot - Collected Statistic | Refresh
- **Network Database - View:** Details | Events | Alarms | Statistics | Refresh
- **Network Database - Object:** *Varies depending on object type*
- **Administration Tools - Policies - Policy:** Add Policy | Search | Refresh
- **Administration Tools - Policies - Edit:** Update Policy | Delete Policy | Execute Policy | Stop Policy

Also, **right-clicking** on a device in the main window will display a menu of options available for that specific device.

Logging out of the Application Client

To log out, perform any of the following procedures:

- From the **SetUp(F)** menu at the top of the screen, choose **Exit**.
- Press **Alt+F4**.

A Confirmation Message dialog box is displayed. Click **Yes** to quit the client.

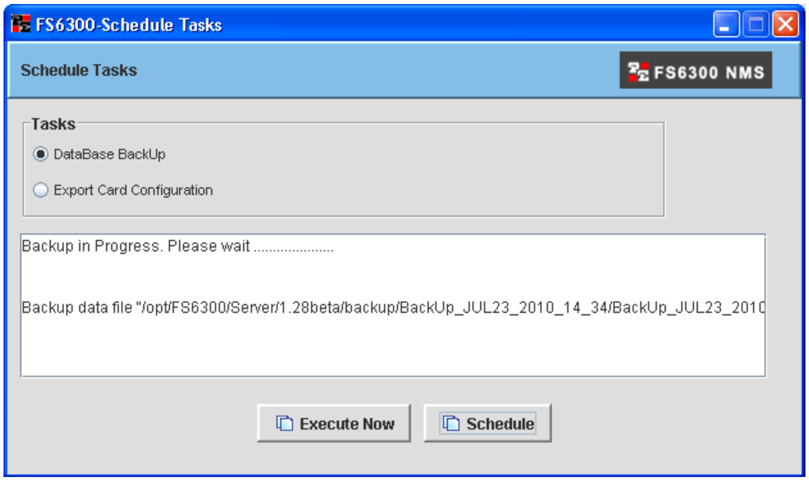
Note Do not use the **X** button to close the client. Always use the **Exit** option. Using the **X** button may lock the user out of the system.

Backing Up the Database

The FS6300 NMS provides a tool for backing up the database. You may also create a policy to backup the database automatically based on a schedule.

Creating a backup file of the database

1. Click **Tools** > **Schedule Tasks** in the main window. In the **FS6300-Schedule Tasks** window, select the radio button for **Database Backup**.
2. Click **Execute Now**. A status message will display as the system completes the backup process.



● DataBase BackUp

○ Export Card Configuration

```
Backup in Progress. Please wait ....................

Backup data file "/opt/FS6300/Server/1.28beta/backup/BackUp_JUL23_2010_14_34/BackUp_JUL23_2010
```

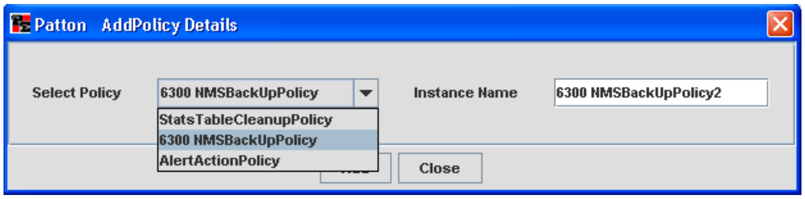
Figure 2. FS6300 Schedule Tasks window

3. The backup file is saved to the *opt/FS6300/<version>/backup/* directory.

Scheduling a policy to backup the database

The **6300 NMS Backup** policy automatically backups the system to reduce the load on the server.

1. Click on **Administration Tools** > **Policies** in the NMS menu tree.
2. Select **Policy** > **Add Policy** from the menu at the top of the screen. The **Add Policy Details** window displays.

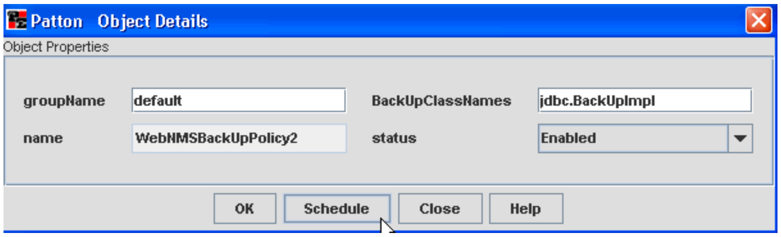


Select Policy: 6300 NMSBackUpPolicy

Instance Name: 6300 NMSBackUpPolicy2

Figure 3. Add Backup Policy

3. Select **6300NMSBackupPolicy** from the drop-down menu. Enter a **Name** for the backup policy and click **Add**. The **Object Details** window displays.



groupName: default

BackUpClassNames: jdbc.BackUpImpl

name: WebNMSBackUpPolicy2

status: Enabled

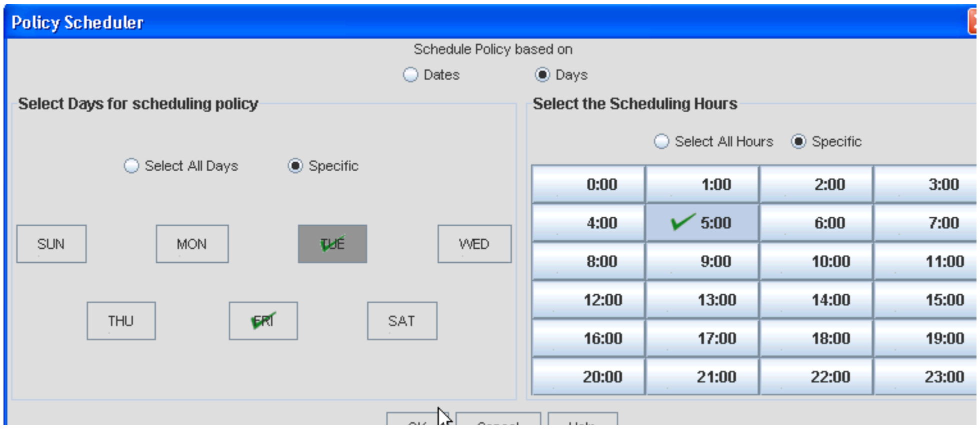
Figure 4. Policy Details

4. Table 2 describes the fields for adding a new **6300NMSBackup** policy.

Table 2. FS6300 NMS Backup Policy Properties

Property	Description
groupname	Specify the name of the group to which the policy belongs. If default is specified, the policy does not belong to any group. (You can execute different policies at the same time by associating them with a common group name).
name	Displays the name of the backup policy. *This field cannot be edited.*
BackUpClassNames	Specify the class name implementing the backup interface.
Status	Specify whether the status of the policy is Enabled or Disabled. The policy can be executed only when it is Enabled.

5. Click **Schedule** in the **Object Details** window. The **Policy Scheduler** window displays. Select the radio buttons for **Dates** or **Days**, depending on what your policy schedule will be based on. You can select all dates/days and hours, or specific selections. Click on the box of the day, date, or hour to make your selection. Then, click **OK**.



Schedule Policy based on ○ Dates ● Days

Select Days for scheduling policy ○ Select All Days ● Specific

Select the Scheduling Hours ○ Select All Hours ● Specific

0:00	1:00	2:00	3:00
4:00	✓ 5:00	6:00	7:00
8:00	9:00	10:00	11:00
12:00	13:00	14:00	15:00
16:00	17:00	18:00	19:00
20:00	21:00	22:00	23:00

Figure 5. Policy Scheduler

6. Click **OK** in the **Object Details** window to save the policy. A confirmation message displays that the policy was added successfully.

Chapter 2 Discovering Your Network

Chapter contents

Overview

The Discovery process is the most important step in working with the NMS. This chapter describes how to add containers before discovering your network, how to schedule rediscovery processes, and how to add a device manually to the system.

To open the **Discovery** window, click on **Tools** > **Discovery Administration** at the top of the screen.

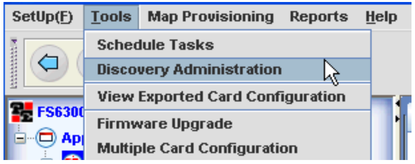


Figure 6. Tools > Discovery Administration

Note The FS6300 supports Patton Models 2616RC, 3096RC, 3196RC and 6511.

Note The FS6300 currently only supports all devices with same community strings and networks with 24 bit masking.

Defining Containers

Containers are unique identification details about the Geographical Areas, Network Nodes, and Chassis in your network. You may pre-define and create a master list of containers before initial discovery of your network, or you may define containers while configuring multiple cards.

Pre-Defining Containers Before Initial Discovery

Before starting discovery, you may create a master list of pre-defined details for the Geographical Areas, Nodes, and Chassis in your network. When you configure multiple cards later, you can refer to your master list of containers. To reach the **Container Definition** window, click on **SetUp(F)** > **6300 Container Definition** at the top of the screen.

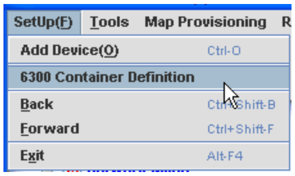
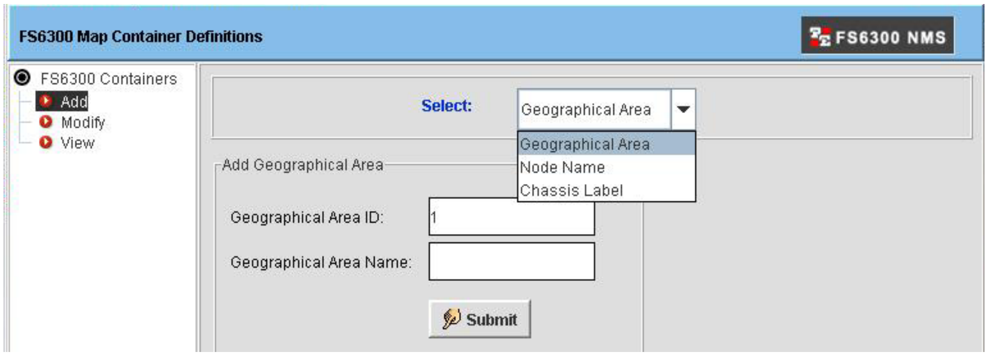


Figure 7. SetUp(F) > 6300 Container Definition

Adding Pre-Defined Containers

To add containers in the NMS:

1. In the Container window, click on **Add** in the menu tree.



Select: Geographical Area

Geographical Area ID: 1

Figure 8. Add Container

2. From the drop-down menu, select which type of container you want to add. You should add the Geographical Areas first, then add the Nodes in that area, then add the Chassis Labels in the Nodes. Each Geographical Area-Node-Chassis combination is unique, and may only be applied to cards in one chassis-subnet.

   – **Geographical Area (GA):** The Geographical Area ID must be numerical, and cannot be changed once it is added to the system. However, the Name may be modified at any time.

   – **Node Name (NN):** Add nodes in the network to a Geographical Area. You may also add details such as system manager and system location.

   – **Chassis Label:** The Chassis ID must be numerical, but the Label Name is optional.

Note The GA ID must be unique across the entire NMS. The NN ID must be unique across the entire Geographical Area it is under. The Chassis ID must be unique across the entire Network Node it is under.

3. Click **Submit**.

Modifying Pre-Defined Containers

To modify pre-defined containers:

1. In the Container window, click on **Modify** in the menu tree.

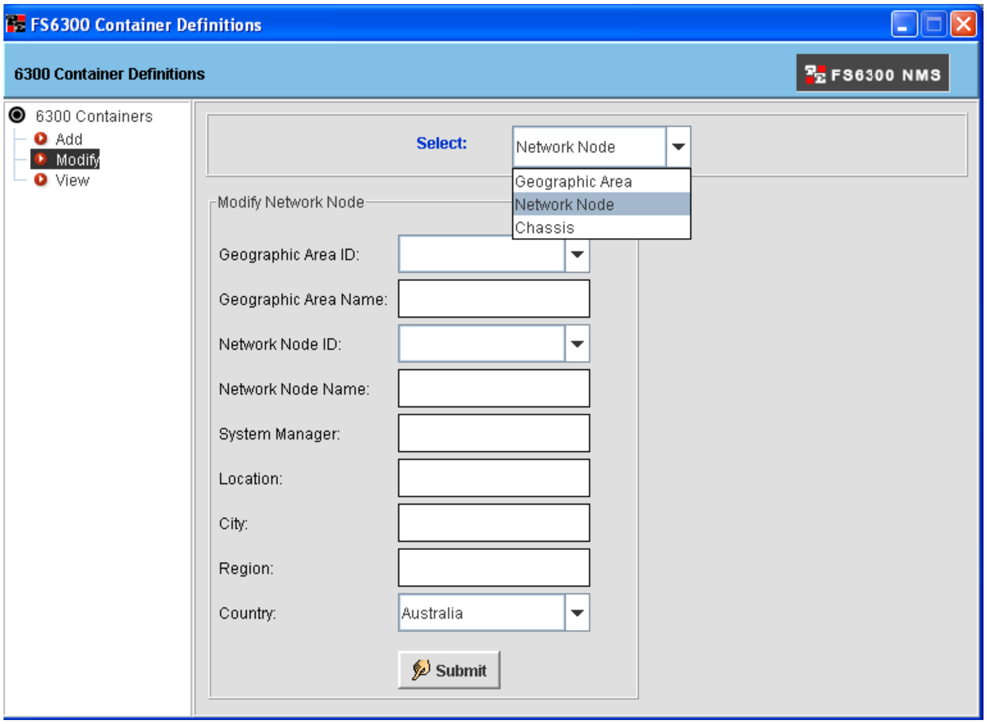


Figure 9. Modify Container

2. From the drop-down menu, select which type of container you want to modify. Some items, such as ID, are permanent and cannot be modified.
3. Click **Submit**.

Viewing and Deleting Containers

To view or delete containers:

1. In the Container window, click on **View** in the menu tree.

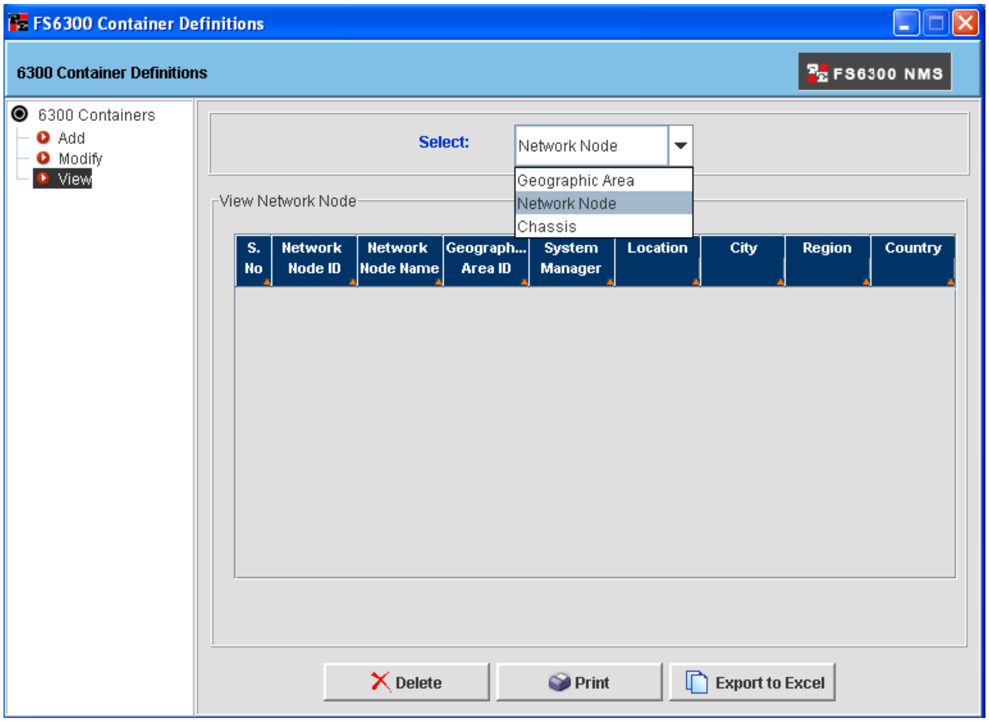


Figure 10. View Containers

2. From the drop-down menu, select which container type you want to view.
3. The table displays a list of containers. This table includes details that were added or modified during multiple card configuration, but it does not reflect the list of Geographical Areas, Network Nodes, or Chassis IDs existing on discovered cards. You can rearrange columns in the table by clicking and dragging the column to the desired order.
4. To delete a container, select the row of the container in the table, and click **Delete**. A container may be deleted ***only*** if the container is **not assigned** to any card in the NMS.
5. If desired, click **Print** to send the list to a printer or **Export to Excel** to save the list to a Microsoft Excel spreadsheet.

Defining Containers During Multiple Card Configuration

You may wish to define containers after all of the chassis in your network have been discovered. In this case, you may add IDs, details, and labels during the multiple card configuration process. To reach the **Multiple Card Configuration**. window, click on **Tools** > **Multiple Card Configuration**. at the top of the screen.

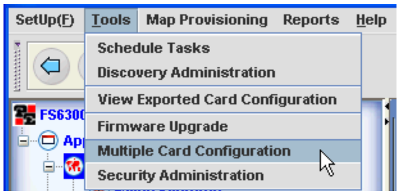
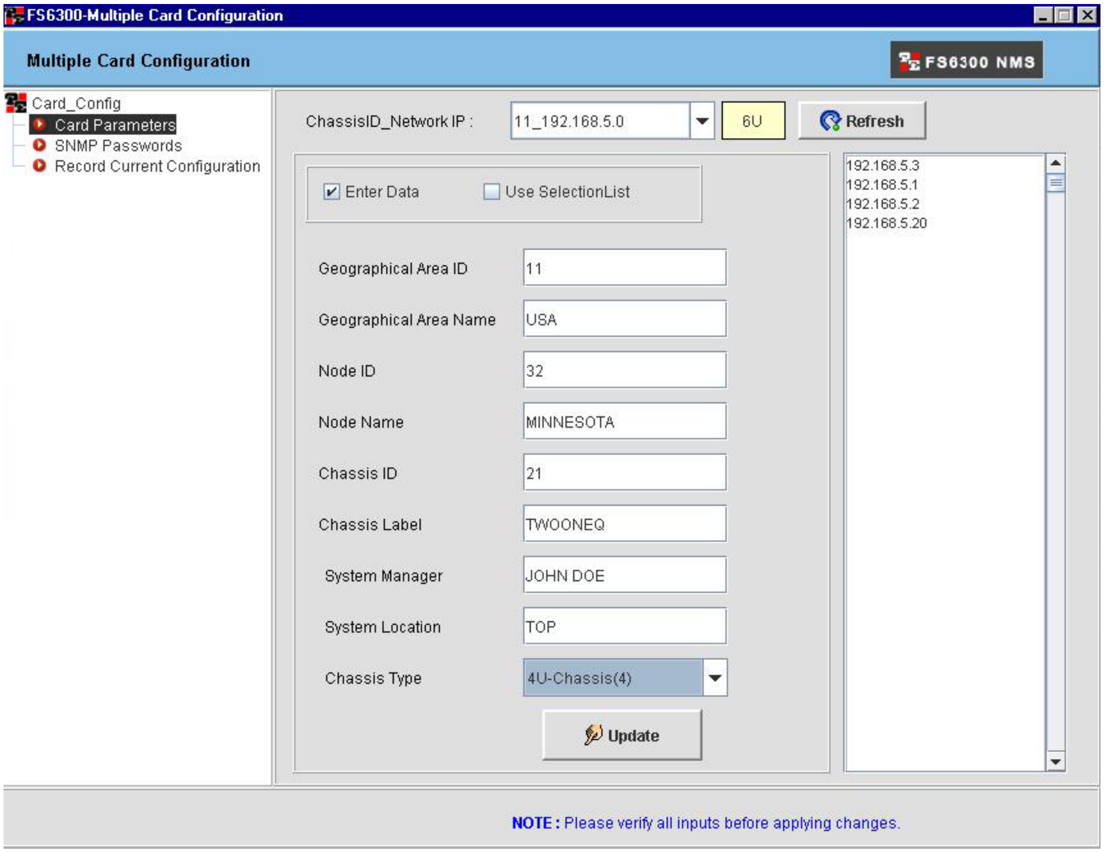


Figure 11. Tools > Multiple Card Configuration

1. Click on **Card Parameters** in the menu tree on the left side of the screen.


FS6300-Multiple Card Configuration
Multiple Card Configuration
FS6300 NMS
Card_Config
Card Parameters
SNMP Passwords
Record Current Configuration
Refresh
Update

ChassisID_Network IP : 11_192.168.5.0 6U

☑ Enter Data ☐ Use SelectionList

192.168.5.3
192.168.5.1
192.168.5.2
192.168.5.20

Geographical Area ID	11
Geographical Area Name	USA
Node ID	32
Node Name	MINNESOTA
Chassis ID	21
Chassis Label	TWOONEQ
System Manager	JOHN DOE
System Location	TOP
Chassis Type	4U-Chassis(4)

NOTE : Please verify all inputs before applying changes.

Figure 12. Multiple Card Configuration > Card Parameters

2. Select the network address for the chassis in the drop-down menu at the top of the window.

3. You can modify containers by typing in the data or using drop-down menus. Select the checkbox at the top of the Card Parameters window for the option you want to use.

4. Enter the information you want to update on the subnet for the following fields, or if you are using the Selection List, you may select containers from the pre-defined master list.

   – **Geographical Area ID** *(This is permanent and cannot be modified).*

- **Geographical Area Name** (Descriptive name of the geographical area)
- **Node ID** *(This is permanent and cannot be modified).*
- **Node Name** (Descriptive name of the node)
- **Chassis ID** *(This is permanent and cannot be modified).*
- **Chassis Label** (Descriptive label for the chassis)
- **System Manager** (Name of the person managing this subnet on the network)
- **System Location** (Description of where the system is located)
- **Chassis Type** (Choose a chassis type from the drop-down menu)

5. Click **Update** to save the information for all of the cards on that subnet.

If the same CH ID exists on cards in a different chassis unit but with the same subnet address, an alert is displayed asking if the cards need to be merged into one unit.

If the same CH ID exists on cards in a different chassis unit and with different subnet address, an alert is displayed that Chassis ID already exists.

This is to ensure uniqueness of Chassis IDs in the NMS.

The following details are also checked when modifying containers during multiple card configuration:

- If there is already an entry for the GA ID and GA Name entered by the Admin
- If not, a new record is added to the master-list.
- If the master-list instead has an entry for GA-101-Michigan or GA-105-Maryland, an alert is displayed requesting the admin to re-enter the ID/Name

The NMS also verifies containers to prevent duplication of ID and name for the Network Node.

- If the values entered are successfully verified and found to be unique, these values are auto-updated in the master-list table (mentioned with Option A above), in the background.
- 6300 NMS does not allow these records to be deleted from the 6300-Conatiner definition interface.
- All cards in the selected chassis are configured with the new container IDs.

figure 13 shows a visual representation of container IDs in the NMS.

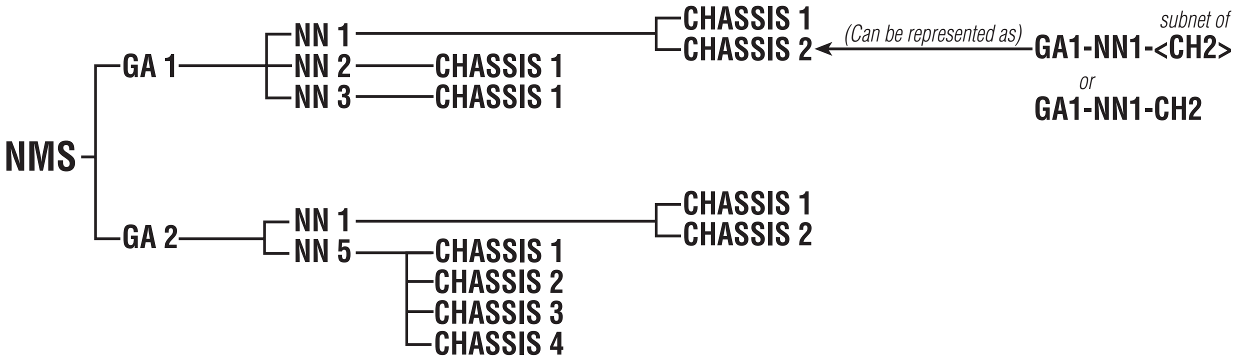


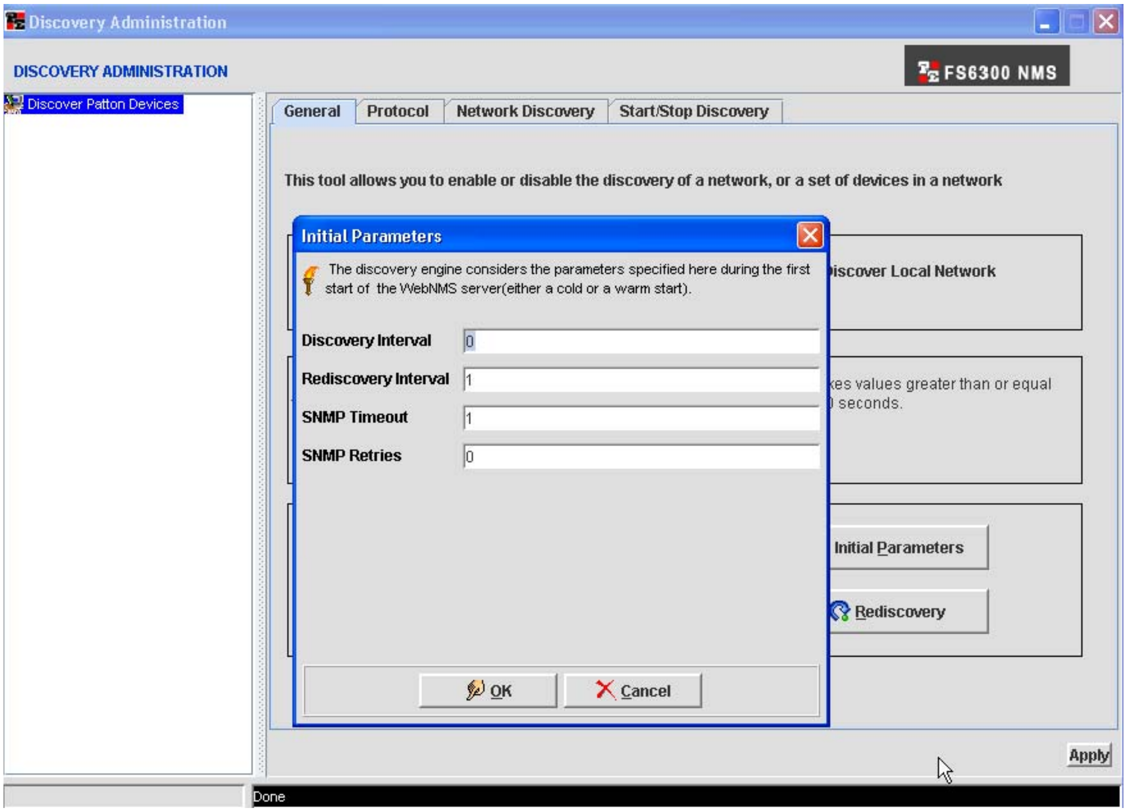
Figure 13. Container IDs in the NMS

Configuring Initial Discovery Parameters

The **Initial Discovery** process is the first discovery process that is started as soon as the FS6300 NMS server loads.

To set initial discovery parameters:

1. Click on **Tools** > **Discovery Administration** at the top of the screen. Then, click on **Discover Patton Devices** in the menu tree of the Discovery window.
2. Click on the **General** tab, then click the **Initial Parameters** button.



This tool allows you to enable or disable the discovery of a network, or a set of devices in a network

Initial Parameters

The discovery engine considers the parameters specified here during the first start of the WebNMS server(either a cold or a warm start).

Discovery Interval: 0

Rediscovery Interval: 1

SNMP Timeout: 1

SNMP Retries: 0

Figure 14. Set Initial Parameters

3. The initial parameters are:
   - **Discovery Interval:** Interval (in seconds) between the discovery of any two devices in the network.
   - **Rediscovery Interval:** Interval (in hours) between two complete discoveries of a network.
   - **SNMP Timeout:** Threshold value, in seconds, for all the SNMP requests.
   - **SNMP Retries:** Number of SNMP retries for discovery, status polling, and data collection.
4. Click **OK**. Then, click **Apply** in the Discovery Administration window.

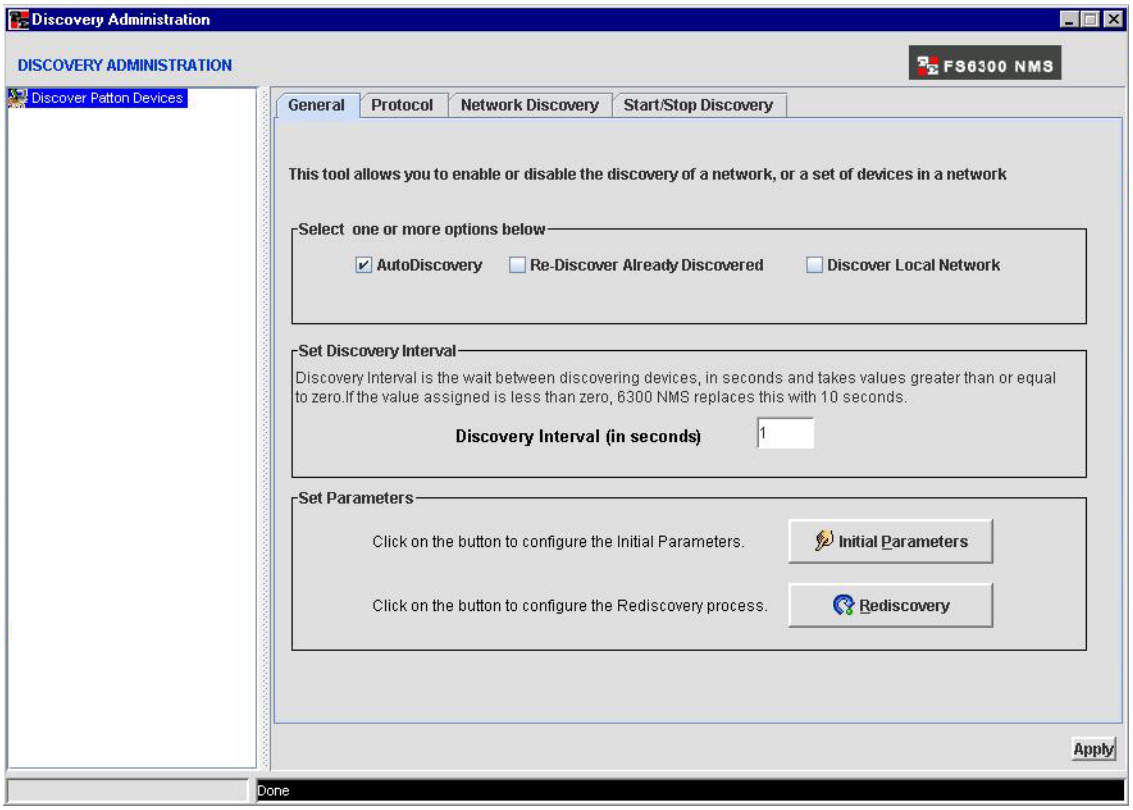
Starting the Discovery Process

Before starting the Discovery process, at least one node must be deployed, powered up, and connected to the network.

Enabling AutoDiscovery

To start Discovery:

1. From the **Tools** menu at the top of the screen, select **Discovery Administration**.
   The Discovery Window displays.
2. Click on **Discover Patton Devices** in the tree on the left side of the screen.
3. Click on the **Auto-Discovery** checkbox.



This tool allows you to enable or disable the discovery of a network, or a set of devices in a network

Select one or more options below

☑ AutoDiscovery □ Re-Discover Already Discovered □ Discover Local Network

Set Discovery Interval

Discovery Interval is the wait between discovering devices, in seconds and takes values greater than or equal to zero.If the value assigned is less than zero, 6300 NMS replaces this with 10 seconds.

Discovery Interval (in seconds) 1

Set Parameters

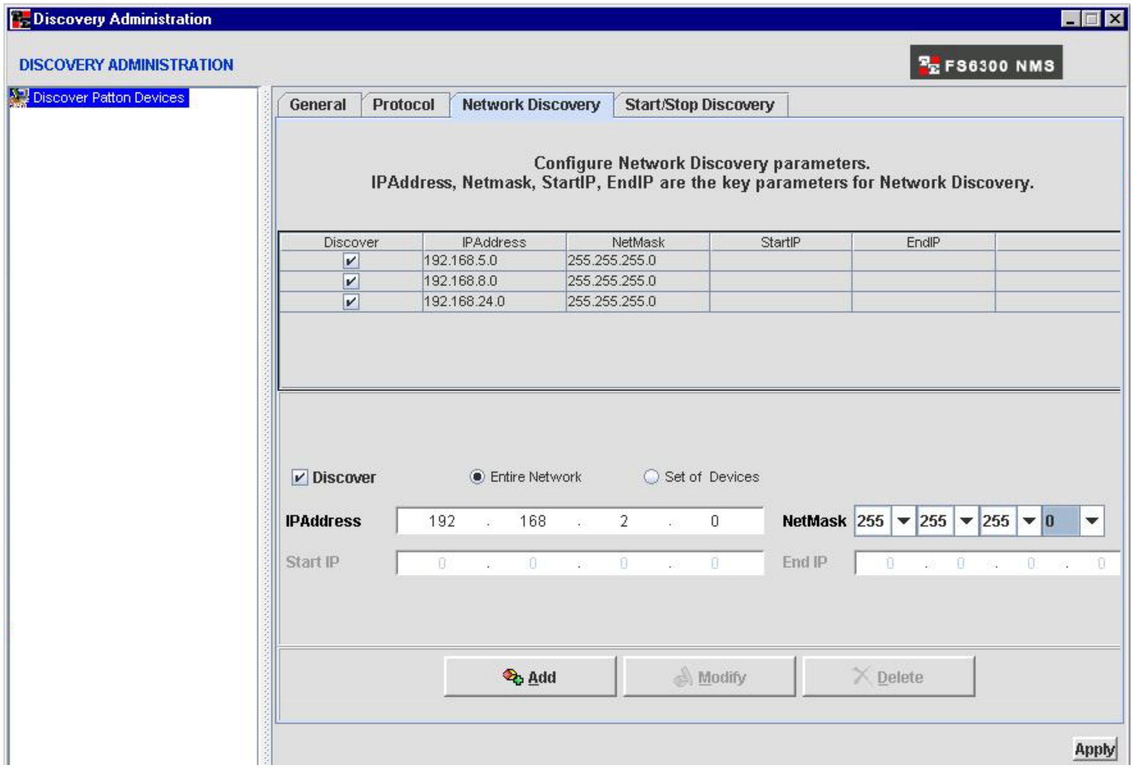
Click on the button to configure the Initial Parameters.

Click on the button to configure the Rediscovery process.

Figure 15. Discovery Window

Configuring Discovery of Specific Networks

4. Click on the **Network Discovery** tab at the top of the Discovery Administration window.



Configure Network Discovery parameters.
IPAddress, Netmask, StartIP, EndIP are the key parameters for Network Discovery.

Discover	IPAddress	NetMask	StartIP	EndIP
☑	192.168.5.0	255.255.255.0		
☑	192.168.8.0	255.255.255.0		
☑	192.168.24.0	255.255.255.0		

☑ Discover ● Entire Network ○ Set of Devices

IPAddress 192 . 168 . 2 . 0 NetMask 255 255 255 0

Start IP 0 . 0 . 0 . 0 End IP 0 . 0 . 0 . 0

Figure 16. Network Discovery tab

5. Enter the **IP Address** of the network or set of devices you want the FS6300 NMS to discover. Click **Add**. Repeat this step to add more networks for the NMS to discover.

6. Click **Apply** to begin the Discovery process.

7. Returning to the main window, click on **Networks** (under *Network Database*) in the menu tree to see if the IP subnet has already been entered into the Networks table for discovery.

Note The discovery process may take some time, depending on how many nodes there are to discover on your network. During the Discovery process, a blue icon with an actively spinning wheel will be in the upper right-hand corner of the main window.

IMPORTANT

It is very important that you do not attempt to configure any parameter during the Discovery process. Attempting to do so could corrupt the data being collected during Discovery.

When the NMS has collected enough information to identify the node, the node will be listed in the Nodes table (under Network Database). As more information is collected through the Discovery process, entries will appear in the **FS6300 Geographical Areas** section (under *Network Maps*).

When the Discovery process is complete, the spinning wheel icon is replaced with a blue box containing a white checkmark. Once Discovery is complete, a new subnet can be entered into the Network Discovery window (**Tools** > **Discovery Administration**).

Setting Discovery Interval

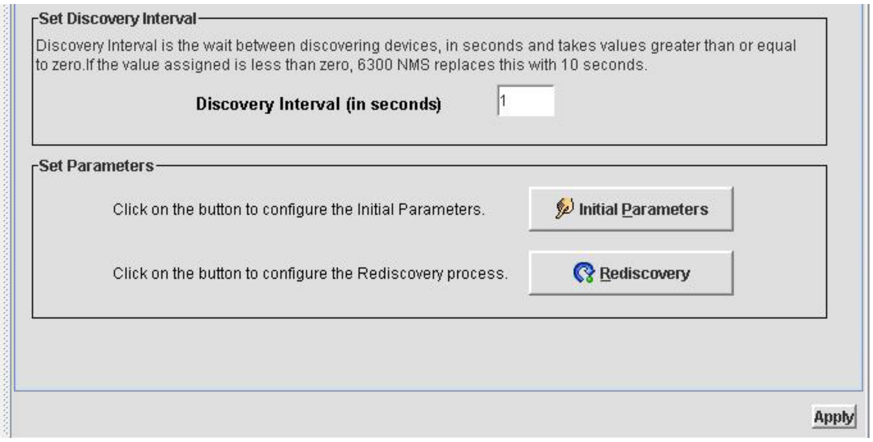
You can set the wait time between discovering devices by configuring the Discovery Interval.

To set the discovery interval:

1. In the **General** tab of the Discovery Configurator,

1. Click on **Tools** > **Discovery Administration** at the top of the screen. Then, click on **Discover Patton Devices** in the menu tree of the Discovery window.

2. Click on the **General** tab, then enter the interval value (in seconds) in the **Discovery Interval** box. The value can be greater than or equal to zero and the default value is 1 second.



Set Discovery Interval

Discovery Interval is the wait between discovering devices, in seconds and takes values greater than or equal to zero.If the value assigned is less than zero, 6300 NMS replaces this with 10 seconds.

Discovery Interval (in seconds): 1

Set Parameters

Click on the button to configure the Initial Parameters.

Click on the button to configure the Rediscovery process.

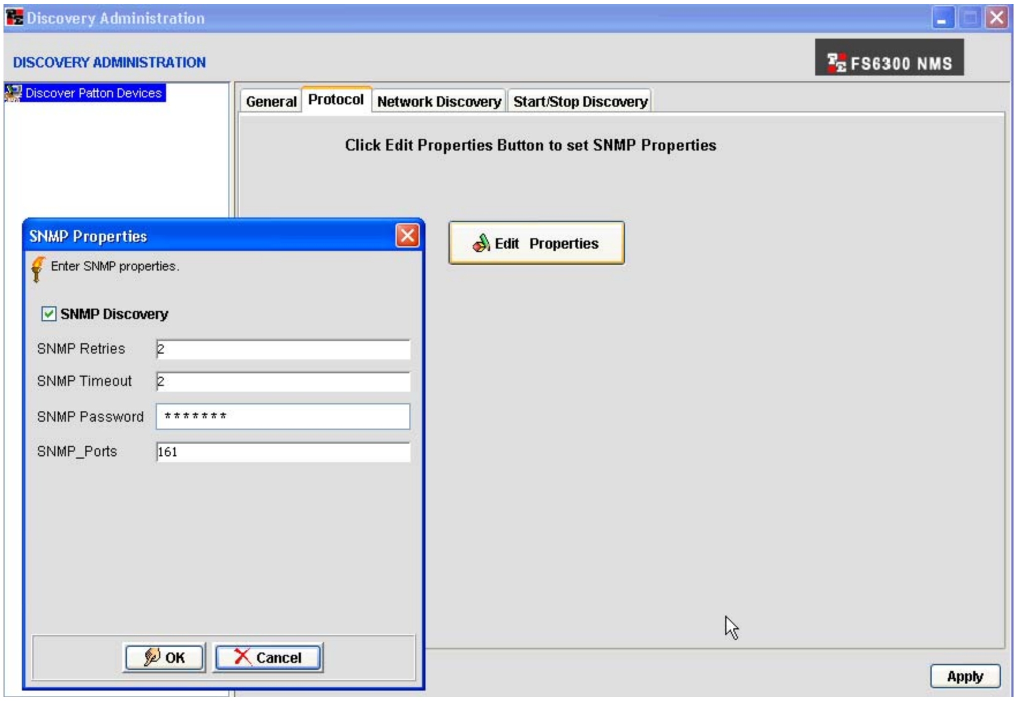
Figure 17. Set Discovery Interval

3. Click **Apply**.

Configuring Discovery of SNMP Devices

SNMPdevices may not be discovered through the default discovery process. To enable discovery of SNMP devices:

1. Click on **Tools** > **Discovery Administration** at the top of the screen. Then, click on **Discover Patton Devices** in the menu tree of the Discovery window.
2. Click on the **Protocol** tab, then click the **Edit Properties** button. The **SNMP Properties** window opens.



Click Edit Properties Button to set SNMP Properties

Enter SNMP properties.

☑ SNMP Discovery

SNMP Retries 2

SNMP Timeout 2

SNMP Password *******

SNMP_Ports 161

Figure 18. Configure Discovery for SNMP Devices

3. Enter information for the following parameters:

- **SNMP Discovery:** Select the checkbox to enable or disable discovery of SNMP devices.
- **SNMP Retries:** Specify the number of times the system will attempt to query the device if it does not respond to the first query.
- **SNMP Timeout:** Specify how many seconds the system will wait for a response before attempting to contact the device again.
- **SNMP Password:** Enter your password for configuring the SNMP device.
- **SNMP Ports:** Specify the ports to use to communicate with the SNMP agents.

4. Click **OK** to close the SNMP Properties window. Then, click **Apply** to save your changes to the server.

Adding a Device Manually

To add a single device to the NMS database:

1. Click on **SetUp(F)** > **Add Device** at the top of the screen.

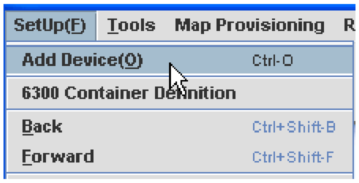
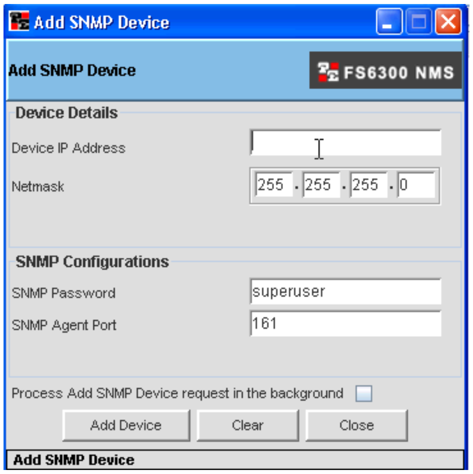


Figure 19. SetUp > Add Device

2. The **Add SNMP Device** window displays.



Device Details

Device IP Address:

Netmask: 255 . 255 . 255 . 0

SNMP Configurations

SNMP Password: superuser

SNMP Agent Port: 161

Process Add SNMP Device request in the background □

Figure 20. Add SNMP Device

Enter information for the following fields:

– **Device IP Address:** Enter the IP address of the device you want to add.

– **Netmask:** Enter the netmask for the device IP address. Default = 255.255.255.0

– **SNMP Password:** Enter the password to access the device.

– **SNMP Agent Port:** Enter the port number where the SNMP Agent is running. Default = 161

– **Process Add SNMP Device request in the background:** Select this box if you want continue with other operations in the NMS while the discovery process for the device runs in the background.

3. Click **Add Device**. If the device has been added to the system previously, a message will display that the node already exists in the database.

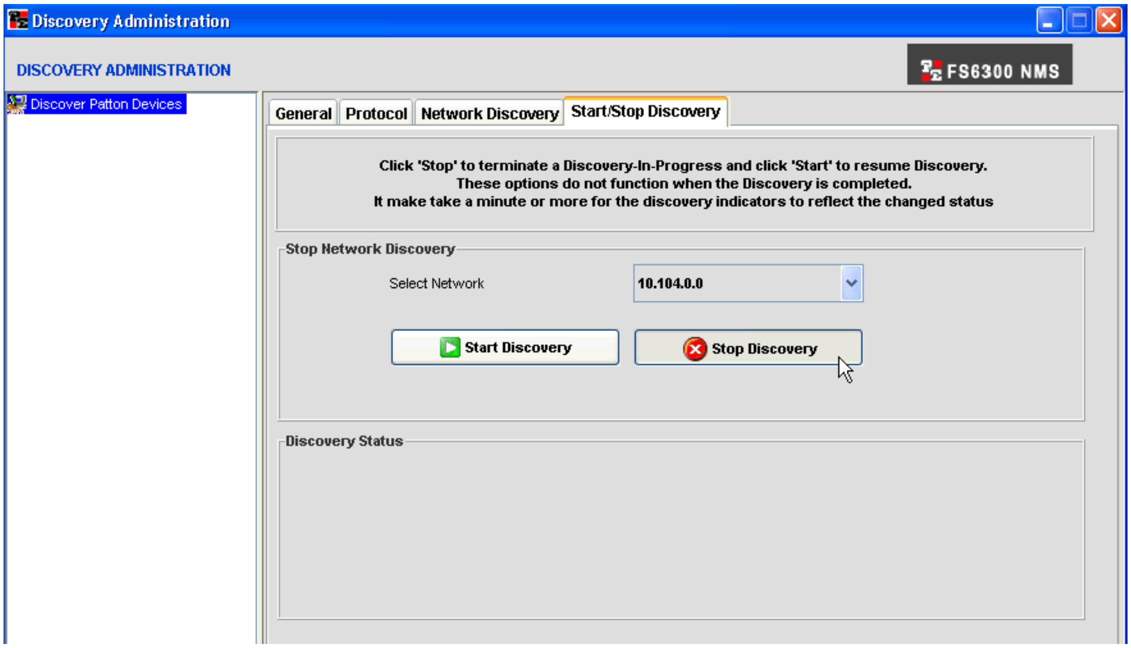
Stopping/Restarting a Discovery Process

You may want to stop a discovery cycle that is already in process to add or modify a network or set of devices.

Note You cannot use the stop/restart discovery feature if the discovery process has already completed. This feature is only for discovery cycles that are in progress.

To stop/restart a discovery in progress:

1. Click on **Tools** > **Discovery Administration** at the top of the screen. Then, click on **Discover Patton Devices** in the menu tree of the Discovery window.
2. Click on the **Start/Stop Discovery** tab. **Select the network** that you want to edit from the drop-down menu. If the network is able to be paused in the discovery process, the **Start Discovery** and **Stop Discovery** buttons will be lit.



Click 'Stop' to terminate a Discovery-In-Progress and click 'Start' to resume Discovery.
These options do not function when the Discovery is completed.
It make take a minute or more for the discovery indicators to reflect the changed status

Select Network: 10.104.0.0

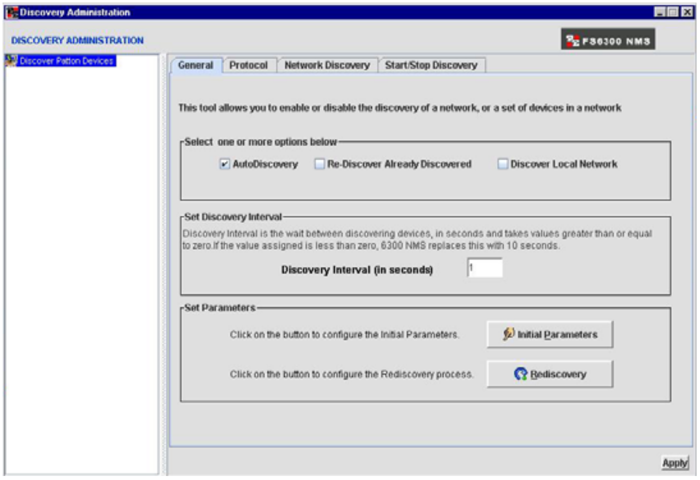
Figure 21. Stop Discovery in progress

3. A message will display in the **Discovery Status** area that discovery is currently disabled for the network.
4. Make the desired changes in the **Network Discovery** and/or **Protocol** tabs and click **Apply**.
5. Return to the **Start/Stop Discovery** tab. Select the network from the drop-down mneu and click **Start Discovery**. The discovery process will continue.

Re-Discovering Already Discovered Devices

By default, the rediscovery process discovers only devices that were not discovered previously. It does not rediscover the already discovered devices. To rediscover already discovered devices:

1. Click on **Tools** > **Discovery Administration** at the top of the screen. Then, click on **Discover Patton Devices** in the menu tree of the Discovery window.
2. Click on the **General** tab, then select the checkbox for **Re-Discover Already Discovered.** By default, this option is disabled.



This tool allows you to enable or disable the discovery of a network, or a set of devices in a network

Select one or more options below

☑ AutoDiscovery ☐ Re-Discover Already Discovered ☐ Discover Local Network

Set Discovery Interval

Discovery Interval is the wait between discovering devices, in seconds and takes values greater than or equal to zero.If the value assigned is less than zero, 6300 NMS replaces this with 10 seconds.

Discovery Interval (in seconds) 1

Set Parameters

Click on the button to configure the Initial Parameters.

Click on the button to configure the Rediscovery process.

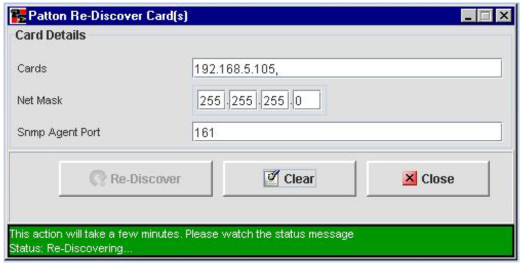
Figure 22. Re-Discover Already Discovered

3. Click **Apply**. This change will take place the next time the NMS goes through the re-discovery process. (See "Scheduling Rediscovery" on page 39).

Re-Discovering Cards Manually

You should re-discover cards after changing a card's configuration, or if you have added a new chassis or devices to the network. To manually re-discover cards:

1. Right-click on the device icon. You can do this in the Geographical Area, Network Node, Chassis, or Card sections of Network Maps.
2. Select **Re-Discover Cards** from the pull-down menu.A window displays with information about the card(s), including IP address, netmask, and SNMP Agent port.
3. Click **Re-Discover**. A message displays at the bottom of the box: "This action will take a few minutes. Please watch the status message. Status: Re-discovering..."



Card Details

Cards 192.168.5.105,

Net Mask 255 . 255 . 255 . 0

Snmp Agent Port 161

This action will take a few minutes. Please watch the status message
Status: Re-Discovering...

Figure 23. Re-Discover Cards

Scheduling Rediscovery

You can configure and schedule how often the network goes through the re-discovery process. The rediscovery process can also be configured to run at a specific hour on a specified date of the month or specified day of the week.

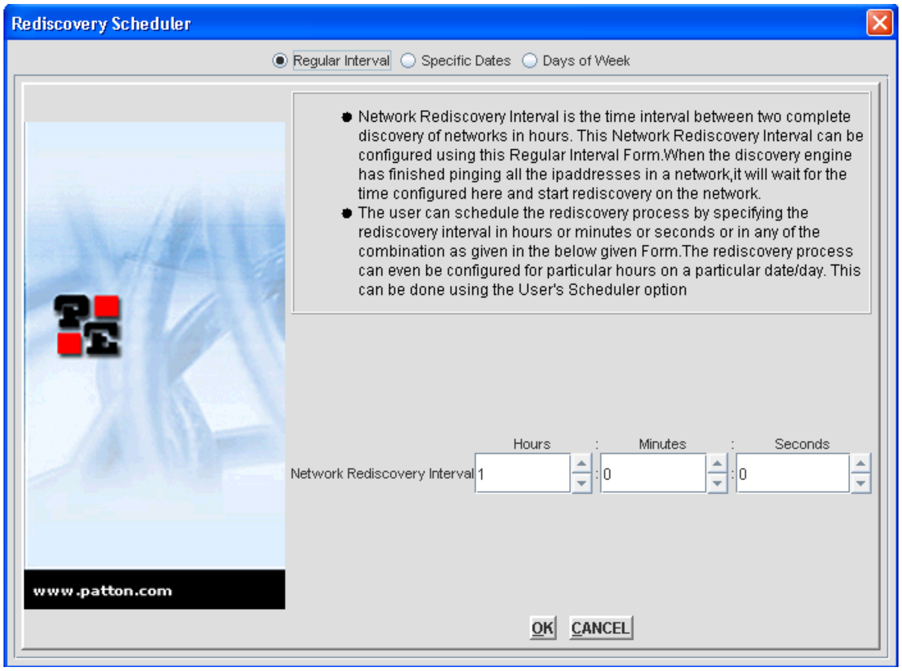
You can set the Rediscovery Interval using one of the following options:

- Regular Interval
- Specific Dates
- Days of the Week

Regular Interval

To schedule re-discovery for a regular interval (for example, every 24 hours):

1. Click on **Tools** > **Discovery Administration** at the top of the screen. Then, click on **Discover Patton Devices** in the menu tree of the Discovery window.
2. Click on the **General** tab, then click the **Rediscovery** button. The **Rediscovery Scheduler** window opens.



- Network Rediscovery Interval is the time interval between two complete discovery of networks in hours. This Network Rediscovery Interval can be configured using this Regular Interval Form.When the discovery engine has finished pinging all the ipaddresses in a network,it will wait for the time configured here and start rediscovery on the network.
- The user can schedule the rediscovery process by specifying the rediscovery interval in hours or minutes or seconds or in any of the combination as given in the below given Form.The rediscovery process can even be configured for particular hours on a particular date/day. This can be done using the User's Scheduler option

	Hours	:	Minutes	:	Seconds
Network Rediscovery Interval	1	:	0	:	0

Figure 24. Schedule Re-Discovery for Regular Intervals

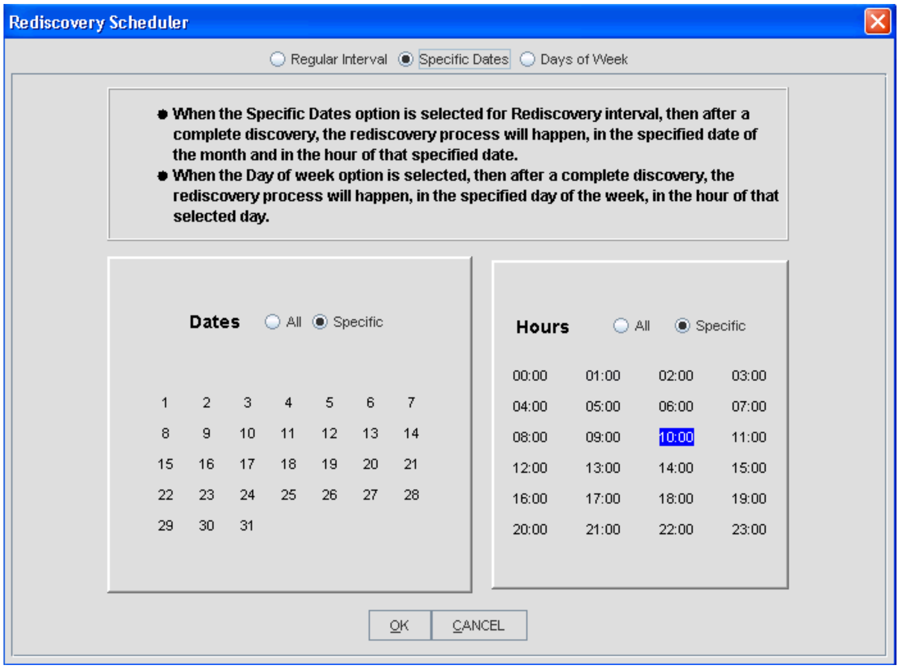
3. Select the **Regular Interval** radio button at the top of the window.
4. Specify the rediscovery interval in Hours, Minutes, and Seconds. By default, the interval is set as 24 hours. You can set any value from 1 to 24 in the hours field.
5. Click **OK.**

Note If the Rediscovery Interval is set using Regular Interval option, then the values set for Specific Dates and Days of Week options will not take effect.

Specific Dates

To set rediscovery on specific dates:

1. Click on **Tools** > **Discovery Administration** at the top of the screen. Then, click on **Discover Patton Devices** in the menu tree of the Discovery window.
2. Click on the **General** tab, then click the **Rediscovery** button. The **Rediscovery Scheduler** window opens.



Rediscovery Scheduler

○ Regular Interval ● Specific Dates ○ Days of Week

- When the Specific Dates option is selected for Rediscovery interval, then after a complete discovery, the rediscovery process will happen, in the specified date of the month and in the hour of that specified date.
- When the Day of week option is selected, then after a complete discovery, the rediscovery process will happen, in the specified day of the week, in the hour of that selected day.

Dates ○ All ● Specific

1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

Hours ○ All ● Specific

00:00	01:00	02:00	03:00
04:00	05:00	06:00	07:00
08:00	09:00	10:00	11:00
12:00	13:00	14:00	15:00
16:00	17:00	18:00	19:00
20:00	21:00	22:00	23:00

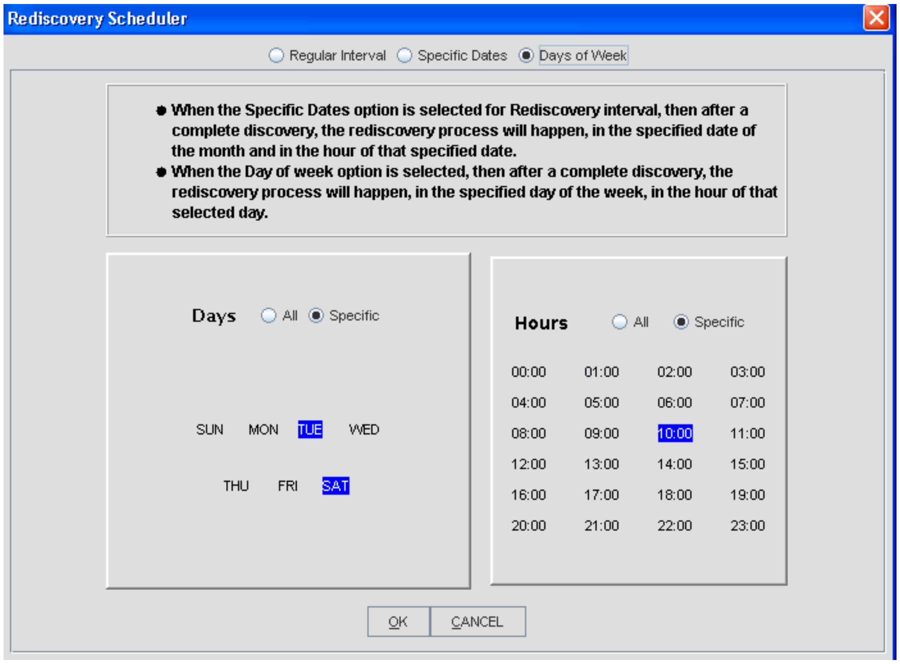
Figure 25. Schedule Re-Discovery for Specific Dates

3. Select the **Specific Dates** radio button at the top of the window.
4. Select the dates that you want re-discovery to occur:
   - **All Dates:** Select the radio button for **All**. Re-Discovery will occur every day.
   - **Specific Dates**: Select the radio button for **Specific**. Then, click on all of the dates in the month that you want re-discovery to occur. For example, if you select 5 and 15, then the rediscovery will take place on the 5th and 15th of every month.
5. Select hours for the selected dates:
   - **All Hours:** Select the radio button for **All** for re-discovery to occur every hour on the specified date(s).
   - **Specific Hours:** Select the radio button for **Specific.** Then, click on all of the hours that you want re-discovery to take place on the specified date(s).
6. Click **OK**.

Days of the Week

To set re-discovery on specific days:

1. Click on **Tools** > **Discovery Administration** at the top of the screen. Then, click on **Discover Patton Devices** in the menu tree of the Discovery window.
2. Click on the **General** tab, then click the **Rediscovery** button. The **Rediscovery Scheduler** window opens.



Rediscovery Scheduler

○ Regular Interval ○ Specific Dates ● Days of Week

- When the Specific Dates option is selected for Rediscovery interval, then after a complete discovery, the rediscovery process will happen, in the specified date of the month and in the hour of that specified date.
- When the Day of week option is selected, then after a complete discovery, the rediscovery process will happen, in the specified day of the week, in the hour of that selected day.

Days ○ All ● Specific

SUN MON [✓ TUE] WED

THU FRI [✓ SAT]

Hours ○ All ● Specific

00:00 01:00 02:00 03:00
04:00 05:00 06:00 07:00
08:00 09:00 [✓ 10:00] 11:00
12:00 13:00 14:00 15:00
16:00 17:00 18:00 19:00
20:00 21:00 22:00 23:00

Figure 26. Schedule Re-Discovery for Days of the Week

3. Select the **Days of the Week** radio button at the top of the window.
4. Select the day(s) that you want re-discovery to occur:
   - – **All Days:** Select the radio button for **All**. Re-Discovery will occur every day.
   - – **Specific Days:** Select the radio button for **Specific**. Then, click on all of the days of the week that you want re-discovery to occur. For example, if you select MON TUES WED, the re-discovery occurs only on those days, every week.
5. Select hours for the selected days:
   - – **All Hours:** Select the radio button for **All** for re-discovery to occur every hour on the specified day(s).
   - – **Specific Hours:** Select the radio button for **Specific.** Then, click on all of the hours that you want re-discovery to take place on the specified day(s).
6. Click **OK**.

Note When both dates and days are configured, then the **Specific Dates** settings will take place and the Days of the Week settings will be ignored.

Configuring Multiple Cards

If you have separate subnets that are supposed to be in the same Geographical Area but in a specifically named Node and Chassis, you will want to update the subnet information so that is displayed as it actually is located in the network.

Updating the Configuration

To configure multiple cards:

1. Select **Tools** from the menu at the top of the screen, then **Multiple Card Configuration**. The Multiple Card Configuration window appears.

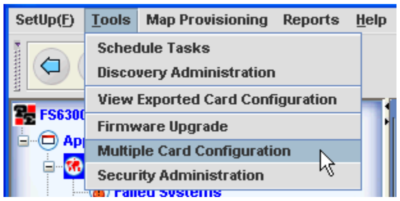
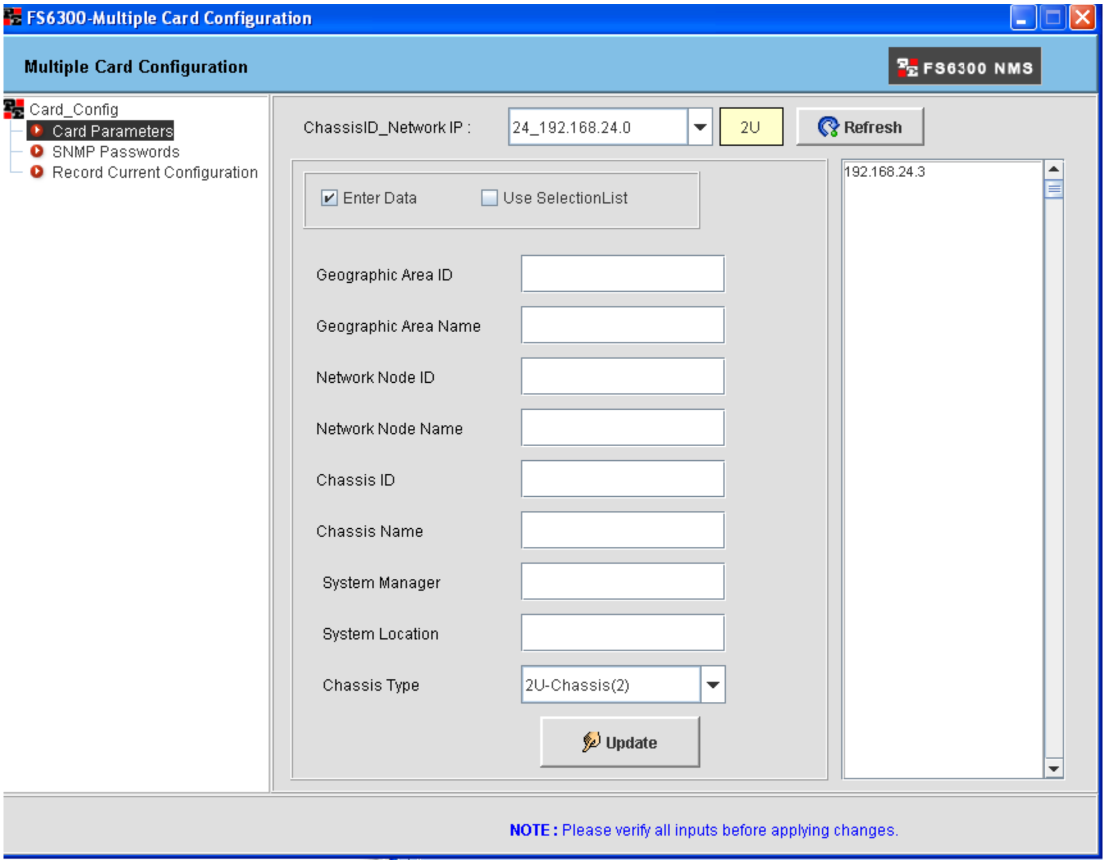


Figure 27. Tools > Multiple Card Configuration

2. Click on **Card Parameters** in the menu tree on the left side of the screen.



ChassisID_Network IP : 24_192.168.24.0 2U

☑ Enter Data ☐ Use SelectionList

Chassis Type 2U-Chassis(2)

192.168.24.3

NOTE : Please verify all inputs before applying changes.

Figure 28. Multiple Card Configuration > Card Parameters

3. Select the subnet you would like to update from the **Network IP** drop-down menu. The list on the right side of the screen shows the IP addresses of all the devices discovered on that specific subnet.

4. Enter the information you would like to update on the subnet for the following fields:
   – Geographical Area ID (Integer that identies the geographical area)
   – Geographical Area Name (Descriptive name of the geographical area)
   – Network Node ID (Integer used to identify the node on the network)
   – Network Node Name (Descriptive name of the node)
   – Chassis ID (Integer used to identify the chassis on the network)
   – Chassis Name (Descriptive label for the chassis)
   – System Manager (Name of the person managing this subnet on the network)
   – System Location (Description of where the system is located)
   – Chassis Type (Choose a chassis type from the drop-down menu)

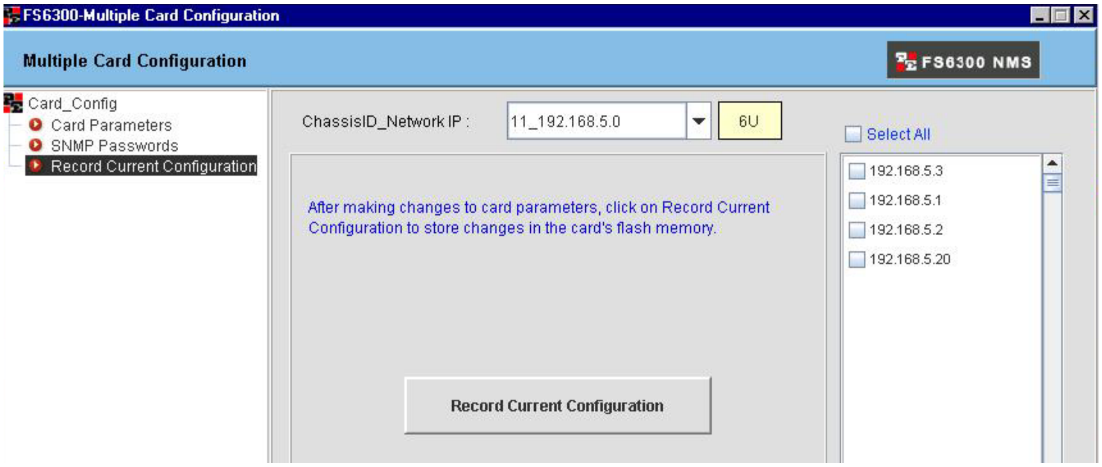
5. Click **Update** to save the information for all of the cards on that subnet.

Note After clicking Update, it is very important to save this information in the cards' non-volatile memory so that the values will not be lost in case of a power failure or card reboot.

Saving the Configuration

To save the information to non-volatile memory:

1. Click on **Record Current Configuration** in the menu tree on the left side of the screen. This will save all current configurations in non-volatile memory for the devices listed in the panel on the right side of the screen.


FS6300-Multiple Card Configuration
Multiple Card Configuration
FS6300 NMS
Card_Config
Card Parameters
SNMP Passwords
Record Current Configuration
□ Select All
Record Current Configuration

ChassisID_Network IP : 11_192.168.5.0 6U

After making changes to card parameters, click on Record Current Configuration to store changes in the card's flash memory.

□ 192.168.5.3
□ 192.168.5.1
□ 192.168.5.2
□ 192.168.5.20

Figure 29. Multiple Card Configuration > Record Current Configuration

Forcing Discovery for Selected Cards

Though the cards have the updated information saved, the NMS will not display the changes until the cards have been re-discovered. To re-discover specific cards and not the entire subnet, see "Re-Discovering Cards Manually" on page 38.

Upgrading Firmware

The FS6300 NMS supports the following Patton models:

Supported Rack Cards	Supported CPE Devices
6511	3201
3196RC	3088
3096RC	3086
2616RC	1082 (C/D/I/F)

The rack cards must have the following minimum firmware version installed in order to operate properly:

Card	Minimum Firmware Version Required
6511	6511RC-1.2.9.img
3196RC	3196RC-1.3.9.img
3096RC	3096RC-1.5.16.img
2616RC	2616RC-1.3.9.img

To update the firmware for a rack card:

1. Click on **Tools** > **Firmware Upgrade** at the top of the screen.

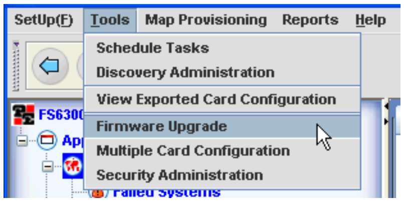
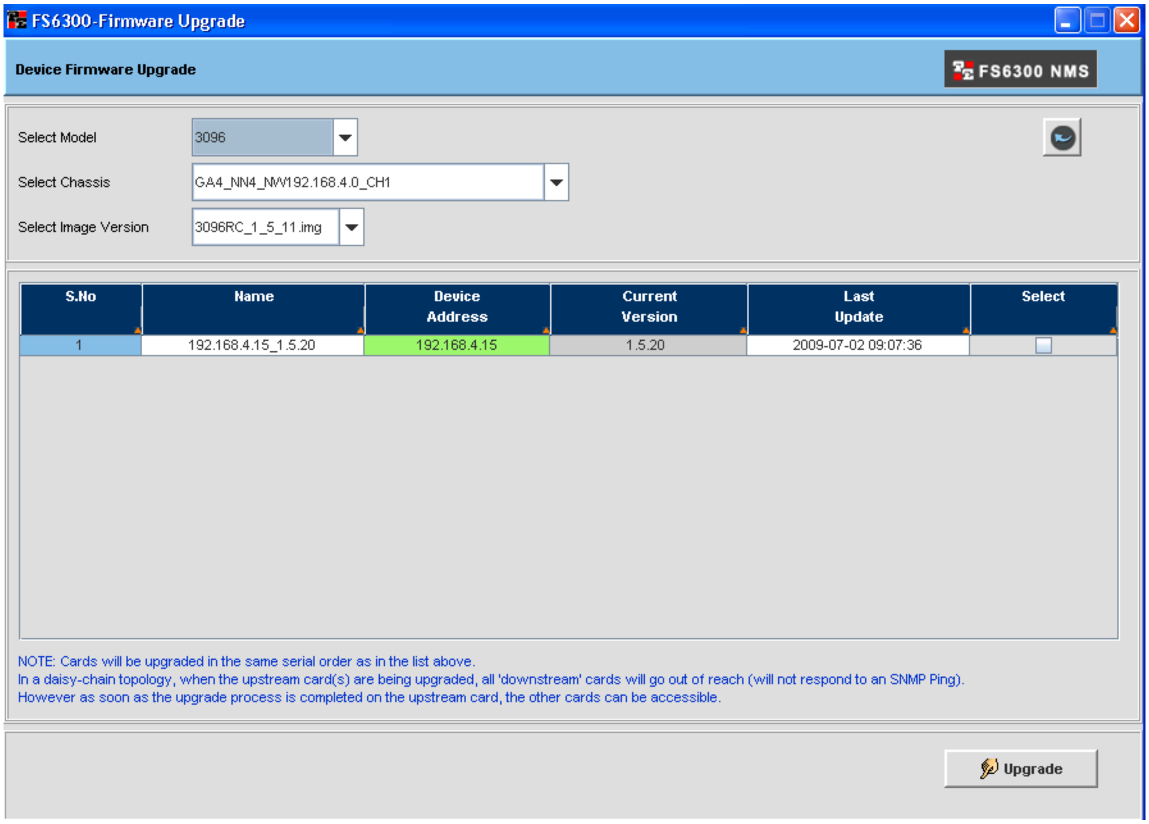


Figure 30. Tools > Firmware Upgrade

2. The **FS6300 Firmware Upgrade** window displays.



Select Model 3096

Select Chassis GA4_NN4_NW192.168.4.0_CH1

Select Image Version 3096RC_1_5_11.img

S.No	Name	Device Address	Current Version	Last Update	Select
1	192.168.4.15_1.5.20	192.168.4.15	1.5.20	2009-07-02 09:07:36	□

NOTE: Cards will be upgraded in the same serial order as in the list above.
In a daisy-chain topology, when the upstream card(s) are being upgraded, all 'downstream' cards will go out of reach (will not respond to an SNMP Ping).
However as soon as the upgrade process is completed on the upstream card, the other cards can be accessible.

Figure 31. Firmware Upgrade window

3. Select the desired **Model**, **Chassis**, and **Image Version** from the drop-down menus. Available cards will display in the firmware table.

4. **Select the checkbox** in the table for the card(s) you want to upgrade.

Note The NMS will upgrade the cards in the same order that they are listed in the table. In a daisy-chain topology, when the upstream card(s) are being upgraded, all “downstream” cards will be temporarily unavailable and will not respond to an SNMP ping request. However, the other cards will be accessible as soon as the upgrade is completed for the upstream card.

5. Click **Upgrade**.

Chapter 3 Configuring Alarms and Clocking

Chapter contents

Introduction

Before you can receive alarm indications, you must first configure the alarms and clocking for the NMS. When you discover your network for the first time, there will be alarms because the synchronization clocking has not been fully configured yet.

Configuring the Alarm Trap Manager

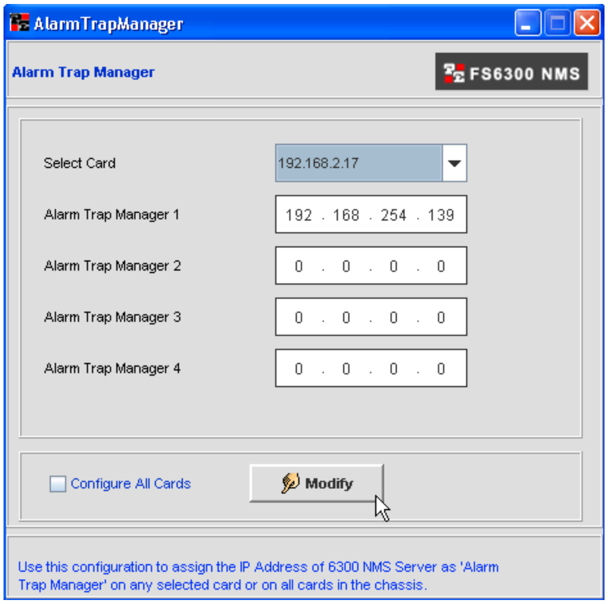
In order to configure alarms, you need to configure the IP address of the NMS server which traps the alarm reports from each of the cards in the network. By default, the Alarm Trap IP address is 0.0.0.0, so no alarms are detected by the NMS.

You can configure the Alarm Trap Manager in two different ways, by right-clicking on a network node in the Geographical Areas section, or by right-clicking on a card in the Chassis section.

Configuring Alarms through the Network Node

To configure the IP address for the Alarm Trap field for each card:

1. From the menu tree on the left side of the screen, select the **Geographical Area** for the node that you want to configure.
2. In the main window, right-click on the **Network Node**, then select **Alarm Trap Manager.**
   The **Configure Alarm Trap Manager** window dispalys. You may configure the Alarm Trap Manager for any particular card in the chassis' subnet or you can configure all of the cards in the subnet at once.



Select Card: 192.168.2.17

Alarm Trap Manager 1: 192 . 168 . 254 . 139

Alarm Trap Manager 2: 0 . 0 . 0 . 0

Alarm Trap Manager 3: 0 . 0 . 0 . 0

Alarm Trap Manager 4: 0 . 0 . 0 . 0

□ Configure All Cards

Use this configuration to assign the IP Address of 6300 NMS Server as 'Alarm Trap Manager' on any selected card or on all cards in the chassis.

Figure 32. Alarm Trap Manager

3. Select the card that you would like to configure from the **Select Card** drop-down menu. If you would like to configure all of the cards at the same time, select the **Configure All Cards** checkbox at the bottom of the screen.
4. Enter the IP address of the NMS server in the **Alarm Trap Manager 1** field.

5. Click the **Modify** button.

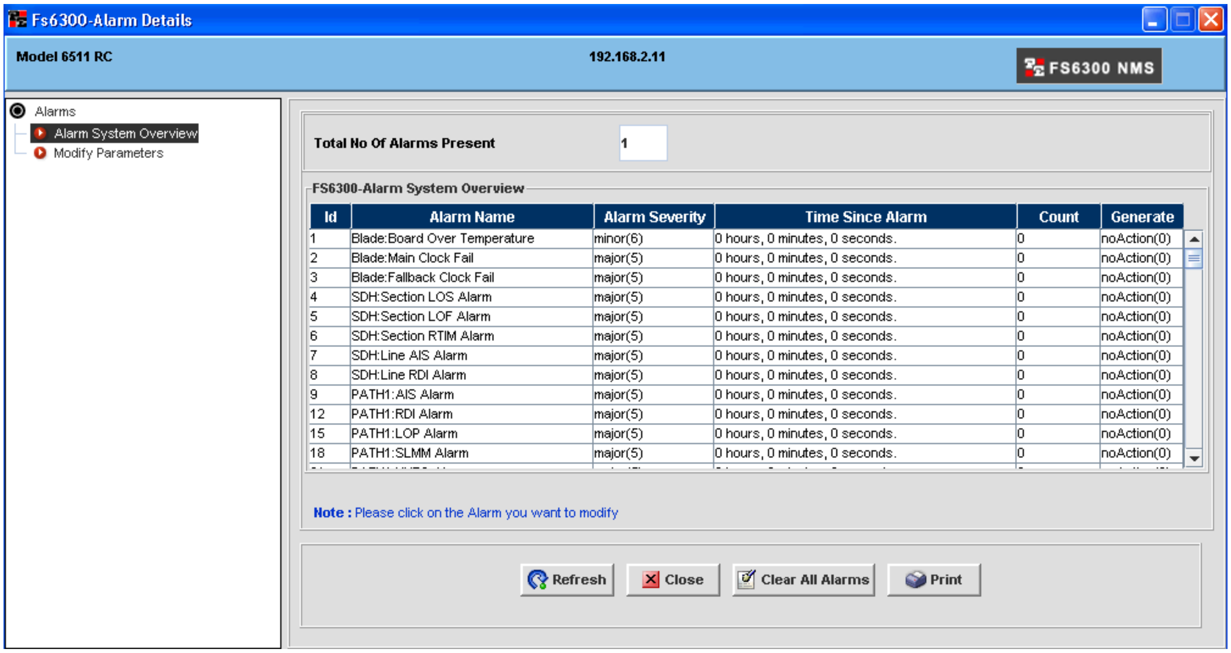
6. If the configuration was successful, a “Configuration Result” window displays. Click **OK**.

Configuring Alarms through a Card in the Chassis

To configure the IP address for the Alarm Trap field for each card:

1. From the menu tree on the left side of the screen, select the **Chassis** for the card that you want to configure.

2. In the main window, right-click on the **Card**, then select **Alarm Parameter Configuration.**
   The **FS6300 Alarm Details** window appears. Click on the **Alarm System Overview** to view information about the alarms.



Model 6511 RC

192.168.2.11

Total No Of Alarms Present: 1

FS6300-Alarm System Overview

Id	Alarm Name	Alarm Severity	Time Since Alarm	Count	Generate
1	Blade:Board Over Temperature	minor(6)	0 hours, 0 minutes, 0 seconds.	0	noAction(0)
2	Blade:Main Clock Fail	major(5)	0 hours, 0 minutes, 0 seconds.	0	noAction(0)
3	Blade:Fallback Clock Fail	major(5)	0 hours, 0 minutes, 0 seconds.	0	noAction(0)
4	SDH:Section LOS Alarm	major(5)	0 hours, 0 minutes, 0 seconds.	0	noAction(0)
5	SDH:Section LOF Alarm	major(5)	0 hours, 0 minutes, 0 seconds.	0	noAction(0)
6	SDH:Section RTIM Alarm	major(5)	0 hours, 0 minutes, 0 seconds.	0	noAction(0)
7	SDH:Line AIS Alarm	major(5)	0 hours, 0 minutes, 0 seconds.	0	noAction(0)
8	SDH:Line RDI Alarm	major(5)	0 hours, 0 minutes, 0 seconds.	0	noAction(0)
9	PATH1:AIS Alarm	major(5)	0 hours, 0 minutes, 0 seconds.	0	noAction(0)
12	PATH1:RDI Alarm	major(5)	0 hours, 0 minutes, 0 seconds.	0	noAction(0)
15	PATH1:LOP Alarm	major(5)	0 hours, 0 minutes, 0 seconds.	0	noAction(0)
18	PATH1:SLMM Alarm	major(5)	0 hours, 0 minutes, 0 seconds.	0	noAction(0)

Note : Please click on the Alarm you want to modify

Figure 33. View Alarm Details

Alarm System Overview: The Alarm System Overview window shows the entire alarm system, including the following information for each alarm:

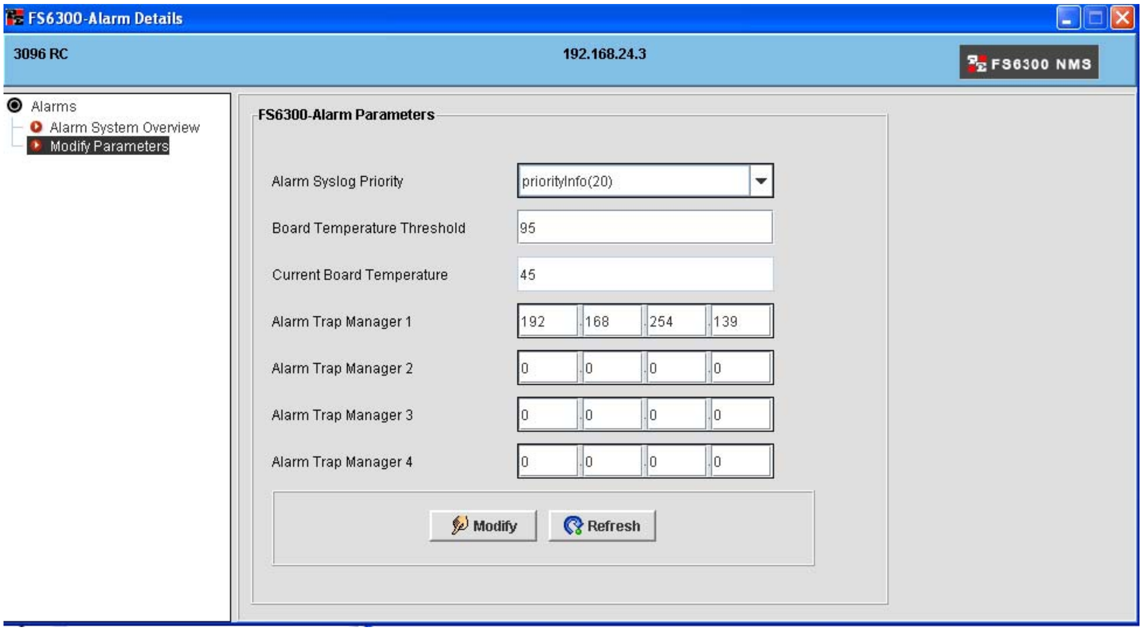
– Alarm Name

– Alarm Severity

– Time Since Alarm

– Count– the number of times this alarm has occurred since being cleared

3. Click on **Modify Parameters** to configure the alarms.



FS6300-Alarm Parameters

Alarm Syslog Priority: priorityInfo(20)

Board Temperature Threshold: 95

Current Board Temperature: 45

Alarm Trap Manager 1: 192.168.254.139

Alarm Trap Manager 2: 0.0.0.0

Alarm Trap Manager 3: 0.0.0.0

Alarm Trap Manager 4: 0.0.0.0

Figure 34. Modify Alarm Details

Modify Parameters: Configure the FS6300 Alarm Parameters through the Modify Parameters window.

– Alarm Syslog Priority

– Board Temperature Threshold

– Current Board Temperature

– Alarm Trap Managers 1-4

4. Click **Modify** to commit your configuration to the card. You will need to record the configuration to save it to the card's volatile memory. (See "Record the current configuration" on page 60).

5. Return to the **Alarm Systems Overview** screen. Before the most severe active alarm is propagated to the icons in the NMS, you must first do Steps 6-7.

6. Click on the **Clear All Alarms** button. You should receive a "Configuration Result" window indicating success.

7. Click on the **Refresh** button.

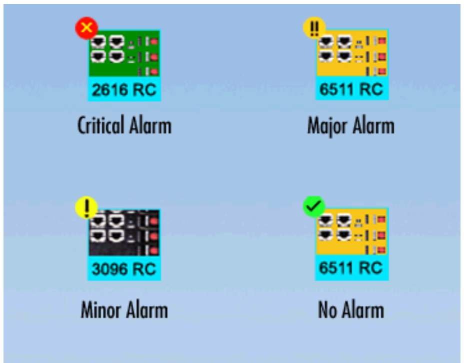
8. Close the Alarm Details window.

9. Repeat Steps 2-8 for each card in the chassis. After this is completed, return to the view of the chassis in the main NMS window.

Alarm Indications

The following are symbols that appear on a card or node icon when the NMS receives an alarm:

- **Critical:** Red circle with a yellow “X”
- **Major:** Orange circle with two black exclamation points
- **Minor:** Yellow circle with a single black exclamation point
- **No Alarm/Informational:** Green circle with black checkmark



Alarms are propagated up to the next level throughout the **Network Maps** section in the menu tree.The **Chassis** icon indicates an alarm alert if one or more of the cards have an alarm. On the **Geographical Area** level, a network node will also display alarm alerts if a card in a chassis has an alarm.

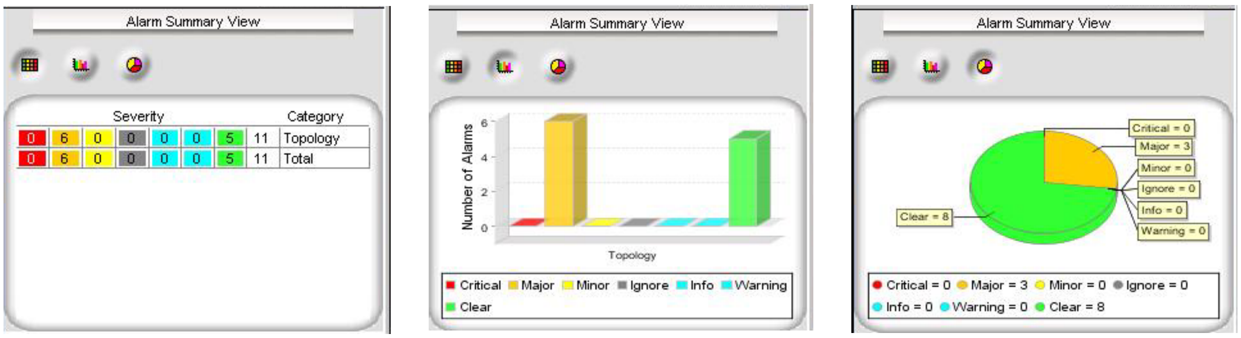
Viewing Alarms

Viewing a Summary of Alarms

To view a summary of all systems with an alarm, click on **Failed Systems** (under Network Maps) in the menu tree on the left side of the screen. The Failed Systems map shows all the cards that have alarm alerts.

The **Alarm Summary View** window always appears in the bottom left corner of the screen under the main menu tree. It offers a quick glance at the status of alarms that are currently occurring in the system. You can change how the Alarm Summary View is displayed by clicking on the icons in the Alarm Summary View window. There are three different view options:

- Tabular View
- Graphical View
- Pie Chart View


Alarm Summary View

Severity								Category
0	6	0	0	0	0	5	11	Topology
0	6	0	0	0	0	5	11	Total

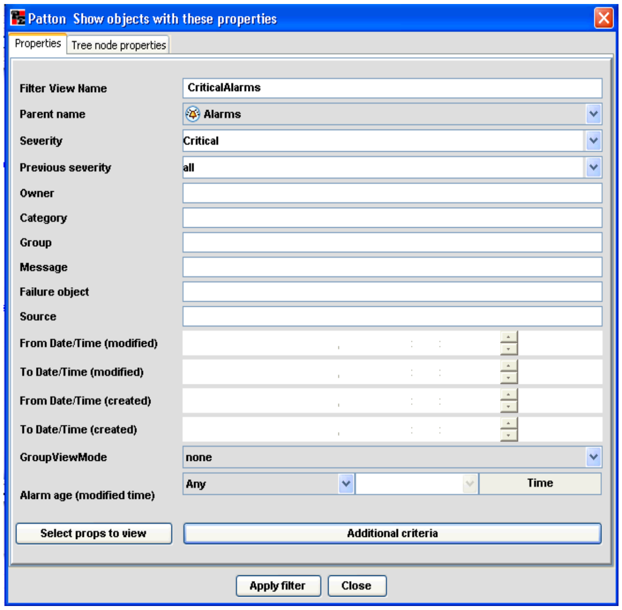
Figure 35. Alarm Summary View options (Tabular, Graphical, and Pie Chart)

Managing Alarm Custom Views

The NMS provides the ability to create custom views for specific alarms. Use custom views to display all alarms in a certain state or to view all alarms from one card or network.

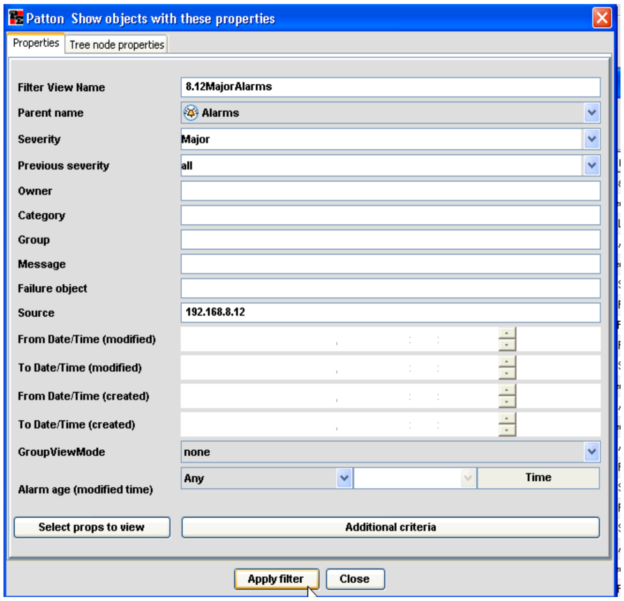
Adding an Alarm Custom View

1. From the menu tree on the left side of the screen, select **Alarms** under **Fault Management**.
2. Select **Custom View** > **Add Custom View** from the top of the screen. The object properties window displays.



Filter View Name	CriticalAlarms
Parent name	Alarms
Severity	Critical
Previous severity	all
Owner	
Category	
Group	
Message	
Failure object	
Source	
From Date/Time (modified)	
To Date/Time (modified)	
From Date/Time (created)	
To Date/Time (created)	
GroupViewMode	none
Alarm age (modified time)	Any Time

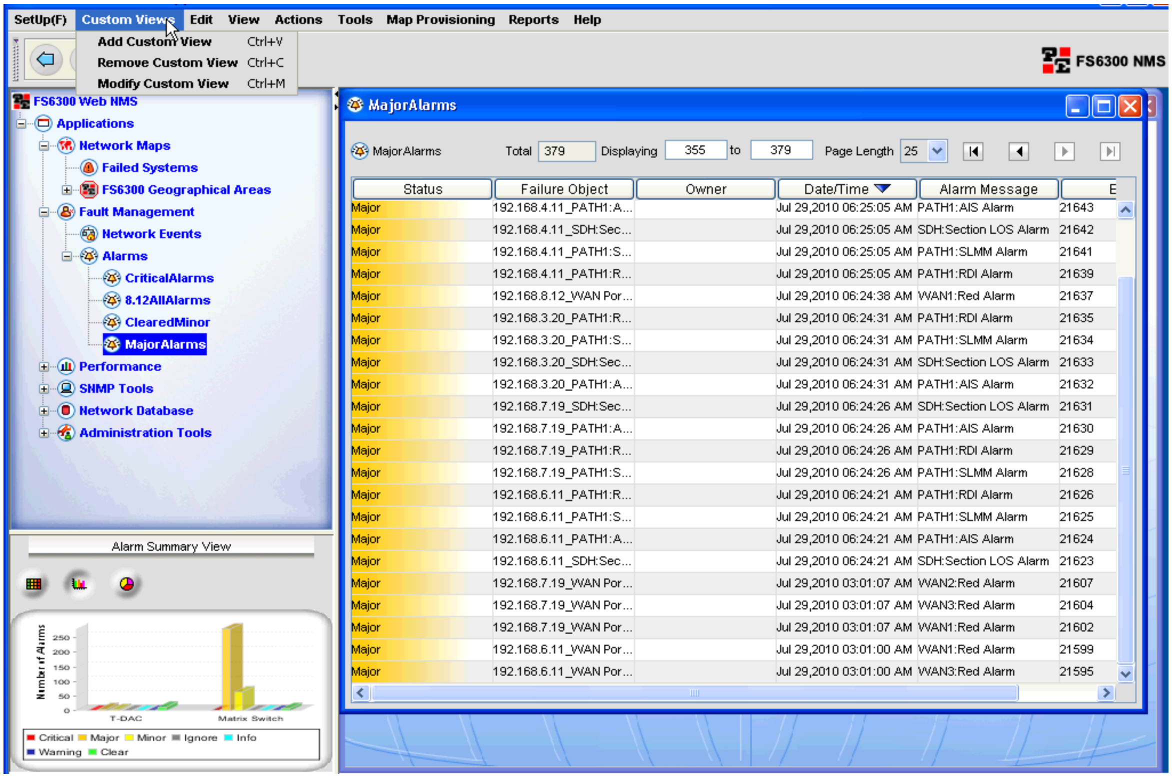
Figure 36. Example: Custom Alarm View for Critical Alarms



Filter View Name	8.12MajorAlarms
Parent name	Alarms
Severity	Major
Previous severity	all
Owner	
Category	
Group	
Message	
Failure object	
Source	192.168.8.12
From Date/Time (modified)	
To Date/Time (modified)	
From Date/Time (created)	
To Date/Time (created)	
GroupViewMode	none
Alarm age (modified time)	Any Time

Figure 37. Example: Custom Alarm View for Specific Card

3. Enter the desired criteria for the custom view, then click **Apply Filter**. The new table displays and the NMS will automatically include the custom view as a submenu item under **Alarms** in the main menu tree.



MajorAlarms Total 379 Displaying 355 to 379 Page Length 25

Status	Failure Object	Owner	Date/Time	Alarm Message	E
Major	192.168.4.11_PATH1:A...		Jul 29,2010 06:25:05 AM	PATH1:AIS Alarm	21643
Major	192.168.4.11_SDH:Sec...		Jul 29,2010 06:25:05 AM	SDH:Section LOS Alarm	21642
Major	192.168.4.11_PATH1:S...		Jul 29,2010 06:25:05 AM	PATH1:SLMM Alarm	21641
Major	192.168.4.11_PATH1:R...		Jul 29,2010 06:25:05 AM	PATH1:RDI Alarm	21639
Major	192.168.8.12_WAN Por...		Jul 29,2010 06:24:38 AM	WAN1:Red Alarm	21637
Major	192.168.3.20_PATH1:R...		Jul 29,2010 06:24:31 AM	PATH1:RDI Alarm	21635
Major	192.168.3.20_PATH1:S...		Jul 29,2010 06:24:31 AM	PATH1:SLMM Alarm	21634
Major	192.168.3.20_SDH:Sec...		Jul 29,2010 06:24:31 AM	SDH:Section LOS Alarm	21633
Major	192.168.3.20_PATH1:A...		Jul 29,2010 06:24:31 AM	PATH1:AIS Alarm	21632
Major	192.168.7.19_SDH:Sec...		Jul 29,2010 06:24:26 AM	SDH:Section LOS Alarm	21631
Major	192.168.7.19_PATH1:A...		Jul 29,2010 06:24:26 AM	PATH1:AIS Alarm	21630
Major	192.168.7.19_PATH1:R...		Jul 29,2010 06:24:26 AM	PATH1:RDI Alarm	21629
Major	192.168.7.19_PATH1:S...		Jul 29,2010 06:24:26 AM	PATH1:SLMM Alarm	21628
Major	192.168.6.11_PATH1:R...		Jul 29,2010 06:24:21 AM	PATH1:RDI Alarm	21626
Major	192.168.6.11_PATH1:S...		Jul 29,2010 06:24:21 AM	PATH1:SLMM Alarm	21625
Major	192.168.6.11_PATH1:A...		Jul 29,2010 06:24:21 AM	PATH1:AIS Alarm	21624
Major	192.168.6.11_SDH:Sec...		Jul 29,2010 06:24:21 AM	SDH:Section LOS Alarm	21623
Major	192.168.7.19_WAN Por...		Jul 29,2010 03:01:07 AM	WAN2:Red Alarm	21607
Major	192.168.7.19_WAN Por...		Jul 29,2010 03:01:07 AM	WAN3:Red Alarm	21604
Major	192.168.7.19_WAN Por...		Jul 29,2010 03:01:07 AM	WAN1:Red Alarm	21602
Major	192.168.6.11_WAN Por...		Jul 29,2010 03:01:00 AM	WAN1:Red Alarm	21599
Major	192.168.6.11_WAN Por...		Jul 29,2010 03:01:00 AM	WAN3:Red Alarm	21595

Figure 38. Alarm Custom Views

Modifying an Alarm Custom View

To modify an existing custom view:

1. Select the custom view in the menu on the left side of the screen.
2. Click **Custom Views** > **Modify Custom View** from the top of the screen.
3. Make the desired changes, then click **Apply Filter**.

Deleting an Alarm Custom View

To remove an existing custom view:

1. Select the custom view in the menu on the left side of the screen.
2. Click **Custom Views** > **Remove Custom View** from the top of the screen.
3. A confirmation message displays. Click **Yes** to delete the custom view.

Configuring Clocking Synchronization

To configure clocking synchronization for a chassis:

1. From the menu tree on the left side of the screen, select **Node** (under Geographical Area).
2. In the main window, right-click on the chassis that you want to configure clocking for.
3. Select **Chassis Clocking Synchronization** from the pull-down menu.

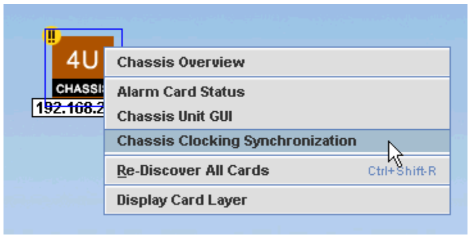
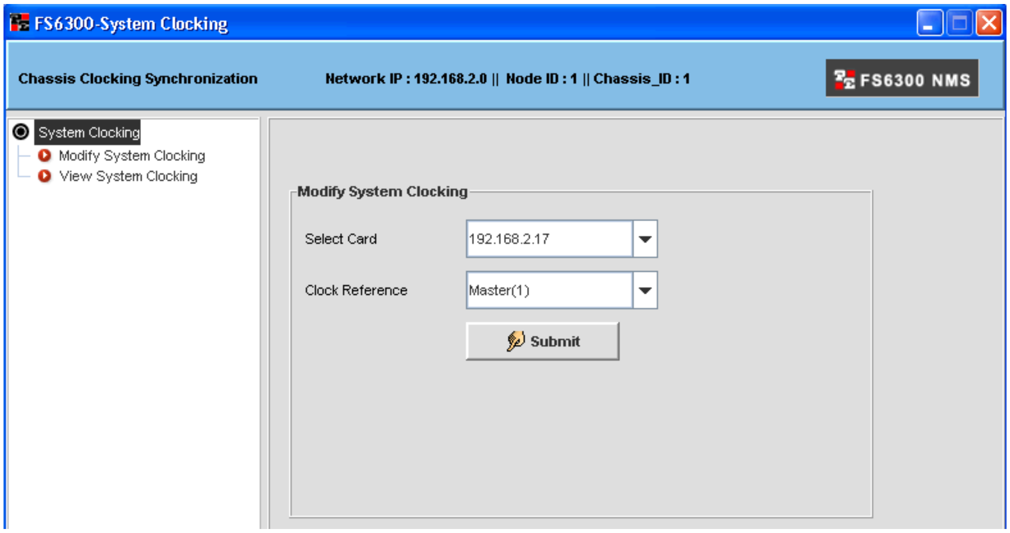


Figure 39. Chassis Menu > Chassis Clocking Sync

The **Chassis Clocking Synchronization** window displays.



Chassis Clocking Synchronization   Network IP : 192.168.2.0 || Node ID : 1 || Chassis_ID : 1

Modify System Clocking

Select Card: 192.168.2.17

Clock Reference: Master(1)

Figure 40. Modify System Clocking

4. Select **Modify System Clocking** from the menu tree on the left side of the screen.
5. Select a card from the **Select Card** drop-down menu, and select a clock from the **Clock Reference** drop-down menu. The Clock Reference can be **Master**(1), **Secondary**(2), or **Slave**(3). Click **Submit**.
6. Repeat Step 5 for each card in the chassis.

Note A chassis can have only one master and one secondary, so if you accidentally select another master in the same chassis, the NMS will not allow you to save the clock for that card as the Master.

Refreshing the alarms after configuring clocking

After you have configured clocking for the chassis, you can refresh the alarms that occurred before clocking was configured. To refresh the alarms for a card:

1. Right-click on the card icon and select **Alarm Parameter Configuration**.
   The **FS6300 Alarm Details** window displays (see Figure 33 on page 48).
2. Click on **Alarm System Overview** in the menu tree on the left side of the screen.
3. Click the **Clear All Alarms** button.
4. Click the **Refresh** button.

All of the alarms that were related to clocking should be cleared. (Other alarms not related to clocking may still be present). The next step after configuring clocking synchronization is to configure clocking options for the card system, including Clock Fallback and Clock Auto Recover.

Configuring Card System Clocking

In addition to setting a clock to Master, Secondary, or Slave, you must also select the source for clocking and determine whether to enable or disable Clock Fallback and Clock Auto Recover. To configure card system clocking:

1. Right-click on the card icon and select **Card System Clocking**.

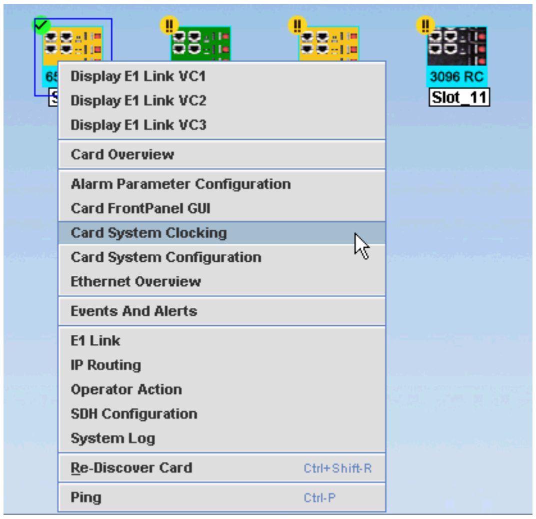
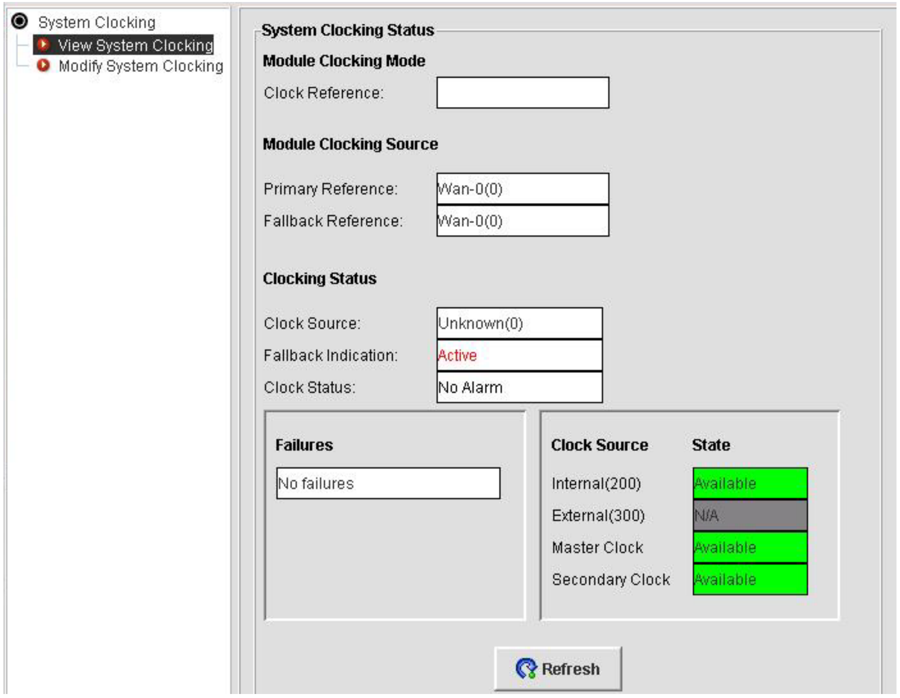


Figure 41. Card Menu > Card System Clocking

The **System Clocking** window displays.

2. Click on **View System Clocking** in the menu tree on the left side of the screen. From this window, you can view and verify the configuration settings for the card's entire clocking system, including whether any failures have occurred and if any clock-related alarms are active.



System Clocking Status

Module Clocking Mode

Clock Reference:

Module Clocking Source

Primary Reference: Wan-0(0)
Fallback Reference: Wan-0(0)

Clocking Status

Clock Source: Unknown(0)
Fallback Indication: Active
Clock Status: No Alarm

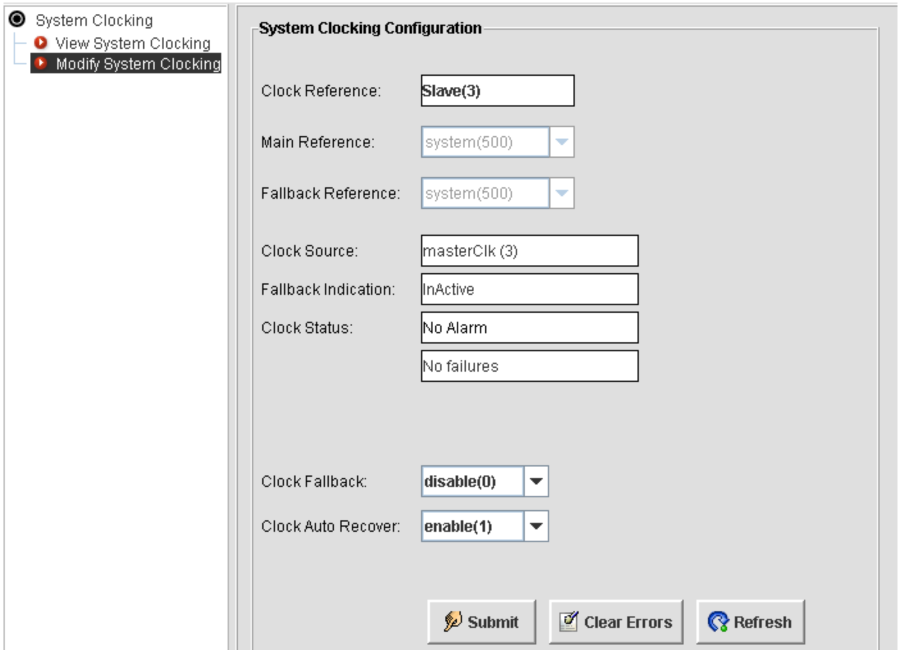
Failures

No failures

Clock Source	State
Internal(200)	Available
External(300)	N/A
Master Clock	Available
Secondary Clock	Available

Figure 42. View System Clocking

3. To change any of the card's clocking paramters, click on **Modify System Clocking** in the menu tree on the left side of the screen.



System Clocking Configuration

Clock Reference: Slave(3)
Main Reference: system(500)
Fallback Reference: system(500)

Clock Source: masterClk (3)
Fallback Indication: InActive
Clock Status: No Alarm
No failures

Clock Fallback: disable(0)
Clock Auto Recover: enable(1)

Figure 43. Modify System Clocking

Main Reference and Fallback Reference

The Main Reference and Fallback Reference parameters define a primary and secondary (fallback) reference for the card system clock source (and for all blades in the chassis when the card's clocking mode is defined as master). The card will use the fallback reference if and only if the main reference becomes unavailable.

When defining the main and fallback clocking sources, you can select a WAN port or the card's internal clock pulse oscillator. The card will use the main reference as its system clocking source unless the main reference fails or is disconnected.

When the main reference becomes unavailable, the card 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 card's fallback mechanism (see below). For the card's main and secondary clocking references, you can choose:

- • *wan(602)*—Clocking derived from the network clock received at the WAN interface.
- • *internal(200)*—Uses the card's internal free-running oscillator for the clock source.

Clock Fallback

Select to enable or disable the card's fallback feature. The fallback feature, when enabled, allows the card to switch to a secondary clock as follows:

- *Enable - Master or secondary mode*—The card, upon failure of the primary reference clock source, will switch to the selected fallback reference clock source.
- *Disable - Slave Mode*—The card 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.

Clock Auto Recover

Select to enable or disable the clock auto recover feature. The Auto Recovery Feature , when enabled, will cause a card (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.

When disabled, the card, operating on fallback reference clock, will not switch back to primary reference clock, even if the primary reference becomes available.

Click **Submit** to commit your changes. You will need to record the current configuration to save your changes to the card's volatile memory. (See "Record the current configuration" on page 60).

Chapter 4 Configuring and Managing Devices

Chapter contents

Introduction

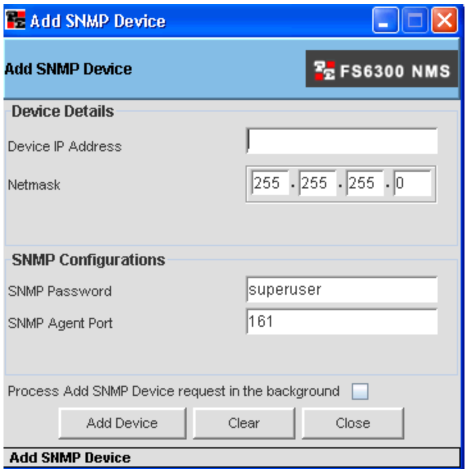
Devices can be individually configured and monitored through the FS6300 NMS. The NMS organizes devices by geographical area in the **Network Maps** section of the menu tree, where device-specific menus can be viewed by right-clicking on a device. Devices can also be monitored through the **Network Database** section of the menu tree.

This chapter describes what information you can find and configure about specific devices through the Network Maps and Network Database sections of the FS6300 NMS.

Adding Devices

To add individual devices to the FS6300 NMS:

1. Click **Setup**(F) at the top of the screen, then click **Add Device**(o).
   OR, press **Ctrl+O**. The **Add SNMP Device** window appears.



Add SNMP Device

Device Details

Device IP Address

Netmask 255 . 255 . 255 . 0

SNMP Configurations

SNMP Password superuser

SNMP Agent Port 161

Process Add SNMP Device request in the background □

Figure 44. Add SNMP Device window

2. Enter the **IP address** and **Netmask** of the device you want to add.
3. If desired, you may modify the **SNMP Password** and **SNMP Agent Port**.
4. If you don't want to monitor the status of your request to add this device to the system, select the checkbox for **Process Add SNMP Device request in the background**.
5. Click **Add Device**.

Working with Network Maps

The **Network Maps** section of the NMS shows a map of the devices located on the network at various levels.

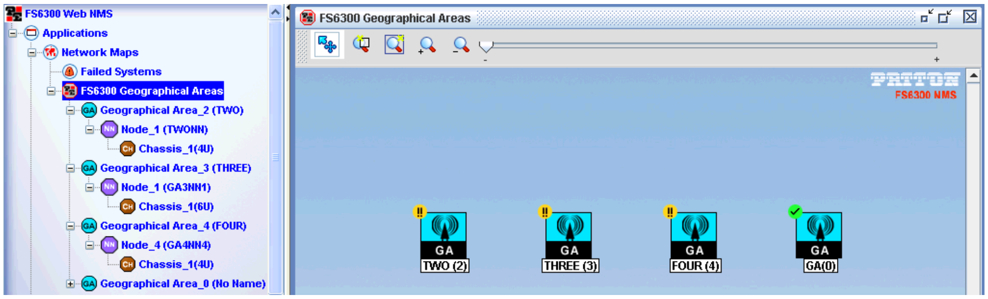


Figure 45. Network Maps

Geographical Areas

Click on a **Geographical Area** in the main menu tree to view a map of **Network Nodes** in the NMS.

Right-click on the icon of a **Network Node** in the main window to view a pull-down menu of options.

Nodes

Click on a **Network Node** in the main menu tree to view a map of **Chassis** in that node.

Right-click on the icon of a **Chassis** in the main window to view a pull-down menu of options..

Chassis

Click on a **Chassis** in the main menu tree to view a map of **Devices** in that chassis.

Right-click on the icon of a **Device** in the main window to view a pull-down menu of options..

Slots/Devices

Click on a **Device** in the main menu tree to view a map of **Ports** in that device.

Right-click on the icon of a **Port** in the main window to view a pull-down menu of options.

Ports/Interfaces

Right-click on a port to configure its link or set it to be managed or unmanaged.

Note For details on adding containers, see "Defining Containers" on page 25. Figure 46 shows a visual representation of container IDs in the NMS.

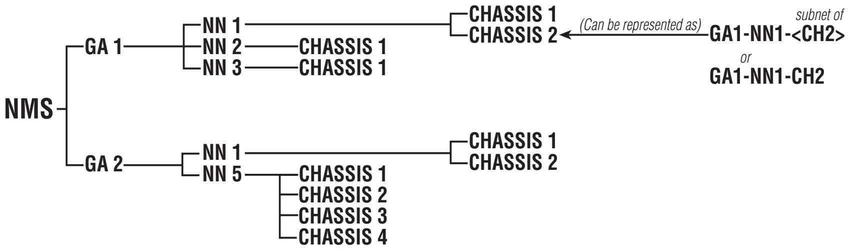


Figure 46. Container IDs in the NMS

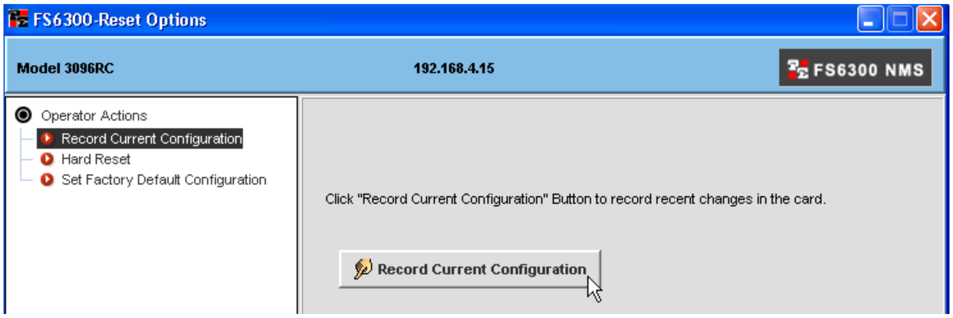
Managing Operator Actions

Operators may want to reboot a device or save the current configuration to memory, in case problems arise in the system. To reach the Operator Actions menu, right-click on the Device icon and select **Operator Action**.

Record the current configuration

To save the current configuration of a device to memory:

1. In the main menu tree under **Network Maps**, navigate to the **Chassis** or **Card/Slot.**
2. Right-click on the card's icon in the main window and select **Operator Action**. The **Reset Options** window appears. It shows the card model, IP address, and software revision of the card.


FS6300-Reset Options
Model 3096RC
192.168.4.15
FS6300 NMS
Operator Actions
Record Current Configuration
Hard Reset
Set Factory Default Configuration
Record Current Configuration

Click "Record Current Configuration" Button to record recent changes in the card.

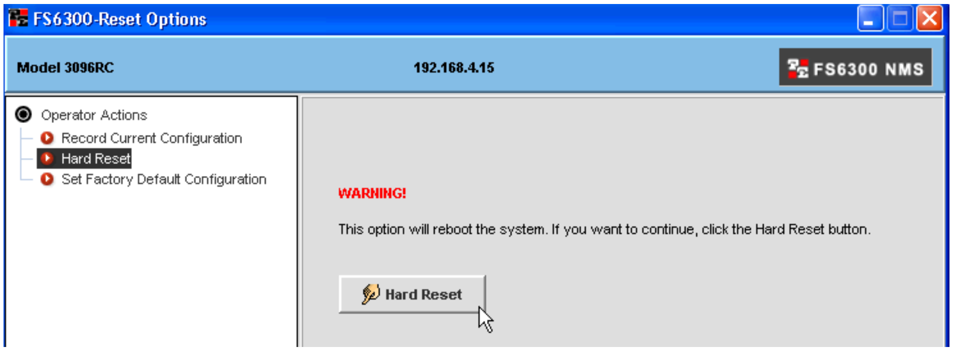
Figure 47. Record Current Configuration

3. Select **Record Current Configuration** from the menu tree in the Reset Options window.
4. Click the **Record Current Configuration** button.

Reboot the device

To reboot a chassis or card:

1. In the main menu tree under **Network Maps**, navigate to the **Chassis** *or* **Card/Slot.**
2. Right-click on the card's icon in the main window and select **Operator Action**. The **Reset Options** window appears. It shows the card model, IP address, and software revision of the card.



WARNING!

This option will reboot the system. If you want to continue, click the Hard Reset button.

Figure 48. Hard Reset

3. Select **Hard Reset** from the menu tree in the Reset Options window.

4. Click the **Hard Reset** button.

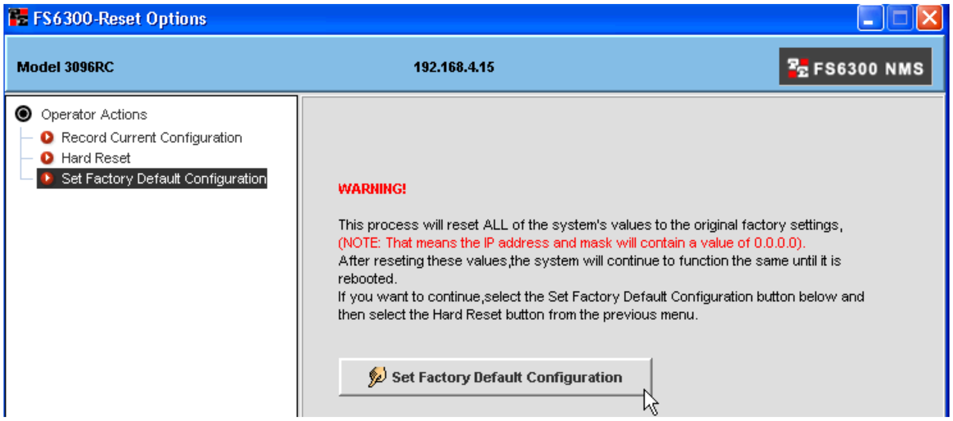
IMPORTANT

The **Hard Reset** process will reset ALL of the system's values to the original factory settings. After resetting these values, the system will continue to function the same until the system is rebooted.

Set the factory default configuration

To set the factory default configuration for a device:

1. In the main menu tree under **Network Maps**, navigate to the **Chassis** *or* **Card/Slot.**
2. Right-click on the card's icon in the main window and select **Operator Action**. The **Reset Options** window appears. It shows the card model, IP address, and software revision of the card.


FS6300-Reset Options
Model 3096RC
192.168.4.15
FS6300 NMS
Operator Actions
Record Current Configuration
Hard Reset
Set Factory Default Configuration
Set Factory Default Configuration

WARNING!

This process will reset ALL of the system's values to the original factory settings,
(NOTE: That means the IP address and mask will contain a value of 0.0.0.0).
After reseting these values,the system will continue to function the same until it is rebooted.
If you want to continue,select the Set Factory Default Configuration button below and then select the Hard Reset button from the previous menu.

Figure 49. Set Factory Default Configuration

3. Select **Set Factory Default Configuration** from the menu tree in the Reset Options window.
4. Click the **Set Factory Default Configuration** button.
5. Click the **Hard Reset** button.

IMPORTANT

The **Hard Reset** process will reset ALL of the system's values to the original factory settings. After resetting these values, the system will continue to function the same until the system is rebooted.

Configuring Cards

See the following chapters for detailed information on configuring specific cards:

- **2616RC** – Chapter 5, “Configuring the 2616RC Card” on page 67
- **3096RC** – Chapter 6, “Configuring the 3096RC Card” on page 83
- **3196RC** – Chapter 7, “Configuring the 3196RC Card” on page 105
- **6511RC** – Chapter 8, “Configuring the 6511RC Card” on page 126

Note Although this guide supplies basic information for configuring cards in the FS6300 NMS, you may also want to refer to the card’s *Administrator’s Reference Guide* and *User Manual* for more detailed information on installing and configuring the card.

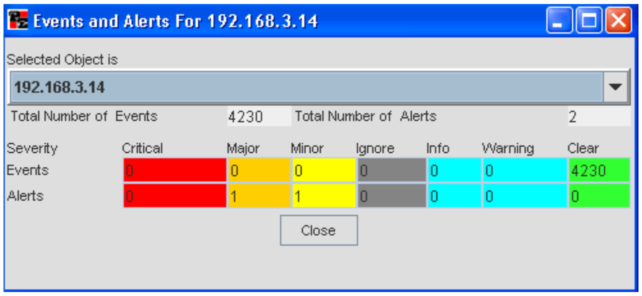
The following sections include procedures that are the same for all cards:

- “Viewing Events and Alerts” on page 62
- “Exporting the Configuration” on page 63
- “Importing the Configuration” on page 64
- “Viewing/Modifying System Log Configuration” on page 65
- “Changing Alarm Status” on page 65
- “Viewing/Modifying System Log Configuration” on page 65

Viewing Events and Alerts

Events are occurrences in the network, such as the discovery of an element, status update of an element, or a filure of an element. **Alarms/Alerts** are a result of events in the network and they represent failures that require immediate attention.

To view a color-coded chart that shows the amount of alarms and severity of alarms for the card, select **Events and Alerts** from the card’s configuration menu.



Selected Object is

192.168.3.14

Total Number of Events 4230 Total Number of Alerts 2

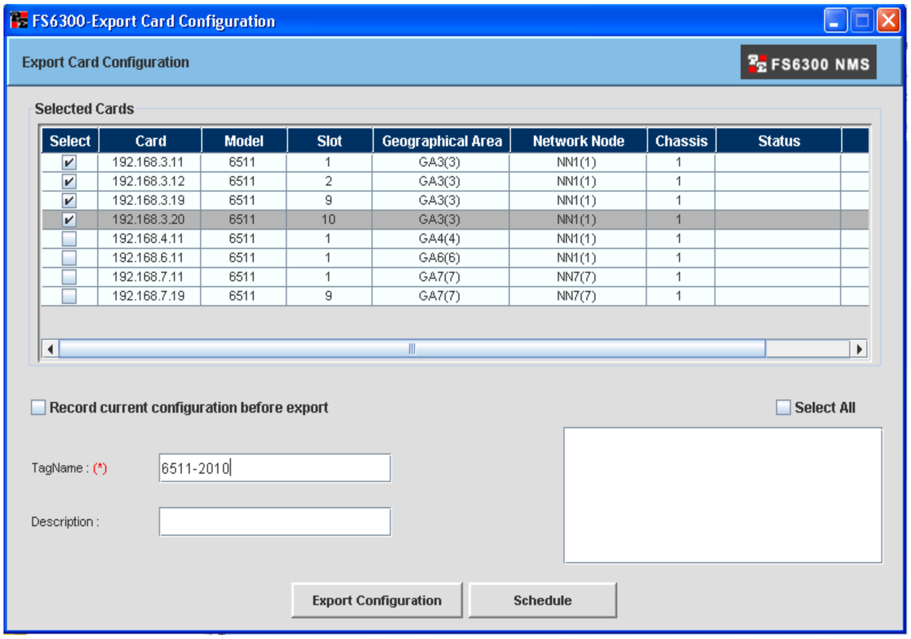
Severity	Critical	Major	Minor	Ignore	Info	Warning	Clear
Events	0	0	0	0	0	0	4230
Alerts	0	1	1	0	0	0	0

Figure 50. Card Events and Alerts

Exporting the Configuration

To save a card configuration:

1. Click **Tools** > **Schedule Tasks** in the main window. In the **FS6300-Schedule Tasks** window, select the radio button for **Export Card Configuration**. Select the **Card Model** from the drop-down menu.
2. Click **Execute Now**. The **Export Card Configuration** window displays a list of cards.



Select	Card	Model	Slot	Geographical Area	Network Node	Chassis	Status
☑	192.168.3.11	6511	1	GA3(3)	NN1(1)	1	
☑	192.168.3.12	6511	2	GA3(3)	NN1(1)	1	
☑	192.168.3.19	6511	9	GA3(3)	NN1(1)	1	
☑	192.168.3.20	6511	10	GA3(3)	NN1(1)	1	
□	192.168.4.11	6511	1	GA4(4)	NN1(1)	1	
□	192.168.6.11	6511	1	GA6(6)	NN1(1)	1	
□	192.168.7.11	6511	1	GA7(7)	NN7(7)	1	
□	192.168.7.19	6511	9	GA7(7)	NN7(7)	1	

□ Record current configuration before export

□ Select All

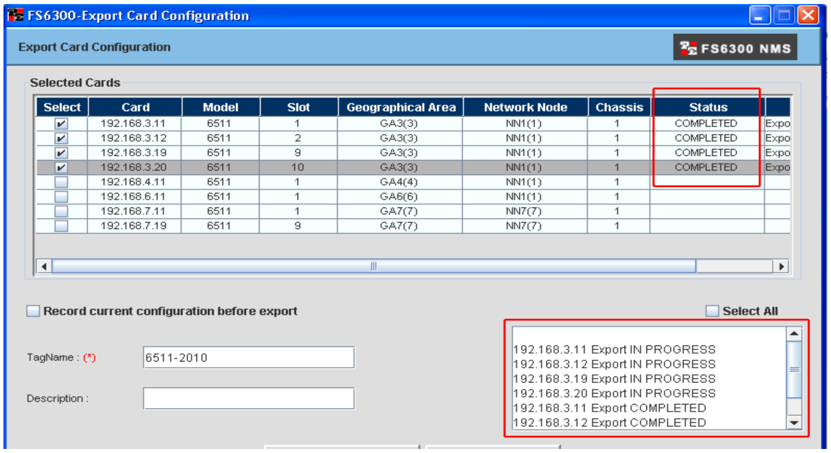
TagName : (*) 6511-2010

Description :

Figure 51. FS6300 Export Card Configuration window

3. Select the boxes of the desired cards. Enter a name for the configuartion in the **TagName** field. Then, click **Export Configuration**.

The window displays a “COMPLETED” status message after the system successfully exports the configuration file. Exported files are on the NMS in the directory: */opt/FS6300/Server/<nms version>/ExportedFiles/Device-Config/<card type>*.



Select	Card	Model	Slot	Geographical Area	Network Node	Chassis	Status	
☑	192.168.3.11	6511	1	GA3(3)	NN1(1)	1	COMPLETED	Expo
☑	192.168.3.12	6511	2	GA3(3)	NN1(1)	1	COMPLETED	Expo
☑	192.168.3.19	6511	9	GA3(3)	NN1(1)	1	COMPLETED	Expo
☑	192.168.3.20	6511	10	GA3(3)	NN1(1)	1	COMPLETED	Expo
□	192.168.4.11	6511	1	GA4(4)	NN1(1)	1		
□	192.168.6.11	6511	1	GA6(6)	NN1(1)	1		
□	192.168.7.11	6511	1	GA7(7)	NN7(7)	1		
□	192.168.7.19	6511	9	GA7(7)	NN7(7)	1		

□ Record current configuration before export

□ Select All

TagName : (*) 6511-2010

Description :

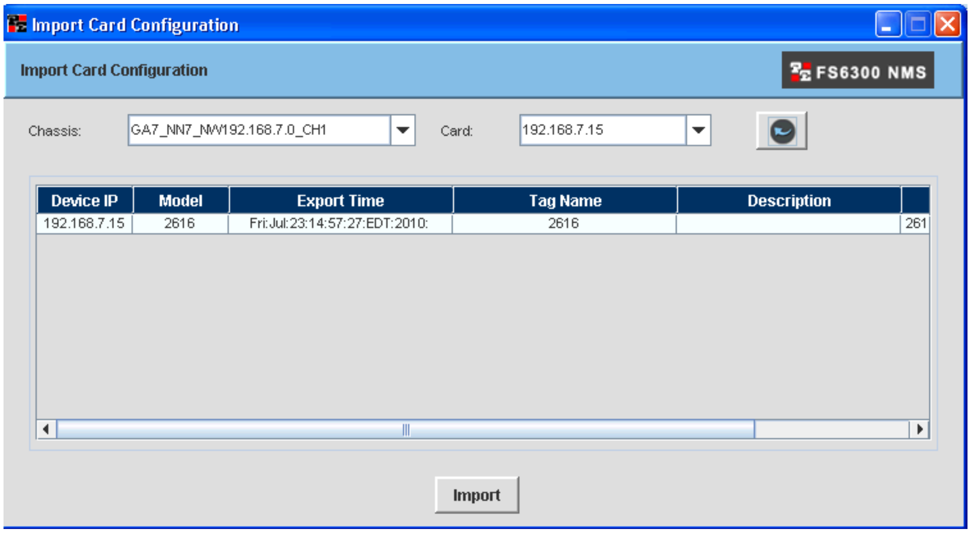
```
192.168.3.11 Export IN PROGRESS
192.168.3.12 Export IN PROGRESS
192.168.3.19 Export IN PROGRESS
192.168.3.20 Export IN PROGRESS
192.168.3.11 Export COMPLETED
192.168.3.12 Export COMPLETED
```

Figure 52. Export Complete

Importing the Configuration

To load a configuration file for a card:

1. Click **Tools** > **View Exported Card Configuration** in the main window. The **Import Card Configuration** window displays.



Chassis: GA7_NN7_NW192.168.7.0_CH1

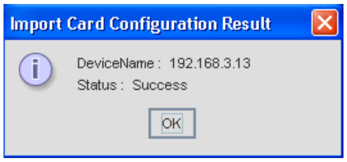
Card: 192.168.7.15

Device IP	Model	Export Time	Tag Name	Description	
192.168.7.15	2616	Fri:Jul:23:14:57:27:EDT:2010:	2616		261

Figure 53. Import Card Configuration

2. Select the desired **Chassis** and **Card** IP address from the drop-down menus. Click the button to refresh the available device configuration list.

3. Select the configuration file from the list and click **Import**. A confirmation message displays after the system successfully applies the configuration file.

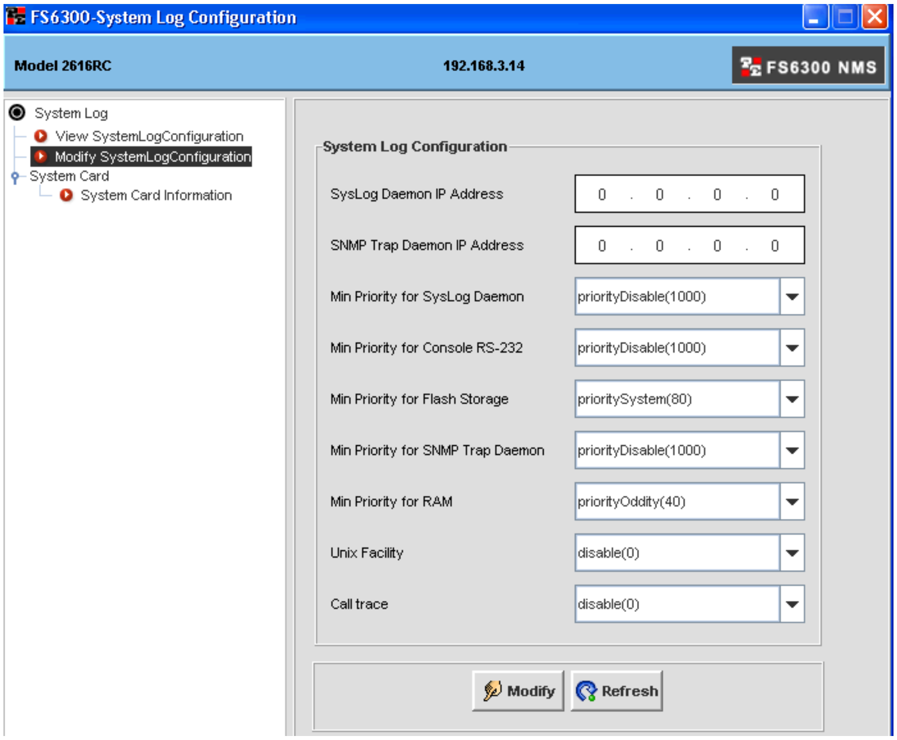


DeviceName : 192.168.3.13
Status : Success

Figure 54. Successful Import

Viewing/Modifying System Log Configuration

Select **System Log** from the card's configuration menu to view and modify syslog information. If you only want to view the syslog configuration, click on **View SystemLog Configuration** in the System Log window. To configure the syslog information, click on **Modify SystemLog Configuration** in the menu tree in the Syslog window.



System Log Configuration

SysLog Daemon IP Address	0 . 0 . 0 . 0
SNMP Trap Daemon IP Address	0 . 0 . 0 . 0
Min Priority for SysLog Daemon	priorityDisable(1000)
Min Priority for Console RS-232	priorityDisable(1000)
Min Priority for Flash Storage	prioritySystem(80)
Min Priority for SNMP Trap Daemon	priorityDisable(1000)
Min Priority for RAM	priorityOddity(40)
Unix Facility	disable(0)
Call trace	disable(0)

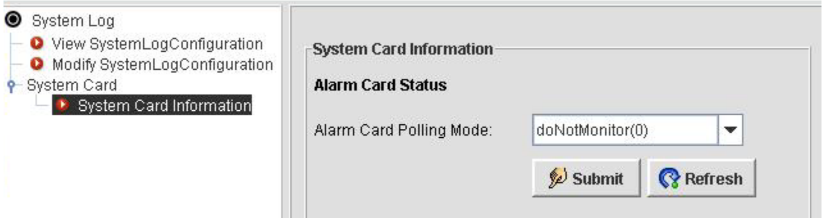
Figure 55. Modify System Log

Changing Alarm Status

To change the alarm status of a card:

> **Note** There must only be **one** card on the entire chassis that is configured for alarm card monitoring.

1. Click on **System Card Information** in the System Log window.



System Card Information

Alarm Card Status

Alarm Card Polling Mode: doNotMonitor(0)

Figure 56. Set System Card Alarm Status

2. Select an option for the card from the **Alarm Card Polling Mode** drop-down menu.
3. Click **Submit**.

Viewing LEDs

To view the real-time LEDs of a chassis or card:

1. Navigate to **Network Maps** in the menu tree, then right-click on the card or chassis icon in the main window.
2. Click on **Chassis Unit GUI** or **Card Front Panel GUI**.
3. A graphic of the front panel displays. The LEDs are shown in real-time.

Chapter 5 Configuring the 2616RC Card

Chapter contents

Introduction

The Patton Model 2616RC is a digital cross-connect with 16 T1/E1 ports. There are several ways to reach the configuration menu for the 2616RC card:

- Click on **Network Maps** in the main menu tree, then click on **Chassis.** Right-click on the 2616RC icon.
- Navigate to **Network Database** > **Managed Objects** > **Cards** in the main menu tree, then right-click on the IP address of the card in the table in the main window.

The best way to reach the configuration menu for a card is to select the card's chassis in the menu tree, then right-click on the card's icon in the main window.

2616RC Configuration Menu

The following options are available in the pull-down menu for the 2616RC card:

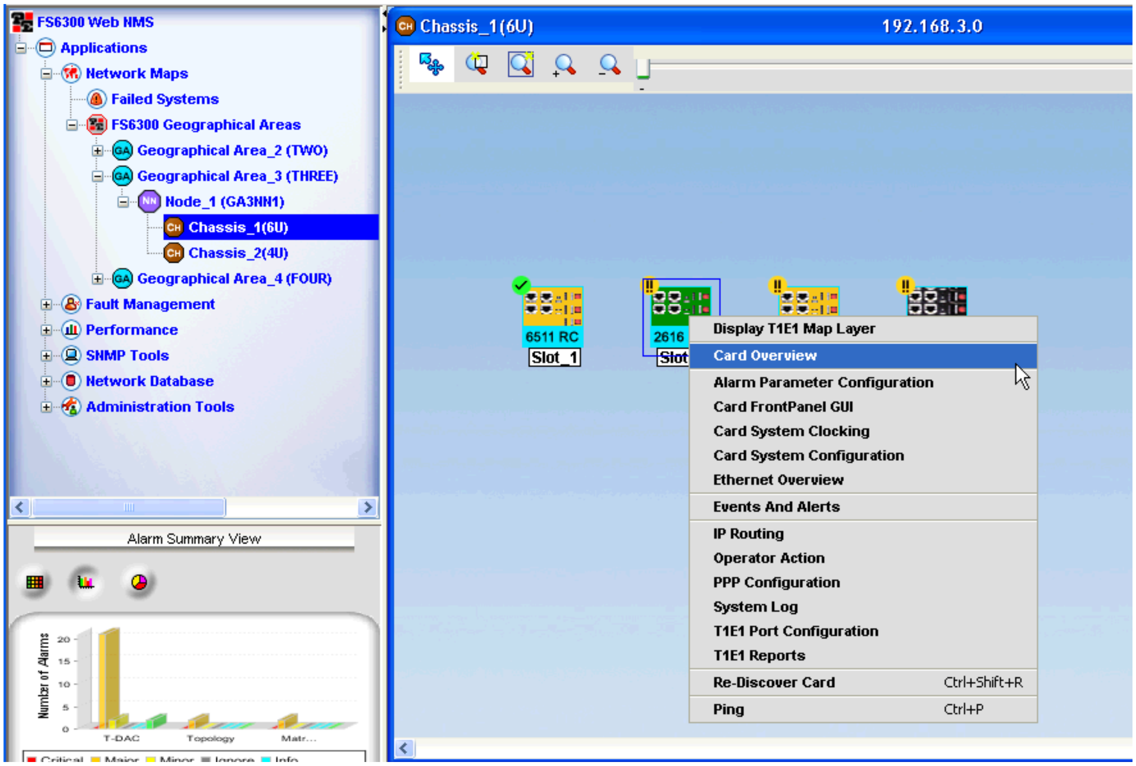


Figure 57. 2616RC Configuration Menu

- Display T1E1 Map Layer – See "Viewing the T1/E1 Map Layer" on page 82
- Card Overview – Shows information for Box Status, Card Info, and Alarm Info
- Alarm Parameter Configuration – See "Configuring Alarms through a Card in the Chassis" on page 48
- Card Front Panel GUI – See "Viewing the Front Panel" on page 69
- Card System Clocking – See "Configuring Card System Clocking" on page 54
- Card System Configuration – See "Configuring the Card System" on page 69

- Ethernet Overview – See "Configuring Ethernet Settings" on page 71
- Events and Alerts – See "Viewing Events and Alerts" on page 62
- IP Routing – See "Configuring IP Routing" on page 72
- Operator Action – See "Managing Operator Actions" on page 60
- PPP Configuration – See "Configuring PPP" on page 74
- System Log – See "Viewing/Modifying System Log Configuration" on page 65
- T1E1 Port Configuration – See "Configuring the T1/E1 Ports" on page 78
- T1E1 Reports – See "Viewing T1/E1 Reports" on page 82
- Re-Discover Card – See "Re-Discovering Cards Manually" on page 38
- Ping – Displays a status message after pinging the interface.

Viewing the Front Panel

Click on **Card Front Panel GUI** to view the front panel of the card in real-time.

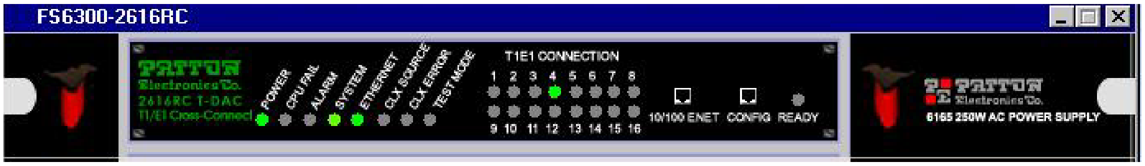


Figure 58. 2616RC Front Panel LEDs

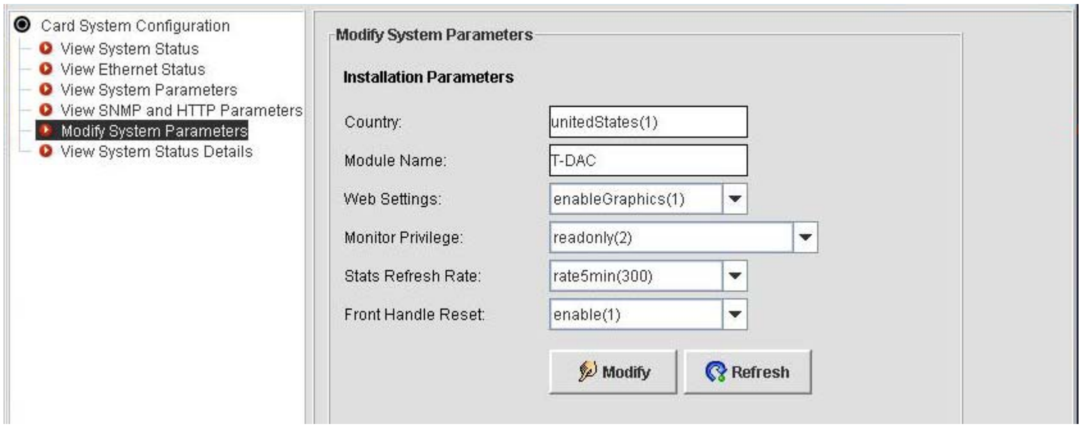
Configuring the Card System

Click on **Card System Configuration** to configure system parameters. You can also view the system status, ethernet status, system parameters, SNMP and HTTP Parameters, and system status details.

Modify System Parameters

If you only want to view the system parameters, click on **View System Parameters** in the Card System Configuration window.

To configure the card system, click on **Modify System Parameters** in the menu tree in the Card System Configuration window (see Figure 57 on page 68).



Installation Parameters

Country: unitedStates(1)

Module Name: T-DAC

Web Settings: enableGraphics(1)

Monitor Privilege: readonly(2)

Stats Refresh Rate: rate5min(300)

Front Handle Reset: enable(1)

Figure 59. Modify 2616RC Card System Parameters

1. Select to enable or disable graphics from the **Web Settings** drop-down menu.
2. Select a privilege option for configuring the card through the NMS from the **Monitor Privilege** drop-down menu.
3. Select how often you would like to refresh statistics information from the **Stats Refresh Rate** drop-down menu.
4. Select to enable or disable front handle reset from the **Front Handle Reset** drop-down menu.
5. Click **Modify** to save your changes. Click **Refresh**.

View System Status

Click on **View System Status** in the Card System Configuration window to see an overview of the physical status of the card and the system status. **View System Status** shows information about the handle switches, front/rear LEDs, alarm and clock LEDs, and the board temperature.

View System Status Details

Click on **View System Status Details** in the Card System Configuration window to see information on CPU statistics, Message Block statistics, Memory statistics, Manufacturer details, and the Enclosure System temperature.

View Ethernet Status

Click on **View Ethernet Status** in the Card System Configuration window to see the LEDs and speeds of the card’s Ethernet ports.

View SNMP and HTTP Parameters

Click on **View SNMP and HTTP Parameters** in the Card System Configuration window to see the SNMP version and passwords.

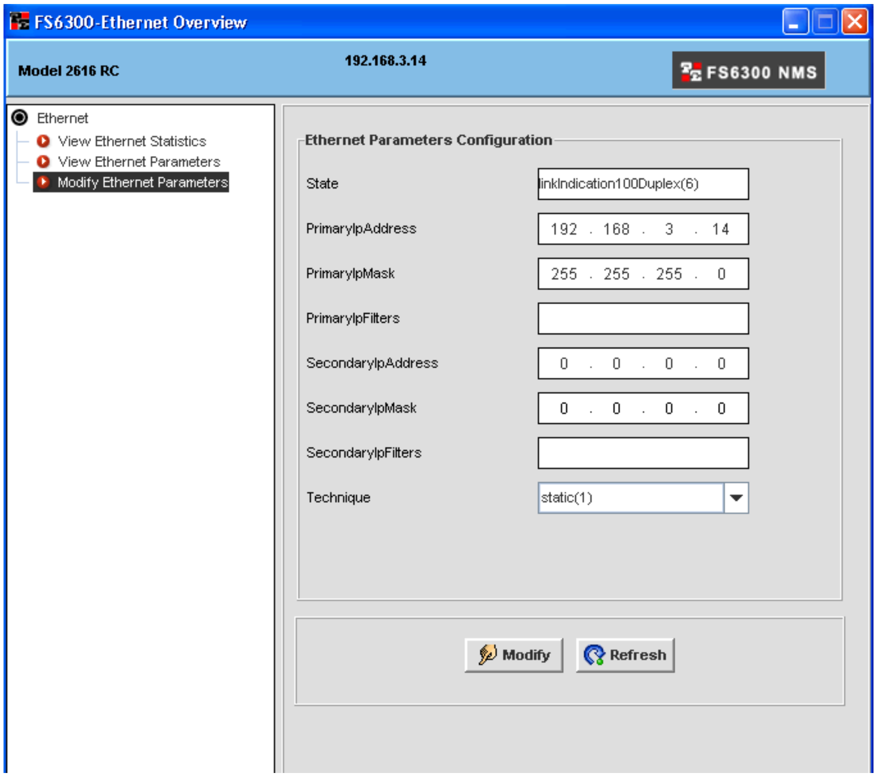
Configuring Ethernet Settings

Click on **Ethernet Overview** to configure Ethernet settings. You can also view Ethernet statistics.

Modify Ethernet Parameters

If you only want to view the Ethernet parameters, click on **View Ethernet Parameters** in the Ethernet Overview window.

To configure the Ethernet settings, click on **Modify Ethernet Parameters** in the menu tree in the Ethernet Overview window (see Figure 60).



State: inkIndication100Duplex(6)
PrimaryIpAddress: 192 . 168 . 3 . 14
PrimaryIpMask: 255 . 255 . 255 . 0
PrimaryIpFilters:
SecondaryIpAddress: 0 . 0 . 0 . 0
SecondaryIpMask: 0 . 0 . 0 . 0
SecondaryIpFilters:
Technique: static(1)

Figure 60. Modify 2616RC Ethernet Parameters

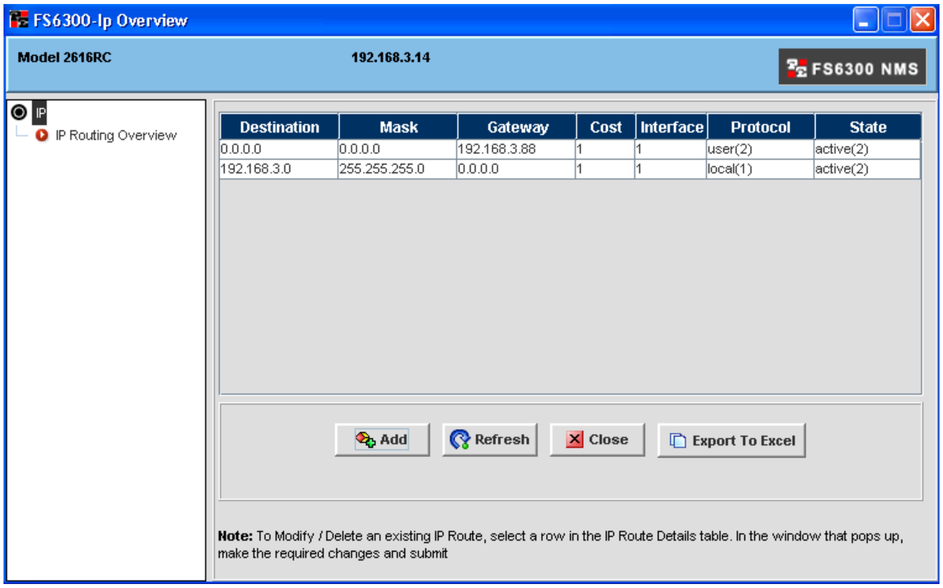
1. Enter the main address and mask for the card in the **Primary IP Address** and **IP Mask** fields.
2. The **IP Filter** needs to be provisioned through the card's configuration website. For more information on setting up IP Filters, refer to the *Model 2616RC Adminstrator's Reference Guide*.
3. From the **Technique** drop-down menu, select **static** if you want to statically assign the IP address, or select **disable** if you want to use DHCP to assign the IP address.
4. Click **Modify** to commit your changes. Click **Refresh**.

View Ethernet Statistics

Click on **View Ethernet Statistics** in the Ethernet Overview window to view statistics for the Ethernet ports on the device, such as errors and frame stats.

Configuring IP Routing

You may configure a host and routes for the 2616RC through the FS6300 NMS. The **IP Overview** window shows details for routing destinations, and includes information for gateway, cost, interface, protocol, and state of each route.



Model 2616RC   192.168.3.14

Destination	Mask	Gateway	Cost	Interface	Protocol	State
0.0.0.0	0.0.0.0	192.168.3.88	1	1	user(2)	active(2)
192.168.3.0	255.255.255.0	0.0.0.0	1	1	local(1)	active(2)

Note: To Modify / Delete an existing IP Route, select a row in the IP Route Details table. In the window that pops up, make the required changes and submit

Figure 61. 2616RC IP Overview

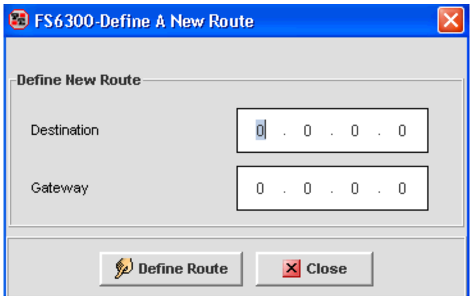
The table in the **IP Overview** window shows a list of defined routes for the 2616RC, and includes the following information for each entry:

- **Destination:** The destination IP address of this route. An entry with a value of 0.0.0.0 is considered a default route.
- **Mask:** The mask that is logical-ANDed with the destination address before being compared to the value in the Destination field.
- **Gateway:** The IP address where the packets should be forwarded.
- **Cost:** The cost of the route as defined by RIP standards. Cost is sometimes considered to be number of hops.
- **Interface:** The index value that uniquely identifies the local interface through which the next hop of this route should be reached.
- **Protocol:** The routing mechanism via which this route was learned.
  - *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 managemen tools.
  - *rip(4)*—Learned via reception of RIP packet.
  - *icmp(5)*—Learned via reception of ICMP packet
- **State:** Shows if a route is valid/in use.

Add Routes

To add an IP route to the 2616RC:

1. In the **IP Overview** window for the 2616RC, click the **Add** button to define a new route.



FS6300-Define A New Route

Define New Route

Destination: 0 . 0 . 0 . 0

Gateway: 0 . 0 . 0 . 0

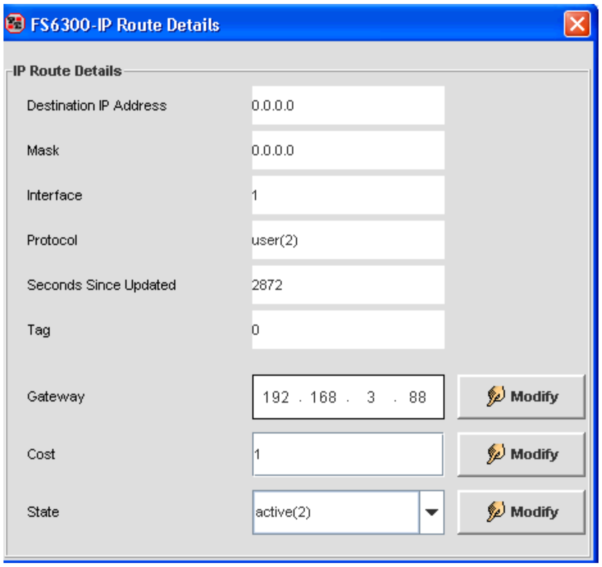
Figure 62. Add a New Route for 2616RC

2. Enter a **Destination** address for the new route. An entry with a value of 0.0.0.0 is considered a default route.
3. Enter a **Gateway** address for the new route. The gateway address specifies the IP address where the packets should be forwarded.
4. Click **Define Route**.

Modify Routes

To modify an existing IP route for the 2616RC:

1. In the **IP Overview** window for the 2616RC, select the entry in the table of the route you want to modify.



FS6300-IP Route Details

IP Route Details

Destination IP Address: 0.0.0.0

Mask: 0.0.0.0

Interface: 1

Protocol: user(2)

Seconds Since Updated: 2872

Tag: 0

Gateway: 192 . 168 . 3 . 88

Cost: 1

State: active(2)

Figure 63. Modifying a Route for 2616RC

2. The **IP Route Details** window displays. You may only modify the gateway address, cost, and state of the route.
3. Enter your desired changes and click **Modify** for each change. A confirmation message displays.

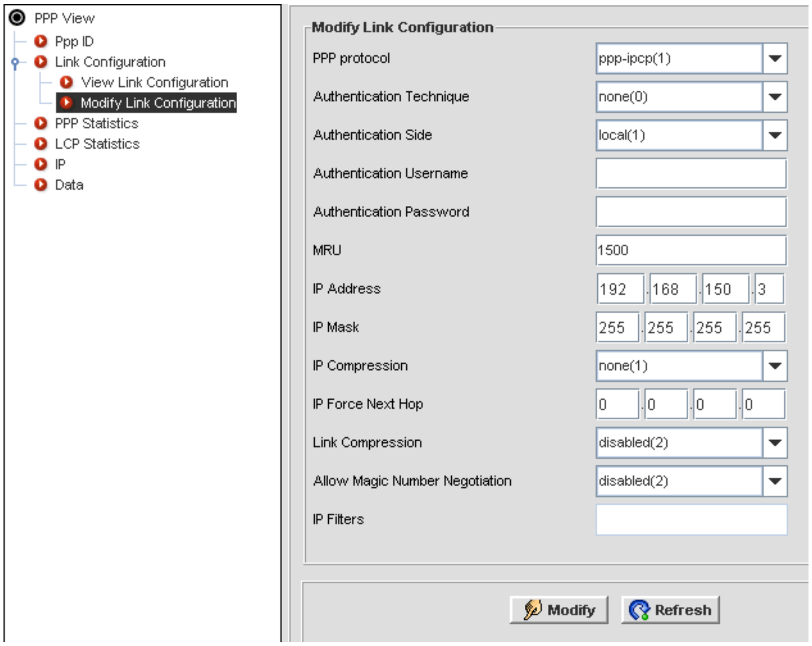
Configuring PPP

Click on **PPP Configuration** to view PPP links for the card. You may also modify the link configuration and default packet settings for PPP links.

Modify PPP Link Configuration

To configure PPP links for the card:

1. Right-click on the card in the main window and select **PPP Configuration**. The **PPP2616** window displays.
2. Click on **PPP View** and select an entry to edit from the table. The **FS6300-PPP** window displays.
3. Select **Modify Link Configuration**..



Modify Link Configuration

PPP protocol	ppp-ipcp(1)
Authentication Technique	none(0)
Authentication Side	local(1)
Authentication Username	
Authentication Password	
MRU	1500
IP Address	192 . 168 . 150 . 3
IP Mask	255 . 255 . 255 . 255
IP Compression	none(1)
IP Force Next Hop	0 . 0 . 0 . 0
Link Compression	disabled(2)
Allow Magic Number Negotiation	disabled(2)
IP Filters	

Figure 64. PPP Link Configuration

4. Edit the desired options:

   – **PPP Protocol:** The desired kind of PPP protocol.

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

   – **Authentication Technique:** The login technique to use for authentication.

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

- **Authentication Side:** The side of the link which will be authenticating.
  - local(1)—local server will be authenticating. Remote needs to log into local server.
  - remote(2)—remote server will be authentication. Local needs to log into remote server.
- **Authentication Username and Password:** The username and password that will be sent to the remote side if the remote machine is authenticating.
- **MRU:** The setting for Maximum Receive Unit (MRU), used for the PPP negotiation.
- **IP Address:** The IP address that will be used for the PPP link.
- **IP Mask:** The IP mask that will be used for the PPP link.
- **IP Compression:** Set whether Van Jacobson (*vj-tcp(2)*) header compression is used or not (*none(1)*).
- **IP Force Next Hop:** The IP address of the interface, which should be the next hop for the packets—fast routing
- **Link Compression:** Enables the PPP link layer address and protocol field compression. When enabled the PPP negotiations will desire link compression but may disable the compression due the other end of the link not accepting link compression. When disabled the PPP negotiations will force no compression on the PPP link.
  - enabled(1)—enable link compression
  - disabled(2)—disable link compression
- **Allow Magic Number Negotiation:** Determines if magic number negotiation should be done.
  - enabled(1)—enable magic number negotiation
  - disabled(2)—disable magic number negotiation
- **IP Filters:** This option is not modifiable through the FS6300 NMS. Refer to the card's *Administrator's Reference Guide* for more information on IP filtering.

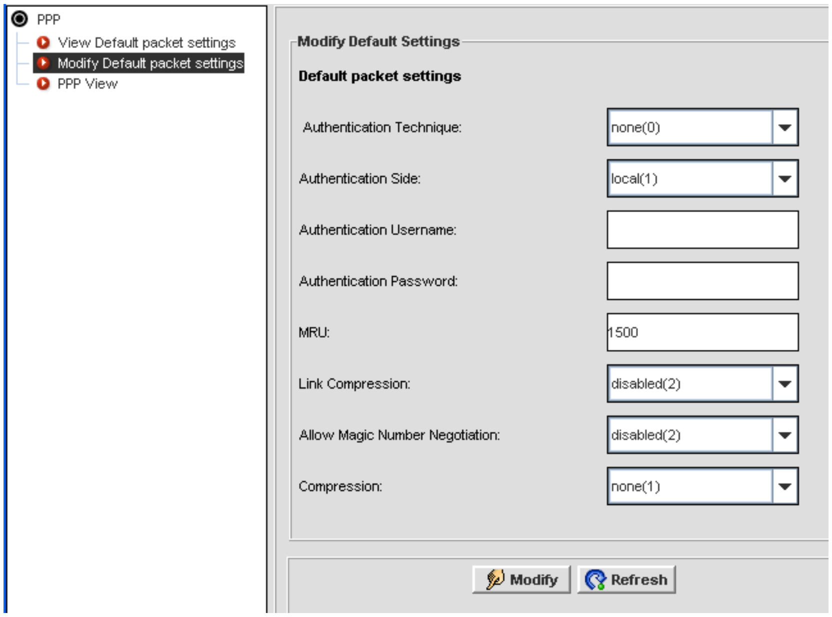
5. Click **Modify** to apply your changes.

Modify Default Packet Settings

You may modify the default PPP settings that each PPP link will take when first initialized. See “Modify PPP Link Configuration” on page 74 for modifying settings for individual links.

To modify default packet settings for PPP links:

1. Right-click on the card in the main window and select **PPP Configuration**. The **PPP2616** window displays.
2. Select **Modify Link Configuration**.



Modify Default Settings

Default packet settings

Authentication Technique: none(0)

Authentication Side: local(1)

Authentication Username:

Authentication Password:

MRU: 1500

Link Compression: disabled(2)

Allow Magic Number Negotiation: disabled(2)

Compression: none(1)

Figure 65. PPP Default Packet Settings

3. Edit the desired options:
   - **Authentication Technique:** The login technique to use for authentication.
     - none(0)—No authentication will be used
     - pap(3)—password authentication protocol will be used
     - chap(4)—challenge handshake authentication protocol will be used
     - chapORpap(5)—chap will be negotiated first, if that fails, pap will be attempted
   - **Authentication Side:** The side of the link which will be authenticating.
     - local(1)—local server will be authenticating. Remote needs to log into local server.
     - remote(2)—remote server will be authentication. Local needs to log into remote server.
   - **Authentication Username and Password:** The username and password that will be sent to the remote side if the remote machine is authenticating.
   - **MRU:** The setting for Maximum Receive Unit (MRU), used for the PPP negotiation.

– **Link Compression:** Enables the PPP link layer address and protocol field compression. When enabled the PPP negotiations will desire link compression but may disable the compression due the other end of the link not accepting link compression. When disabled the PPP negotiations will force no compression on the PPP link.

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

– **Allow Magic Number Negotiation:** Determines if magic number negotiation should be done.

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

– **Compression:** If none(1), then the local node will not attempt to negotiate any IP compression option. Otherwise, the local node will attempt to negotiate compression mode. Changing this option will have effect when the link restarts.

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

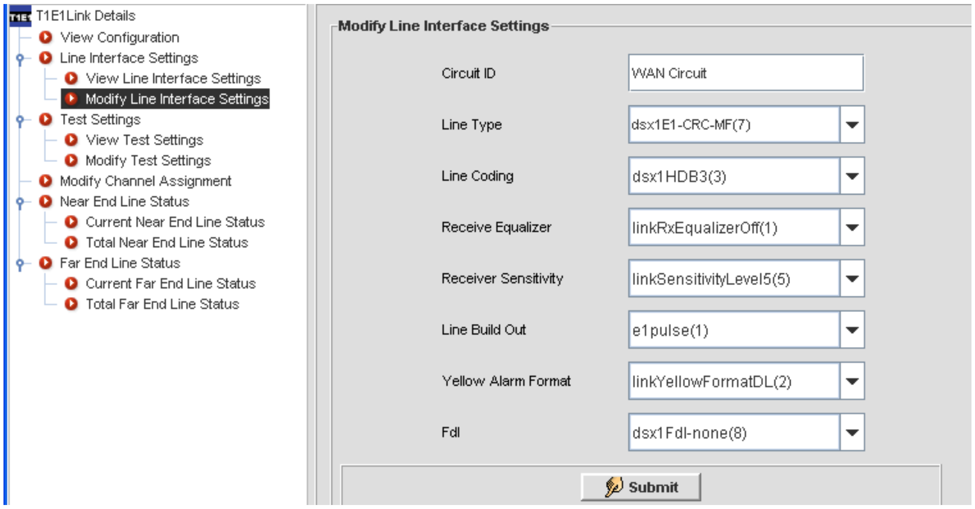
Configuring the T1/E1 Ports

Click on **T1E1 Port Configuration** to view T1/E1 links for the card. Select an entry in the table to configure line interfaces, test settings, and channel assignments for T1/E1 ports.

View Configuration

In the **T1-E1 Port Configuration** window for the selected link, click on **View Configuration**. If there are alarms for the link, click on **Alarms Present** to view the alarm details for the link.

Modify Line Interface Settings


T1E1Link Details
View Configuration
Line Interface Settings
View Line Interface Settings
Modify Line Interface Settings
Test Settings
View Test Settings
Modify Test Settings
Modify Channel Assignment
Near End Line Status
Current Near End Line Status
Total Near End Line Status
Far End Line Status
Current Far End Line Status
Total Far End Line Status
Submit

Modify Line Interface Settings

Circuit ID	WAN Circuit
Line Type	dsx1E1-CRC-MF(7)
Line Coding	dsx1HDB3(3)
Receive Equalizer	linkRxEqualizerOff(1)
Receiver Sensitivity	linkSensitivityLevel5(5)
Line Build Out	e1pulse(1)
Yellow Alarm Format	linkYellowFormatDL(2)
Fdl	dsx1Fdl-none(8)

Figure 66. T1/E1 Link Configuration window

1. In the **T1-E1 Port Configuration** window for the selected link, click on **Modify Line Interface Settings**.
2. Edit the desired options:

   – **Circuit ID:** The transmission vendor’s circuit identifier, for the purpose of facilitating troubleshooting.

   – **Line Type:** the type of DS1 Line implemented on this circuit. The type of circuit affects the number of bits per second that the circuit can reasonably carry, as well as the interpretation of the usage and error statistics. Select fromt he following values:

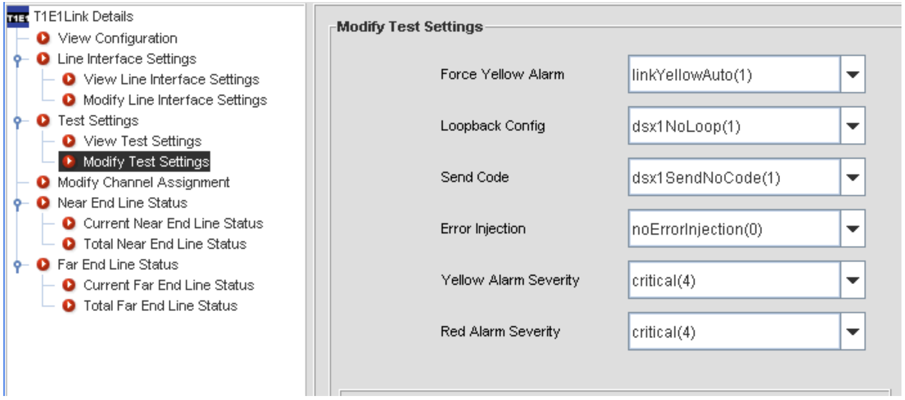
     - other(1)—Link is disabled
     - dsx1ESF(2)—Extended Superframe DS1
     - dsx1D4(3)—AT&T D4 format DS1
     - dsx1E1(4)—Based on CCITT/ITU G.704 without CRC (Cyclical Redundancy Check)
     - dsx1E1-CRC(5)—Based on CCITT/ITU G.704 with CRC (Cyclical Redundancy Check)
     - dsx1E1-MF(6)—Based on CCIT/ITU G.704 without CRC (bit oriented signaling)
     - dsx1E1-CRC-MF(7)—Based on CCIT/ITU G.704 with CRC (bit oriented signaling)
     - dsx1E1-Transparent(8)—Based on CCIT/ITU G.703 without CRC (Cyclical Redundancy Check)

- **Line Coding:** The type of Zero Code Suppression used on the link.
  - dsx1JBZS(1)—Jammed Bit Zero Suppression, in which the AT&T specification of at least one pulse every 8 bit periods is literally implemented by forcing a pulse in bit 8 of each channel. Thus, only seven bits per channel, or 1.344 Mbps, is available for data. This feature is not currently implemented.
  - dsx1B8ZS(2)—The use of a specified pattern of normal bits and bipolar violations which are used to replace a sequence of eight zero bits. The most common coding for T1 circuits.
  - dsx1HDB3(3)—This line coding is used with most E1 circuits today.
  - dsx1ZBTSI(4)—May use dsx1ZBTSI, or Zero Byte Time Slot Interchange. This feature is not currently implemented.
  - dsx1AMI(5)—Refers to a mode wherein no zero code suppression is present and the line encoding does not solve the problem directly. In this application, the higher layer must provide data which meets or exceeds the pulse density requirements, such as inverting HDLC data.
  - other(6)—This feature is not currently supported.
- **Receive Equalizer:** The equalization used on the received signal. Long haul signals should have the equalization set for more. Short haul signals require less equalization.
- **Receiver Sensitivity:** The minimum voltage at which the WAN port will sense that the signal is available. This variable is only used if the **Receiver Equalization** is set to **ON**.
- **Line Build Out:** The T1 or E1 pulse levels used by the T1/E1 ports:
  - triState(0)—When the T1/E1 port is not in use, you may want to place the port in tri-state mode. While in this setting, the input lines to the port are placed in high impedance protection mode.
  - e1pulse(1)—Used when connecting the T1/E1 port to E1 lines.
  - t1pulse0dB(2)—Strong T1 pulse amplitude.
  - t1pulse-7dB(3)—Medium T1 pulse amplitude.
  - t1pulse-15dB(4)—Weak T1 pulse amplitude.
- **Yellow Alarm Format:** The standard used to transmit and identify the Yellow Alarm.
  - link YellowFormatBit2(1)—Bit-2 equal zero in every channel
  - link YellowFormatDL(2)—FF00 pattern in the Data Link
  - link YellowFormatFrame12FS(3)—FS bit of frame 12
- **Fdl:** implementation of FDL is being used, if any. FDL applies only to T1 circuits.
  - other(1)—Indicates that a protocol other than one following is used.
  - dsx1Ansi-T1-403(2)—Refers to the FDL exchange recommended by ANSI.
  - dsx1Att-54016(3)—Refers to ESF FDL exchanges.
  - dsx1Fdl-none(4)—Indicates that the device does not use the FDL.

  If one of the E1 line types has been selected, set **Fdl** to **dsx1Fdl-none**(**8**).

3. Click **Submit** to commit your changes.

Modify Test Settings


T1E1Link Details
View Configuration
Line Interface Settings
View Line Interface Settings
Modify Line Interface Settings
Test Settings
View Test Settings
Modify Test Settings
Modify Channel Assignment
Near End Line Status
Current Near End Line Status
Total Near End Line Status
Far End Line Status
Current Far End Line Status
Total Far End Line Status

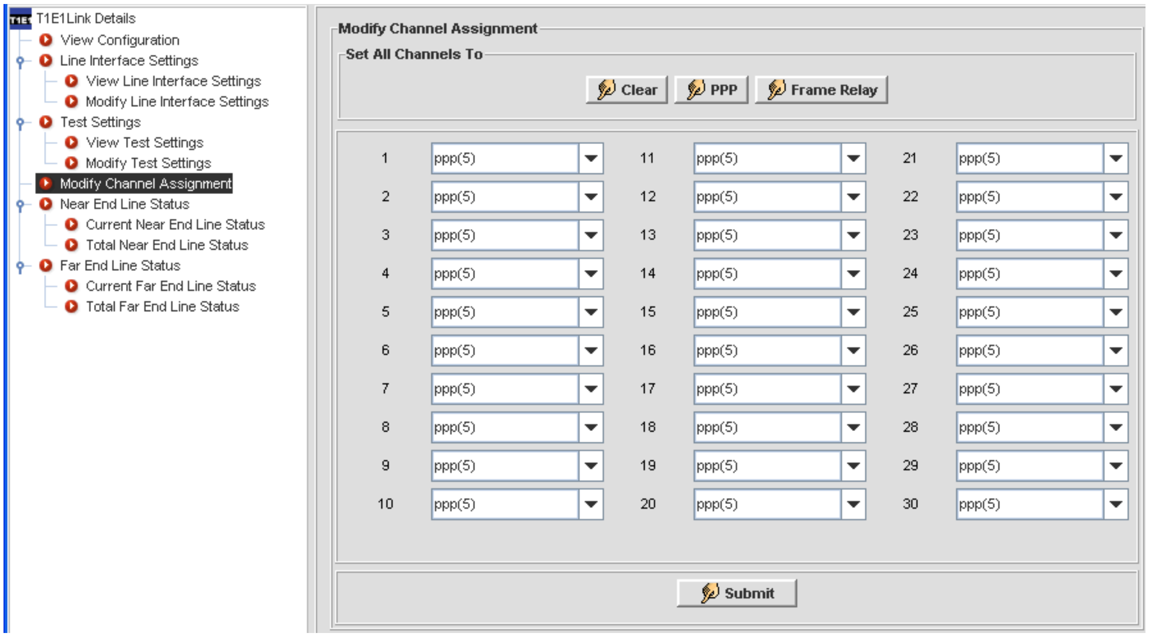
Modify Test Settings

Force Yellow Alarm	linkYellowAuto(1)
Loopback Config	dsx1NoLoop(1)
Send Code	dsx1SendNoCode(1)
Error Injection	noErrorInjection(0)
Yellow Alarm Severity	critical(4)
Red Alarm Severity	critical(4)

Figure 67. T1/E1 Test Settings

1. In the **T1-E1 Port Configuration** window for the selected link, click on **Modify Test Settings**.
2. Edit the desired options:
   - **Force Yellow Alarm:** The standard used to transmit and identify the Yellow Alarm.
     - linkYellowAuto—Do not force the transmission of a yellow alarm. But, yellow alarm may be automatically transmitted.
     - linkYellowOn—Force the transmission of a yellow alarm even if the received signal is in frame.
     - linkYellowDisable—Do NOT transmit a yellow alarm even if the received signal is out of frame.
   - **Loopback Configuration:** The loopback configuration of the DS1 interface.
     - dsx1NoLoop(1)—Not in the loopback state. A device that is not capable of performing a loopback on the interface shall always return this as it's value.
     - dsx1PayloadLoop(2)—The received signal at this interface is looped through the device. Typically the received signal is looped back for retransmission after it has passed through the device's framing function.
     - dsx1LineLoop(3)—The received signal at this interface does not go through the device (minimum penetration) but is looped back out.
     - dsx1OtherLoop(4)—Loopbacks that are not defined here.
   - **Send Code:** The type of code is being sent across the DS1 interface by the device.
     - dsx1SendNoCode(1)—Sending looped or normal data
     - dsx1SendLineCode(2)—Sending a request for a line loopback
     - dsx1SendResetCode(4)—Sending a loopback termination request
   - **Error Injection:** Force an output error to see if the other end detects it.
   - **Yellow Alarm Severity:** Critical / Major / Minor / Info / Ignore
   - **Red Alarm Severity:** Critical / Major / Minor / Info / Ignore
3. Click **Submit** to commit your changes.

Modify Channel Assignments


T1E1Link Details
View Configuration
Line Interface Settings
View Line Interface Settings
Modify Line Interface Settings
Test Settings
View Test Settings
Modify Test Settings
Modify Channel Assignment
Near End Line Status
Current Near End Line Status
Total Near End Line Status
Far End Line Status
Current Far End Line Status
Total Far End Line Status
Modify Channel Assignment
Set All Channels To
Clear
PPP
Frame Relay
Submit

1	ppp(5)	11	ppp(5)	21	ppp(5)
2	ppp(5)	12	ppp(5)	22	ppp(5)
3	ppp(5)	13	ppp(5)	23	ppp(5)
4	ppp(5)	14	ppp(5)	24	ppp(5)
5	ppp(5)	15	ppp(5)	25	ppp(5)
6	ppp(5)	16	ppp(5)	26	ppp(5)
7	ppp(5)	17	ppp(5)	27	ppp(5)
8	ppp(5)	18	ppp(5)	28	ppp(5)
9	ppp(5)	19	ppp(5)	29	ppp(5)
10	ppp(5)	20	ppp(5)	30	ppp(5)

Figure 68. T1/E1 Channel Assignment

In the **Modify Channel Assignment** section of the **T1/E1 Link Configuration** window, you can change selected DS0 channels to carry in-band management information over Frame Relay or PPP links. You can use the buttons at the top of the window to modify all 30 timeslots at once. Or, you can use the 30 drop-down menus to modify selected timeslots individually. Click **Submit** to apply your changes for individual links.

View Line Status

There are two types of line status statistics that you may view in the T1/E1 Link Configuration window – **Near End Line Status** and **Far End Line Status**.

- **Near End Line Status** – Click on **Current Near End Line Status** to view statistics for current near end performance. Click on **Total Near End Line Status** to view statistics totals for near end performance.
- **Far End Line Status** – Click on **Current Far End Line Status** to view statistics for current far end performance. Click on **Total Far End Line Status** to view statistics totals for far end performance.

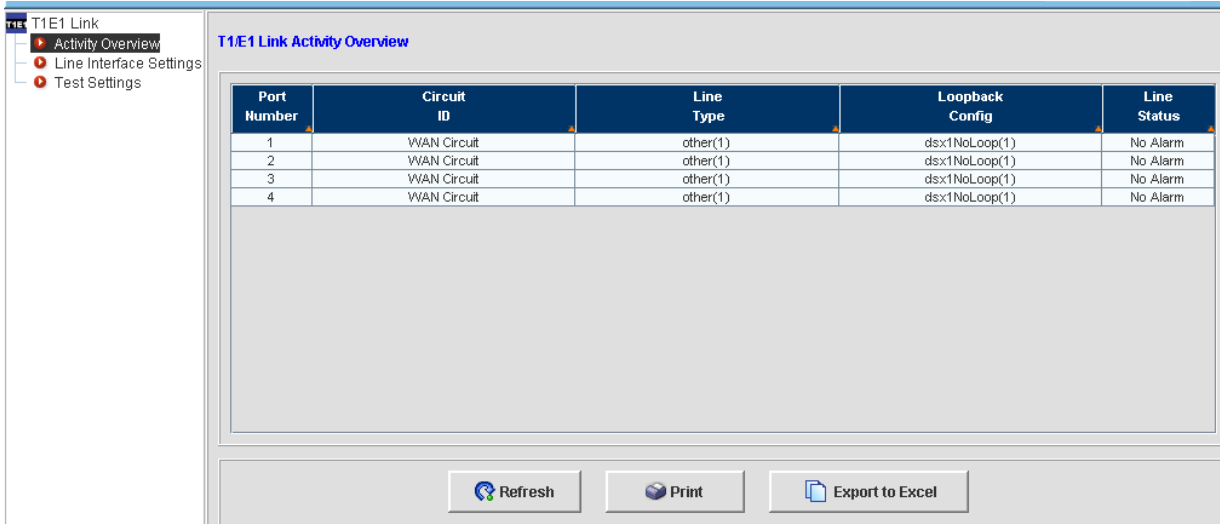
Note Refer to the *2616RC Adminsitrator's Reference Guide* for detailed information about line status statistics.

Viewing T1/E1 Reports

Click on **T1E1 Reports** from the card's configuration menu to view and print different reports about the activity, line interface settings, and test settings of T1/E1 links on the 2616RC card.

Click the **Print** button to send the report to a printer on your network.

Click the **Export to Excel** button to send the report to Microsoft Excel to save in a spreadsheet.



T1/E1 Link Activity Overview

Port Number	Circuit ID	Line Type	Loopback Config	Line Status
1	WAN Circuit	other(1)	dsx1NoLoop(1)	No Alarm
2	WAN Circuit	other(1)	dsx1NoLoop(1)	No Alarm
3	WAN Circuit	other(1)	dsx1NoLoop(1)	No Alarm
4	WAN Circuit	other(1)	dsx1NoLoop(1)	No Alarm

Figure 69. 2616RC T1/E1 Reports

Viewing the T1/E1 Map Layer

Click on **Display T1E1 Map Layer** from the card's configuration menu to show a map of all the T1/E1 ports on the card. Right-click on a port in the map to configure its link. See "Configuring the T1/E1 Ports" on page 78 for more details.

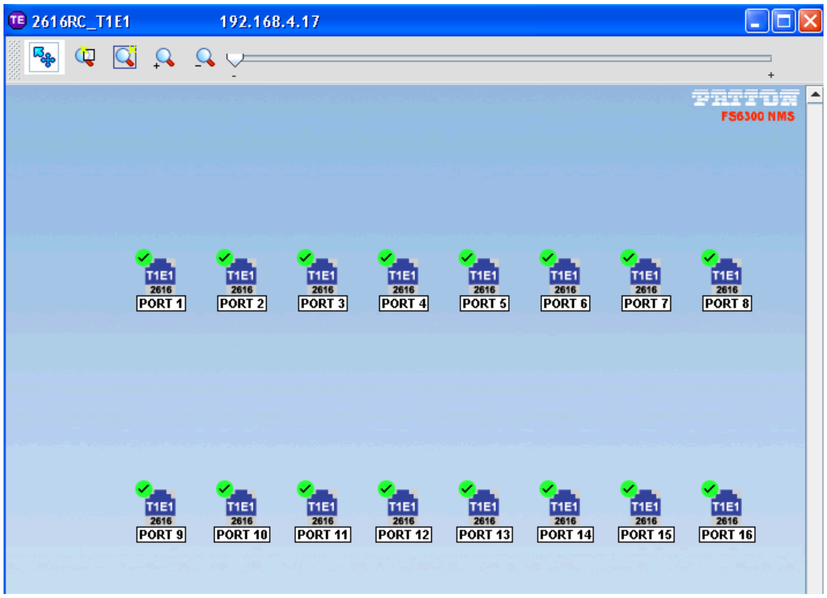


Figure 70. 2616RC T1/E1 Port Map

Chapter 6 Configuring the 3096RC Card

Chapter contents

Introduction

The Patton Model 3096RC is a G.SHDSL TDM Concentrator with 16 G.SHDSL ports. There are several ways to reach the configuration menu for the 3096RC card:

- Click on **Network Maps** in the main menu tree, then click on **Chassis.** Right-click on the 3096RC icon.
- Navigate to **Network Database** > **Managed Objects** > **Cards** in the main menu tree, then right-click on the IP address of the card in the table in the main window.

The best way to reach the configuration menu for a card is to select the card in the main menu tree, then right-click on the card's icon in the main window.

3096RC Configuration Menu

The following options are available in the pull-down menu for the 3096RC card:

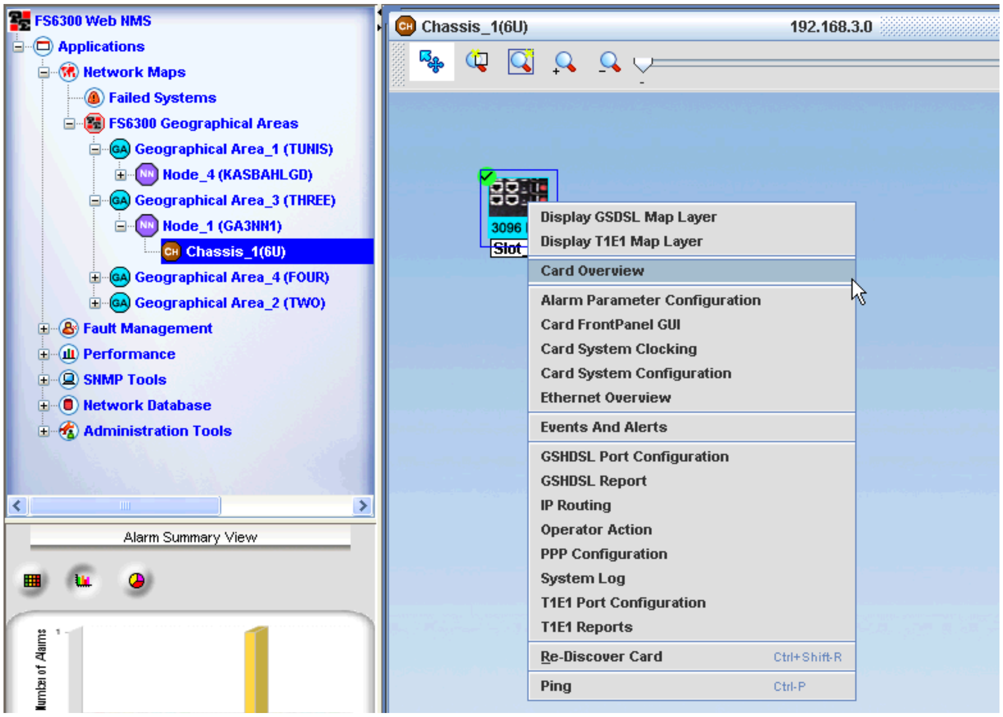


Figure 71. 3096RC Configuration Menu

- Display G.SHDSL Map Layer – "Viewing the G.SHDSL Map Layer" on page 104
- Display T1E1 Map Layer – See "Viewing the T1/E1 Map Layer" on page 103
- Card Overview – Shows information for Box Status, Card Info, and Alarm Info
- Alarm Parameter Configuration – See "Configuring Alarms through a Card in the Chassis" on page 48
- Card Front Panel GUI – See "Viewing the Front Panel" on page 85
- Card System Clocking – See "Configuring Card System Clocking" on page 54
- Card System Configuration – See "Configuring the Card System" on page 85

- Ethernet Overview – See “Configuring Ethernet Settings” on page 87
- Events and Alerts – See “Viewing Events and Alerts” on page 62
- G.SHDSL Port Configuration – See “Configuring G.SHDSL Ports” on page 88
- G.SHDSL Report – See “Viewing G.SHDSL Reports” on page 92
- IP Routing – See “Configuring IP Routing” on page 93
- Operator Action – See “Managing Operator Actions” on page 60
- PPP Configuration – See “Configuring PPP” on page 95
- System Log – See “Viewing/Modifying System Log Configuration” on page 65
- T1E1 Port Configuration – See “Configuring the T1/E1 Ports” on page 99
- T1E1 Reports – See “Viewing T1/E1 Reports” on page 103
- Re-Discover Card – See “Re-Discovering Cards Manually” on page 38
- Ping – Displays a status message after pinging the interface.

Viewing the Front Panel

Click on **Card Front Panel GUI** to view the front panel of the card in real-time.

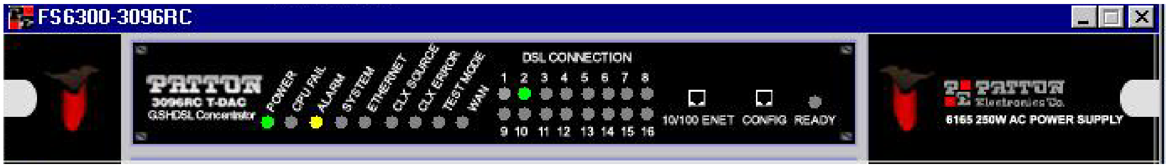


Figure 72. 3096RC Front Panel LEDs

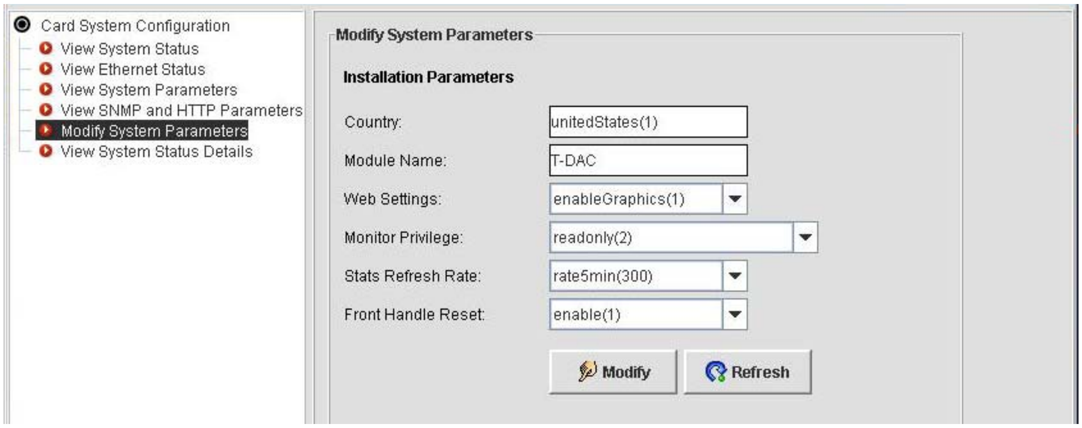
Configuring the Card System

Click on **Card System Configuration** to configure system parameters. You can also view the system status, ethernet status, system parameters, SNMP and HTTP Parameters, and system status details.

Modify System Parameters

If you only want to view the system parameters, click on **View System Parameters** in the Card System Configuration window.

To configure the card system, click on **Modify System Parameters** in the menu tree in the Card System Configuration window (see Figure 71 on page 84).



Modify System Parameters

Installation Parameters

Country: unitedStates(1)

Module Name: T-DAC

Web Settings: enableGraphics(1)

Monitor Privilege: readonly(2)

Stats Refresh Rate: rate5min(300)

Front Handle Reset: enable(1)

Figure 73. Modify Card System Parameters

1. Select to enable or disable graphics from the **Web Settings** drop-down menu.
2. Select a privilege option for configuring the card through the NMS from the **Monitor Privilege** drop-down menu.
3. Select how often you would like to refresh statistics information from the **Stats Refresh Rate** drop-down menu.
4. Select to enable or disable front handle reset from the **Front Handle Reset** drop-down menu.
5. Click **Modify** to save your changes. Click **Refresh**.

View System Status

Click on **View System Status** in the Card System Configuration window to see an overview of the physical status of the card and the system status. **View System Status** shows information about the handle switches, front/ rear LEDs, alarm and clock LEDs, and the board temperature.

View System Status Details

Click on **View System Status Details** in the Card System Configuration window to see information on CPU statistics, Message Block statistics, Memory statistics, Manufacturer details, and the Enclosure System temperature.

View Ethernet Status

Click on **View Ethernet Status** in the Card System Configuration window to see the LEDs and speeds of the card’s Ethernet ports.

View SNMP and HTTP Parameters

Click on **View SNMP and HTTP Parameters** in the Card System Configuration window to see the SNMP version and passwords.

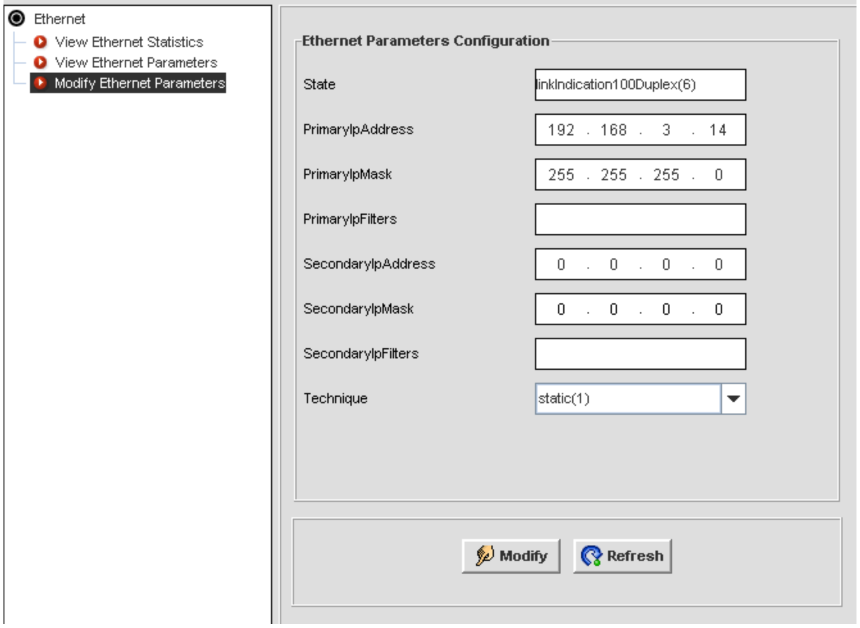
Configuring Ethernet Settings

Click on **Ethernet Overview** to configure Ethernet settings. You can also view Ethernet statistics.

Modify Ethernet Parameters

If you only want to view the Ethernet parameters, click on **View Ethernet Parameters** in the Ethernet Overview window.

To configure the Ethernet settings, click on **Modify Ethernet Parameters** in the menu tree in the Ethernet Overview window (see Figure 74).



State	inkIndication100Duplex(6)
PrimaryIpAddress	192 . 168 . 3 . 14
PrimaryIpMask	255 . 255 . 255 . 0
PrimaryIpFilters	
SecondaryIpAddress	0 . 0 . 0 . 0
SecondaryIpMask	0 . 0 . 0 . 0
SecondaryIpFilters	
Technique	static(1)

Figure 74. Modify Ethernet Parameters

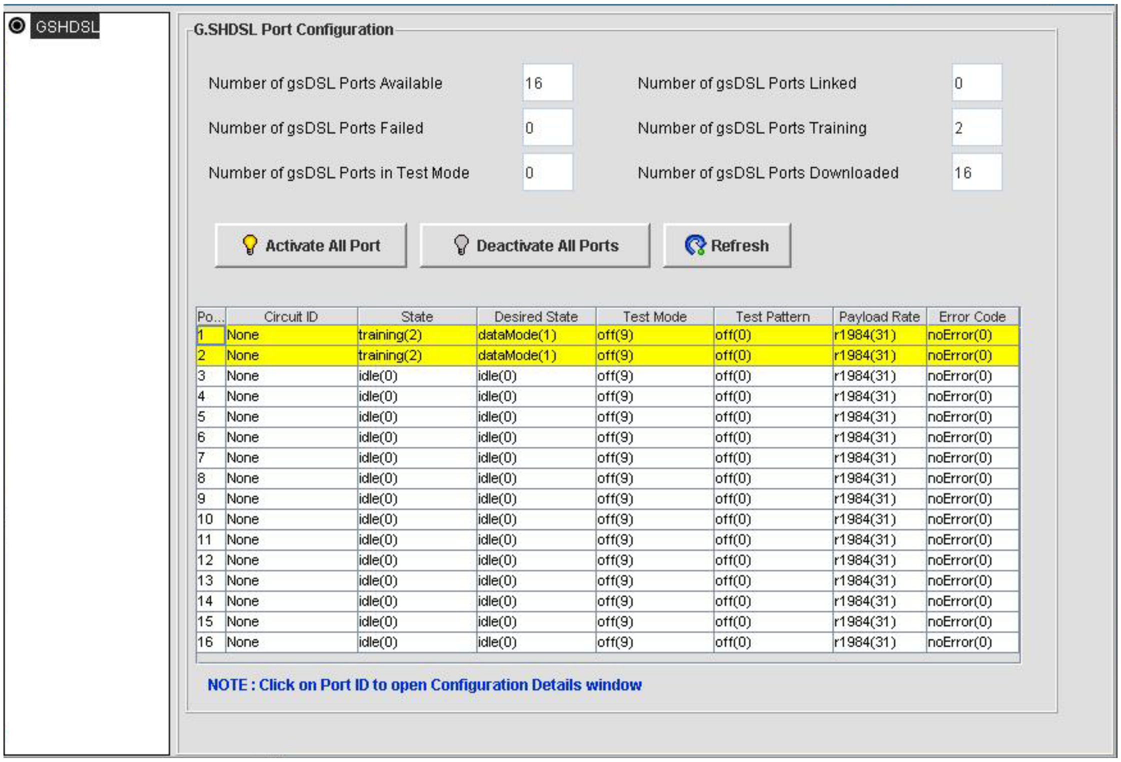
1. Enter the main address and mask for the card in the **Primary IP Address** and **IP Mask** fields.
2. The **IP Filter** needs to be provisioned through the card's configuration website. For more information on setting up IP Filters, refer to the *Model 3096RC Adminstrator's Reference Guide*.
3. From the **Technique** drop-down menu, select **static** if you want to statically assign the IP address, or select **disable** if you want to use DHCP to assign the IP address.
4. Click **Modify** to commit your changes. Click **Refresh**.

View Ethernet Statistics

Click on **View Ethernet Statistics** in the Ethernet Overview window to view statistics for the Ethernet ports on the device, such as errors and frame stats.

Configuring G.SHDSL Ports

Click on **G.SHDSL Port Configuration** in the pull-down menu to bring up the **G.SHDSL** window. The G.SHDSL window shows the number of G.SHDSL ports available, linked ports, failed ports, training ports, ports in test mode, and ports downloaded.



G.SHDSL Port Configuration

Number of gsDSL Ports Available	16	Number of gsDSL Ports Linked	0
Number of gsDSL Ports Failed	0	Number of gsDSL Ports Training	2
Number of gsDSL Ports in Test Mode	0	Number of gsDSL Ports Downloaded	16

Po...	Circuit ID	State	Desired State	Test Mode	Test Pattern	Payload Rate	Error Code
1	None	training(2)	dataMode(1)	off(9)	off(0)	r1984(31)	noError(0)
2	None	training(2)	dataMode(1)	off(9)	off(0)	r1984(31)	noError(0)
3	None	idle(0)	idle(0)	off(9)	off(0)	r1984(31)	noError(0)
4	None	idle(0)	idle(0)	off(9)	off(0)	r1984(31)	noError(0)
5	None	idle(0)	idle(0)	off(9)	off(0)	r1984(31)	noError(0)
6	None	idle(0)	idle(0)	off(9)	off(0)	r1984(31)	noError(0)
7	None	idle(0)	idle(0)	off(9)	off(0)	r1984(31)	noError(0)
8	None	idle(0)	idle(0)	off(9)	off(0)	r1984(31)	noError(0)
9	None	idle(0)	idle(0)	off(9)	off(0)	r1984(31)	noError(0)
10	None	idle(0)	idle(0)	off(9)	off(0)	r1984(31)	noError(0)
11	None	idle(0)	idle(0)	off(9)	off(0)	r1984(31)	noError(0)
12	None	idle(0)	idle(0)	off(9)	off(0)	r1984(31)	noError(0)
13	None	idle(0)	idle(0)	off(9)	off(0)	r1984(31)	noError(0)
14	None	idle(0)	idle(0)	off(9)	off(0)	r1984(31)	noError(0)
15	None	idle(0)	idle(0)	off(9)	off(0)	r1984(31)	noError(0)
16	None	idle(0)	idle(0)	off(9)	off(0)	r1984(31)	noError(0)

NOTE : Click on Port ID to open Configuration Details window

Figure 75. 3096RC G.SHDSL window

Activating/Deactivating All Ports

Click the **Activate All Ports** button to train all of the G.SHDSL ports on the card.

Click the **Deactivate All Ports** button to turn off all of the G.SHDSL ports on the card.

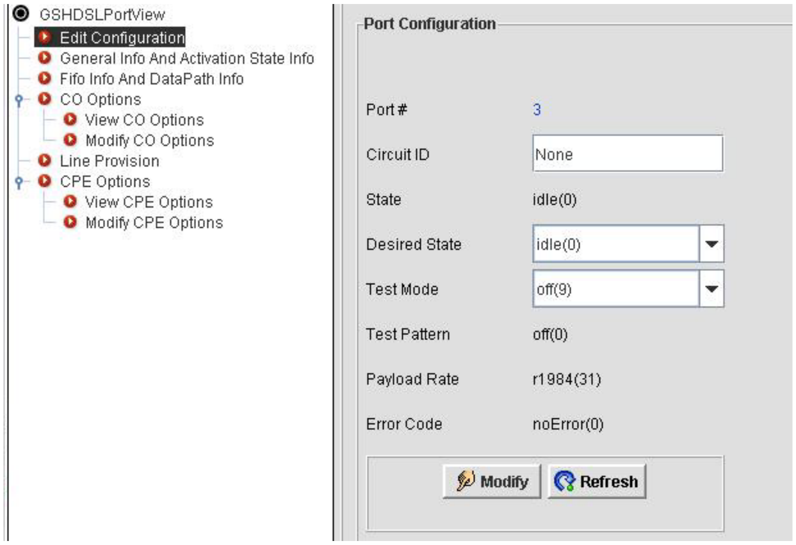
Configuring Individual Ports

To configure an individual port, click on the port in the table to bring up the **Port Configuration** window. From the port Configuration window, you can edit the port's configuration, view port information, edit CO/ CPE options, and edit the line rate.

Edit Configuration

Click on **Edit Configuration** in the menu tree of the Port Configuration window. **Circuit ID**, **Desired State**, and **Test Mode** are configurable.

1. Enter the **Circuit ID** in the text field.
2. Select idle or dataMode from the **Desired State** drop-down menu.
3. Select a loop or "off" from the **Test Mode** drop-down menu.
4. Click **Modify** to save your changes.



Port Configuration

Port #	3
Circuit ID	None
State	idle(0)
Desired State	idle(0)
Test Mode	off(9)
Test Pattern	off(0)
Payload Rate	r1984(31)
Error Code	noError(0)

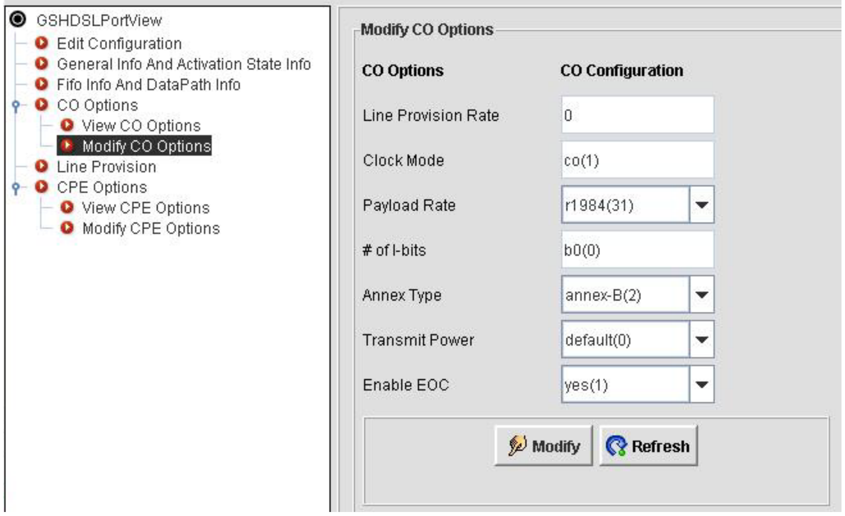
Figure 76. 3096RC Edit G.SHDSL Configuration

View Port Information

Click on **Fifo Info and DataPath Info** in the menu tree of the Port Configuration window to view Fifo and Data Path errors and up times.

Edit CO/CPE Options

Click on **CO Options** or **CPE Options** in the menu tree of the Port Configuration window to view the line provision rate, clock mode, payload rate, I-bits, annex type, transmit power, and EOC status.



Modify CO Options

CO Options	CO Configuration
Line Provision Rate	0
Clock Mode	co(1)
Payload Rate	r1984(31)
# of I-bits	b0(0)
Annex Type	annex-B(2)
Transmit Power	default(0)
Enable EOC	yes(1)

Figure 77. 3096RC Edit CO Options

To edit the CO/CPE options for a port:

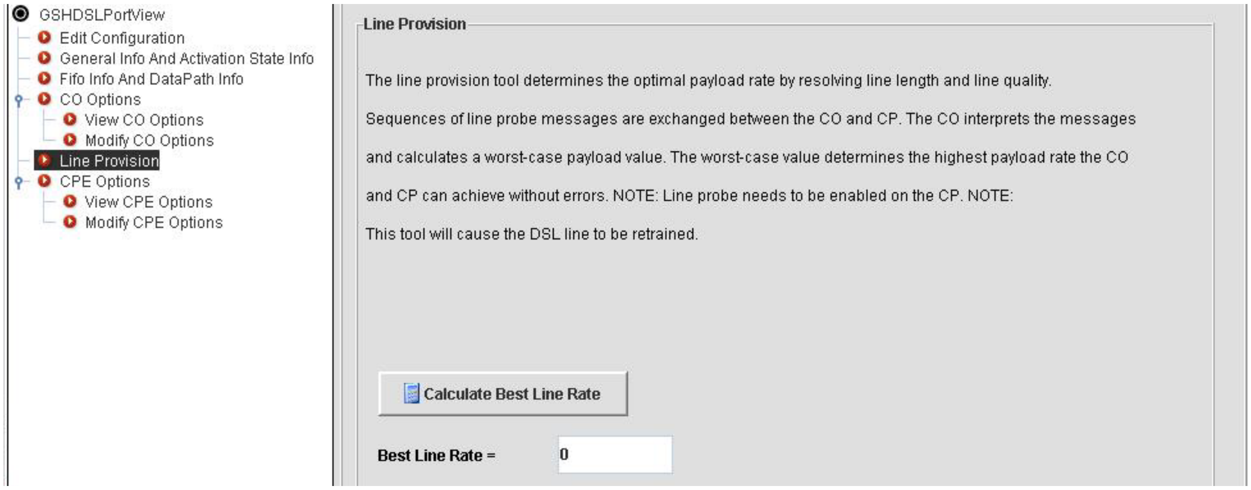
1. Click on **Modify CO Options** or **Modify CPE Options** in the menu tree of the Port Configuration window.
2. Edit the desired, configurable options:
   - **Payload Rate:** Select a rate fromt he drop-down menu. See "Determine Best Payload Rate" on page 91.
   - **Annex Type:** Select **Annex-A** for North America or **Annex-B** for outside North America.
   - **Transmit Power:** Select a value between +1–6dB to -1–6dB from the drop-down menu.
   - **Enable EOC:** Select Yes (to enable EOC) or No (to disable EOC) from the drop-down menu.
3. Click **Modify** to save your changes.

Determine Best Payload Rate

Click on **Line Provision** in the menu tree of the Port Configuration window to determine the best payload rate for the port. The Line Provision tool works by resolving line length and line quality. The CO interprets line probe messages from the CPE and calculates a worst-case payload value. The worst-case value determines the highest payload rate the CO and CPE can acheive without errors.

Note **Line Probe** must be enabled on the CPE for the Line Provision tool to work.

Note The Line Provision tool will retrain the DSL line.



The line provision tool determines the optimal payload rate by resolving line length and line quality.

Sequences of line probe messages are exchanged between the CO and CP. The CO interprets the messages

and calculates a worst-case payload value. The worst-case value determines the highest payload rate the CO

and CP can achieve without errors. NOTE: Line probe needs to be enabled on the CP. NOTE:

This tool will cause the DSL line to be retrained.

Best Line Rate = 0

Figure 78. 3096RC Line Provision Tool

Click the **Calculate Best Line Rate** button to determine the best payload rate.

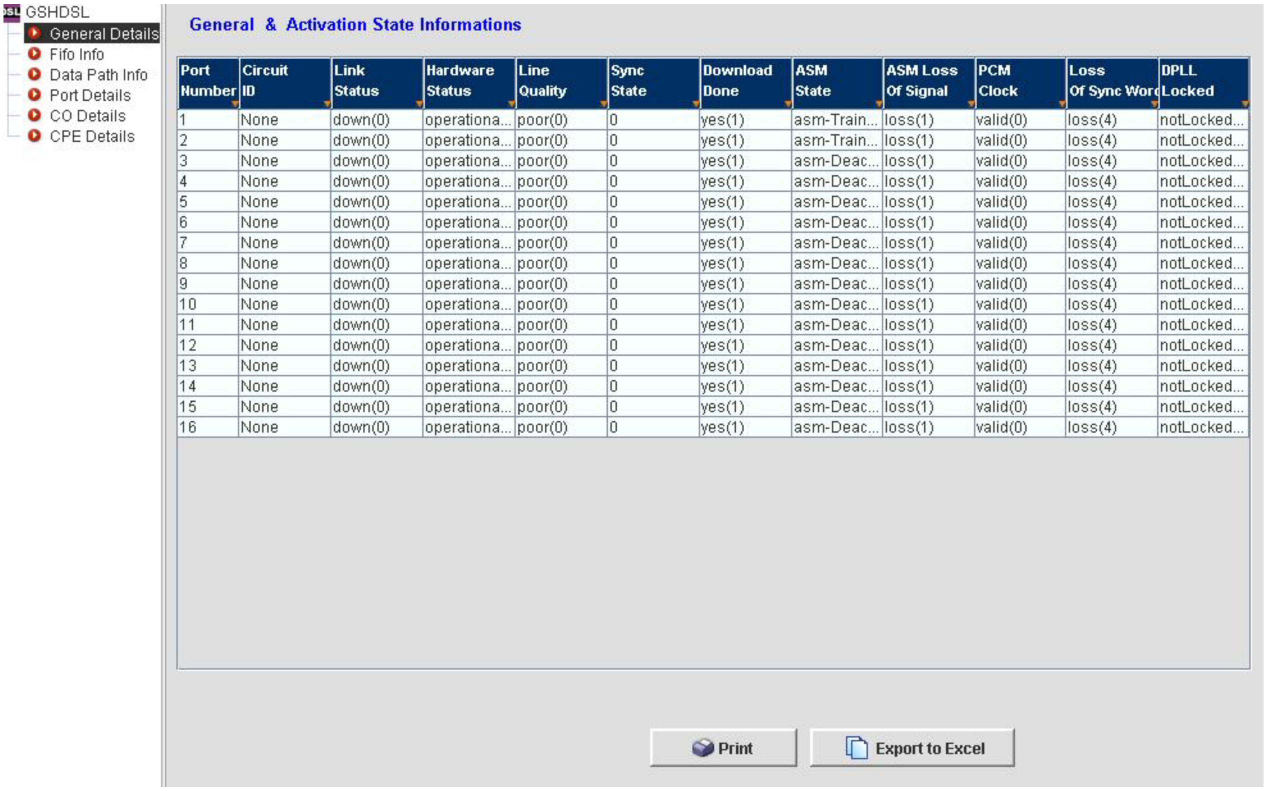
A status message will display when the tool is finished. Click **OK**.

Viewing G.SHDSL Reports

Click on **G.SHDSL Report** to view different reports about port details, CO/CPE details, data path, and Fifo information for the G.SHDSL ports on the 3096RC card.

Click the **Print** button to send the report to a printer on your network.

Click the **Export to Excel** button to send the report to Microsoft Excel to save in a spreadsheet.



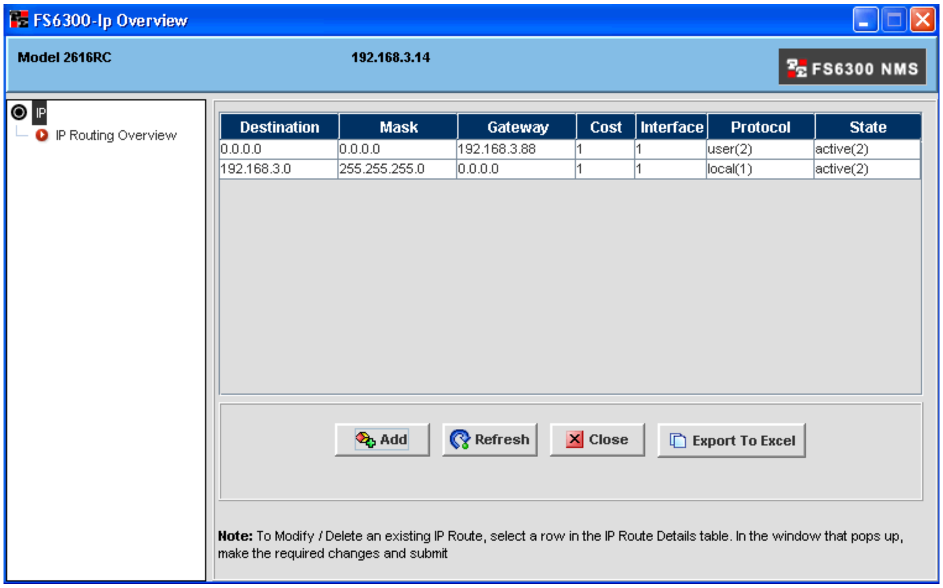
General & Activation State Informations

Port Number	Circuit ID	Link Status	Hardware Status	Line Quality	Sync State	Download Done	ASM State	ASM Loss Of Signal	PCM Clock	Loss Of Sync Word	DPLL Locked
1	None	down(0)	operationa...	poor(0)	0	yes(1)	asm-Train...	loss(1)	valid(0)	loss(4)	notLocked...
2	None	down(0)	operationa...	poor(0)	0	yes(1)	asm-Train...	loss(1)	valid(0)	loss(4)	notLocked...
3	None	down(0)	operationa...	poor(0)	0	yes(1)	asm-Deac...	loss(1)	valid(0)	loss(4)	notLocked...
4	None	down(0)	operationa...	poor(0)	0	yes(1)	asm-Deac...	loss(1)	valid(0)	loss(4)	notLocked...
5	None	down(0)	operationa...	poor(0)	0	yes(1)	asm-Deac...	loss(1)	valid(0)	loss(4)	notLocked...
6	None	down(0)	operationa...	poor(0)	0	yes(1)	asm-Deac...	loss(1)	valid(0)	loss(4)	notLocked...
7	None	down(0)	operationa...	poor(0)	0	yes(1)	asm-Deac...	loss(1)	valid(0)	loss(4)	notLocked...
8	None	down(0)	operationa...	poor(0)	0	yes(1)	asm-Deac...	loss(1)	valid(0)	loss(4)	notLocked...
9	None	down(0)	operationa...	poor(0)	0	yes(1)	asm-Deac...	loss(1)	valid(0)	loss(4)	notLocked...
10	None	down(0)	operationa...	poor(0)	0	yes(1)	asm-Deac...	loss(1)	valid(0)	loss(4)	notLocked...
11	None	down(0)	operationa...	poor(0)	0	yes(1)	asm-Deac...	loss(1)	valid(0)	loss(4)	notLocked...
12	None	down(0)	operationa...	poor(0)	0	yes(1)	asm-Deac...	loss(1)	valid(0)	loss(4)	notLocked...
13	None	down(0)	operationa...	poor(0)	0	yes(1)	asm-Deac...	loss(1)	valid(0)	loss(4)	notLocked...
14	None	down(0)	operationa...	poor(0)	0	yes(1)	asm-Deac...	loss(1)	valid(0)	loss(4)	notLocked...
15	None	down(0)	operationa...	poor(0)	0	yes(1)	asm-Deac...	loss(1)	valid(0)	loss(4)	notLocked...
16	None	down(0)	operationa...	poor(0)	0	yes(1)	asm-Deac...	loss(1)	valid(0)	loss(4)	notLocked...

Figure 79. 3096RC G.SHDSL Reports

Configuring IP Routing

ou may configure a host and routes for the 3096RC through the FS6300 NMS. The **IP Overview** window shows details for routing destinations, and includes information for gateway, cost, interface, protocol, and state of each route.



Destination	Mask	Gateway	Cost	Interface	Protocol	State
0.0.0.0	0.0.0.0	192.168.3.88	1	1	user(2)	active(2)
192.168.3.0	255.255.255.0	0.0.0.0	1	1	local(1)	active(2)

Note: To Modify / Delete an existing IP Route, select a row in the IP Route Details table. In the window that pops up, make the required changes and submit

Figure 80. 3096RC IP Overview

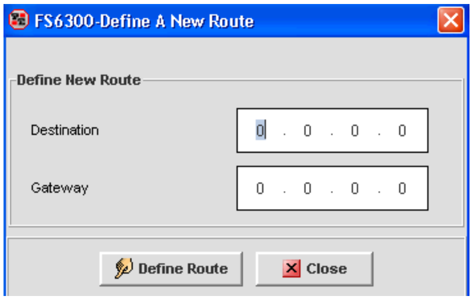
The table in the **IP Overview** window shows a list of defined routes for the 3096RC, and includes the following information for each entry:

- **Destination:** The destination IP address of this route. An entry with a value of 0.0.0.0 is considered a default route.
- **Mask:** The mask that is logical-ANDed with the destination address before being compared to the value in the Destination field.
- **Gateway:** The IP address where the packets should be forwarded.
- **Cost:** The cost of the route as defined by RIP standards. Cost is sometimes considered to be number of hops.
- **Interface:** The index value that uniquely identifies the local interface through which the next hop of this route should be reached.
- **Protocol:** The routing mechanism via which this route was learned.
  - *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 managemen tools.
  - *rip(4)*—Learned via reception of RIP packet.
  - *icmp(5)*—Learned via reception of ICMP packet
- **State:** Shows if a route is valid/in use.

Add Routes

To add an IP route to the 3096RC:

1. In the **IP Overview** window for the 3096RC, click the **Add** button to define a new route.



Destination 0 . 0 . 0 . 0

Gateway 0 . 0 . 0 . 0

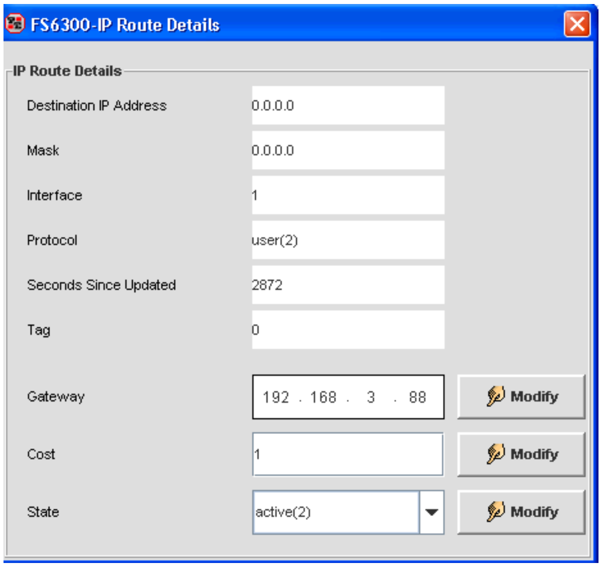
Figure 81. Add a New Route for 3096RC

2. Enter a **Destination** address for the new route. An entry with a value of 0.0.0.0 is considered a default route.
3. Enter a **Gateway** address for the new route. The gateway address specifies the IP address where the packets should be forwarded.
4. Click **Define Route**.

Modify Routes

To modify an existing IP route for the 3096RC:

1. In the **IP Overview** window for the 3096RC, select the entry in the table of the route you want to modify.



Destination IP Address	0.0.0.0
Mask	0.0.0.0
Interface	1
Protocol	user(2)
Seconds Since Updated	2872
Tag	0
Gateway	192 . 168 . 3 . 88
Cost	1
State	active(2)

Figure 82. Modifying a Route for 3096RC

2. The **IP Route Details** window displays. You may only modify the gateway address, cost, and state of the route.
3. Enter your desired changes and click **Modify** for each change. A confirmation message displays.

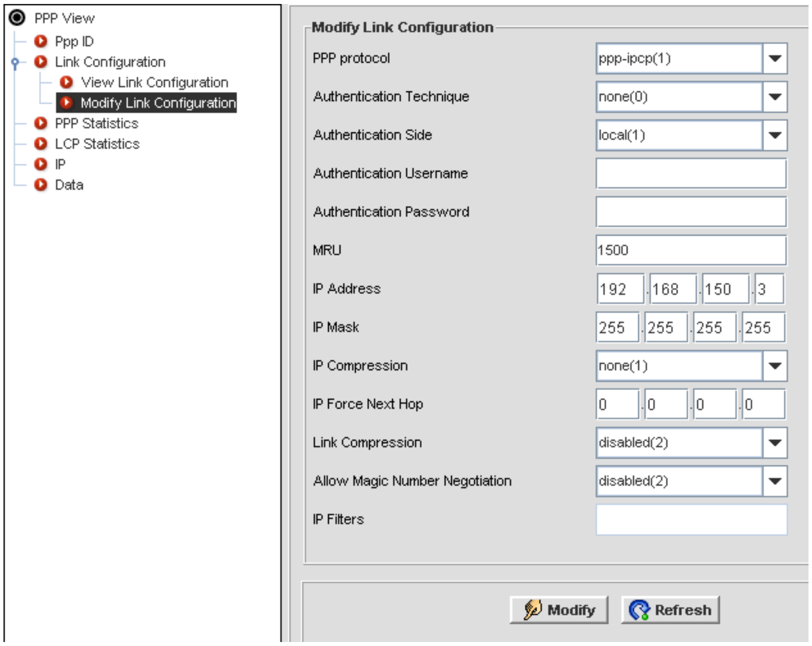
Configuring PPP

Click on **PPP Configuration** to view PPP links for the card. You may also modify the link configuration and default packet settings for PPP links.

Modify PPP Link Configuration

To configure PPP links for the card:

1. Right-click on the card in the main window and select **PPP Configuration**. The **PPP3096** window displays.
2. Click on **PPP View** and select an entry to edit from the table. The **FS6300-PPP** window displays.
3. Select **Modify Link Configuration**..



Modify Link Configuration

PPP protocol	ppp-ipcp(1)
Authentication Technique	none(0)
Authentication Side	local(1)
Authentication Username	
Authentication Password	
MRU	1500
IP Address	192 .168 .150 .3
IP Mask	255 .255 .255 .255
IP Compression	none(1)
IP Force Next Hop	0 .0 .0 .0
Link Compression	disabled(2)
Allow Magic Number Negotiation	disabled(2)
IP Filters	

Figure 83. PPP Link Configuration

4. Edit the desired options:
   - **PPP Protocol:** The desired kind of PPP protocol.
     - ppp-ipcp(1) —point-to-point protocol
     - ppp-bcp(2)—bridge control protocol
   - **Authentication Technique:** The login technique to use for authentication.
     - none(0)—No authentication will be used
     - pap(3)—password authentication protocol will be used
     - chap(4)—challenge handshake authentication protocol will be used
     - chapORpap(5)—chap will be negotiated first, if that fails, pap will be attempted

– **Authentication Side:** The side of the link which will be authenticating.

  • local(1)—local server will be authenticating. Remote needs to log into local server.

  • remote(2)—remote server will be authentication. Local needs to log into remote server.

– **Authentication Username and Password:** The username and password that will be sent to the remote side if the remote machine is authenticating.

– **MRU:** The setting for Maximum Receive Unit (MRU), used for the PPP negotiation.

– **IP Address:** The IP address that will be used for the PPP link.

– **IP Mask:** The IP mask that will be used for the PPP link.

– **IP Compression:** Set whether Van Jacobson (*vj-tcp(2)*) header compression is used or not (*none(1)*).

– **IP Force Next Hop:** The IP address of the interface, which should be the next hop for the packets—fast routing

– **Link Compression:** Enables the PPP link layer address and protocol field compression. When enabled the PPP negotiations will desire link compression but may disable the compression due the other end of the link not accepting link compression. When disabled the PPP negotiations will force no compression on the PPP link.

  • enabled(1)—enable link compression

  • disabled(2)—disable link compression

– **Allow Magic Number Negotiation:** Determines if magic number negotiation should be done.

  • enabled(1)—enable magic number negotiation

  • disabled(2)—disable magic number negotiation

– **IP Filters:** This option is not modifiable through the FS6300 NMS. Refer to the *3096RC Administrator's Reference Guide* for more information on IP filtering.

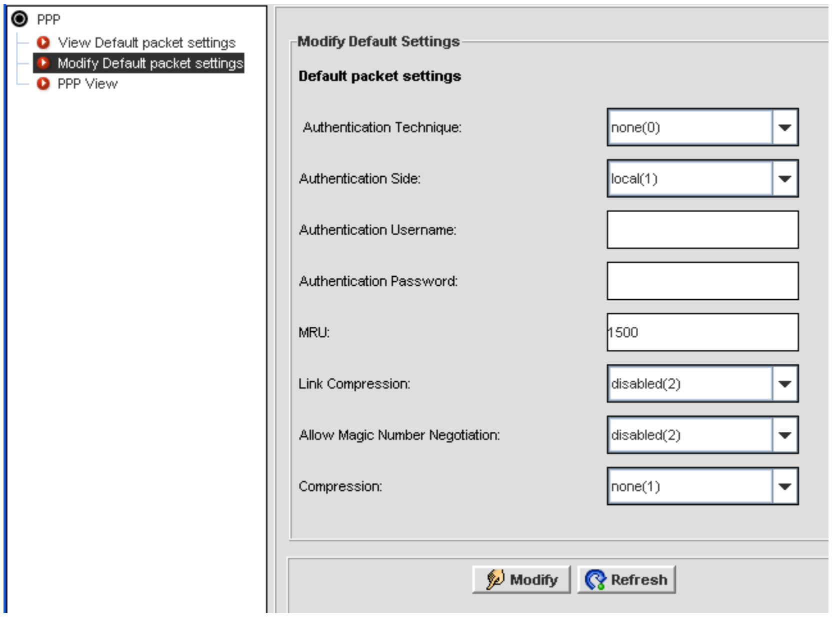
5. Click **Modify** to apply your changes.

Modify Default Packet Settings

You may modify the default PPP settings that each PPP link will take when first initialized. See “Modify PPP Link Configuration” on page 95 for modifying settings for individual links.

To modify default packet settings for PPP links:

1. Right-click on the card in the main window and select **PPP Configuration**. The **PPP2616** window displays.
2. Select **Modify Link Configuration**.



Modify Default Settings

Default packet settings

Authentication Technique: none(0)

Authentication Side: local(1)

Authentication Username:

Authentication Password:

MRU: 1500

Link Compression: disabled(2)

Allow Magic Number Negotiation: disabled(2)

Compression: none(1)

Figure 84. PPP Default Packet Settings

3. Edit the desired options:
   - **Authentication Technique:** The login technique to use for authentication.
     - none(0)—No authentication will be used
     - pap(3)—password authentication protocol will be used
     - chap(4)—challenge handshake authentication protocol will be used
     - chapORpap(5)—chap will be negotiated first, if that fails, pap will be attempted
   - **Authentication Side:** The side of the link which will be authenticating.
     - local(1)—local server will be authenticating. Remote needs to log into local server.
     - remote(2)—remote server will be authentication. Local needs to log into remote server.
   - **Authentication Username and Password:** The username and password that will be sent to the remote side if the remote machine is authenticating.
   - **MRU:** The setting for Maximum Receive Unit (MRU), used for the PPP negotiation.

- **Link Compression:** Enables the PPP link layer address and protocol field compression. When enabled the PPP negotiations will desire link compression but may disable the compression due the other end of the link not accepting link compression. When disabled the PPP negotiations will force no compression on the PPP link.
  - enabled(1)—enable link compression
  - disabled(2)—disable link compression
- **Allow Magic Number Negotiation:** Determines if magic number negotiation should be done.
  - enabled(1)—enable magic number negotiation
  - disabled(2)—disable magic number negotiation
- **Compression:** If none(1), then the local node will not attempt to negotiate any IP compression option. Otherwise, the local node will attempt to negotiate compression mode. Changing this option will have effect when the link restarts.
  - none(1)—do not negotiate IP compression negotiated (default)
  - vj-tcp(2)—van-jacobson TCP/IP header compression will be negotiated per RFC 1332.

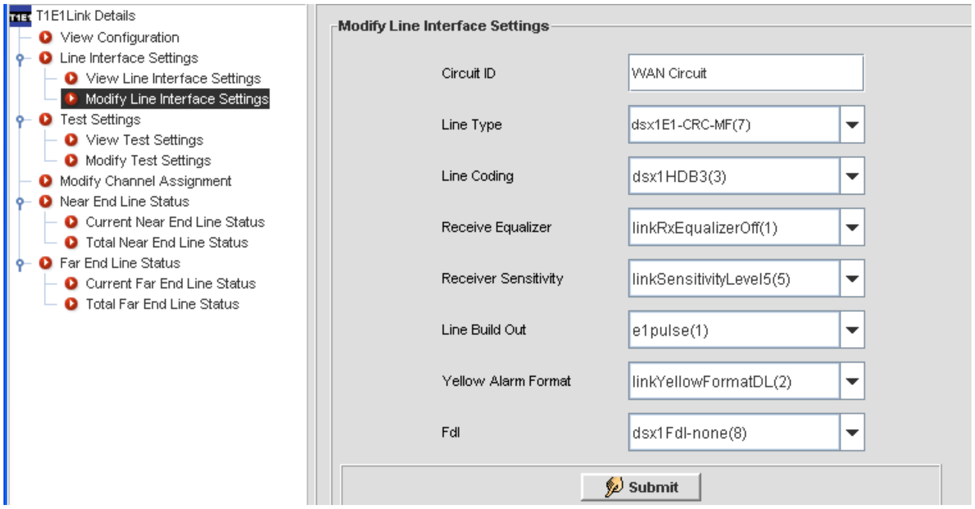
Configuring the T1/E1 Ports

Click on **T1E1 Port Configuration** to view T1/E1 links for the card. Select an entry in the table to configure line interfaces, test settings, and channel assignments for T1/E1 ports.

View Configuration

In the **T1-E1 Port Configuration** window for the selected link, click on **View Configuration**. If there are alarms for the link, click on **Alarms Present** to view the alarm details for the link.

Modify Line Interface Settings


T1E1Link Details
View Configuration
Line Interface Settings
View Line Interface Settings
Modify Line Interface Settings
Test Settings
View Test Settings
Modify Test Settings
Modify Channel Assignment
Near End Line Status
Current Near End Line Status
Total Near End Line Status
Far End Line Status
Current Far End Line Status
Total Far End Line Status
Submit

Modify Line Interface Settings

Circuit ID	WAN Circuit
Line Type	dsx1E1-CRC-MF(7)
Line Coding	dsx1HDB3(3)
Receive Equalizer	linkRxEqualizerOff(1)
Receiver Sensitivity	linkSensitivityLevel5(5)
Line Build Out	e1pulse(1)
Yellow Alarm Format	linkYellowFormatDL(2)
Fdl	dsx1Fdl-none(8)

Figure 85. T1/E1 Link Configuration window

1. In the **T1-E1 Port Configuration** window for the selected link, click on **Modify Line Interface Settings**.
2. Edit the desired options:

   – **Circuit ID:** The transmission vendor’s circuit identifier, for the purpose of facilitating troubleshooting.

   – **Line Type:** the type of DS1 Line implemented on this circuit. The type of circuit affects the number of bits per second that the circuit can reasonably carry, as well as the interpretation of the usage and error statistics. Select fromt he following values:

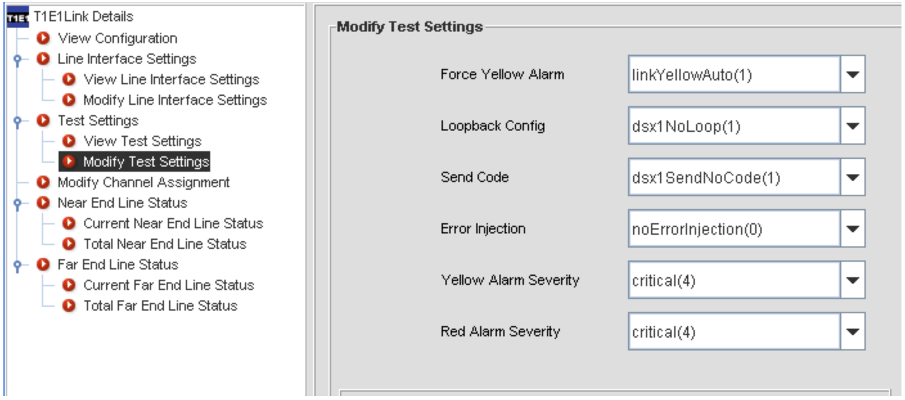
   - other(1)—Link is disabled
   - dsx1ESF(2)—Extended Superframe DS1
   - dsx1D4(3)—AT&T D4 format DS1
   - dsx1E1(4)—Based on CCITT/ITU G.704 without CRC (Cyclical Redundancy Check)
   - dsx1E1-CRC(5)—Based on CCITT/ITU G.704 with CRC (Cyclical Redundancy Check)
   - dsx1E1-MF(6)—Based on CCIT/ITU G.704 without CRC (bit oriented signaling)
   - dsx1E1-CRC-MF(7)—Based on CCIT/ITU G.704 with CRC (bit oriented signaling)
   - dsx1E1-Transparent(8)—Based on CCIT/ITU G.703 without CRC (Cyclical Redundancy Check)

- **Line Coding:** The type of Zero Code Suppression used on the link.
  - dsx1JBZS(1)—Jammed Bit Zero Suppression, in which the AT&T specification of at least one pulse every 8 bit periods is literally implemented by forcing a pulse in bit 8 of each channel. Thus, only seven bits per channel, or 1.344 Mbps, is available for data. This feature is not currently implemented.
  - dsx1B8ZS(2)—The use of a specified pattern of normal bits and bipolar violations which are used to replace a sequence of eight zero bits. The most common coding for T1 circuits.
  - dsx1HDB3(3)—This line coding is used with most E1 circuits today.
  - dsx1ZBTSI(4)—May use dsx1ZBTSI, or Zero Byte Time Slot Interchange. This feature is not currently implemented.
  - dsx1AMI(5)—Refers to a mode wherein no zero code suppression is present and the line encoding does not solve the problem directly. In this application, the higher layer must provide data which meets or exceeds the pulse density requirements, such as inverting HDLC data.
  - other(6)—This feature is not currently supported.
- **Receive Equalizer:** The equalization used on the received signal. Long haul signals should have the equalization set for more. Short haul signals require less equalization.
- **Receiver Sensitivity:** The minimum voltage at which the WAN port will sense that the signal is available. This variable is only used if the **Receiver Equalization** is set to **ON**.
- **Line Build Out:** The T1 or E1 pulse levels used by the T1/E1 ports:
  - triState(0)—When the T1/E1 port is not in use, you may want to place the port in tri-state mode. While in this setting, the input lines to the port are placed in high impedance protection mode.
  - e1pulse(1)—Used when connecting the T1/E1 port to E1 lines.
  - t1pulse0dB(2)—Strong T1 pulse amplitude.
  - t1pulse-7dB(3)—Medium T1 pulse amplitude.
  - t1pulse-15dB(4)—Weak T1 pulse amplitude.
- **Yellow Alarm Format:** The standard used to transmit and identify the Yellow Alarm.
  - link YellowFormatBit2(1)—Bit-2 equal zero in every channel
  - link YellowFormatDL(2)—FF00 pattern in the Data Link
  - link YellowFormatFrame12FS(3)—FS bit of frame 12
- **Fdl:** implementation of FDL is being used, if any. FDL applies only to T1 circuits.
  - other(1)—Indicates that a protocol other than one following is used.
  - dsx1Ansi-T1-403(2)—Refers to the FDL exchange recommended by ANSI.
  - dsx1Att-54016(3)—Refers to ESF FDL exchanges.
  - dsx1Fdl-none(4)—Indicates that the device does not use the FDL.

  If one of the E1 line types has been selected, set **Fdl** to **dsx1Fdl-none(8)**.

3. Click **Submit** to commit your changes.

Modify Test Settings


T1E1Link Details
View Configuration
Line Interface Settings
View Line Interface Settings
Modify Line Interface Settings
Test Settings
View Test Settings
Modify Test Settings
Modify Channel Assignment
Near End Line Status
Current Near End Line Status
Total Near End Line Status
Far End Line Status
Current Far End Line Status
Total Far End Line Status

Modify Test Settings

Force Yellow Alarm: linkYellowAuto(1)

Loopback Config: dsx1NoLoop(1)

Send Code: dsx1SendNoCode(1)

Error Injection: noErrorInjection(0)

Yellow Alarm Severity: critical(4)

Red Alarm Severity: critical(4)

Figure 86. T1/E1 Test Settings

1. In the **T1-E1 Port Configuration** window for the selected link, click on **Modify Test Settings**.
2. Edit the desired options:

   – **Force Yellow Alarm:** The standard used to transmit and identify the Yellow Alarm.

   • linkYellowAuto—Do not force the transmission of a yellow alarm. But, yellow alarm may be automatically transmitted.

   • linkYellowOn—Force the transmission of a yellow alarm even if the received signal is in frame.

   • linkYellowDisable—Do NOT transmit a yellow alarm even if the received signal is out of frame.

   – **Loopback Configuration:** The loopback configuration of the DS1 interface.

   • dsx1NoLoop(1)—Not in the loopback state. A device that is not capable of performing a loopback on the interface shall always return this as it's value.

   • dsx1PayloadLoop(2)—The received signal at this interface is looped through the device. Typically the received signal is looped back for retransmission after it has passed through the device's framing function.

   • dsx1LineLoop(3)—The received signal at this interface does not go through the device (minimum penetration) but is looped back out.

   • dsx1OtherLoop(4)—Loopbacks that are not defined here.

   – **Send Code:** The type of code is being sent across the DS1 interface by the device.

   • dsx1SendNoCode(1)—Sending looped or normal data

   • dsx1SendLineCode(2)—Sending a request for a line loopback

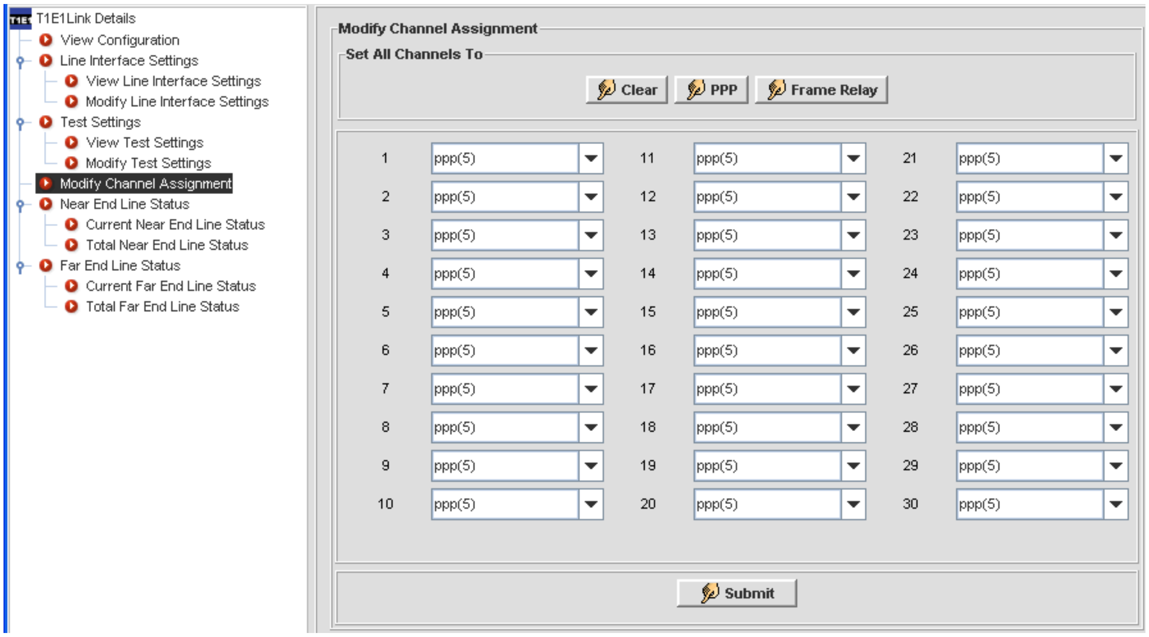
   • dsx1SendResetCode(4)—Sending a loopback termination request

   – **Error Injection:** Force an output error to see if the other end detects it.

   – **Yellow Alarm Severity:** Critical / Major / Minor / Info / Ignore

   – **Red Alarm Severity:** Critical / Major / Minor / Info / Ignore
3. Click **Submit** to commit your changes.

Modify Channel Assignments


T1E1Link Details
View Configuration
Line Interface Settings
View Line Interface Settings
Modify Line Interface Settings
Test Settings
View Test Settings
Modify Test Settings
Modify Channel Assignment
Near End Line Status
Current Near End Line Status
Total Near End Line Status
Far End Line Status
Current Far End Line Status
Total Far End Line Status
Modify Channel Assignment
Set All Channels To
Clear
PPP
Frame Relay
Submit

1	ppp(5)	11	ppp(5)	21	ppp(5)
2	ppp(5)	12	ppp(5)	22	ppp(5)
3	ppp(5)	13	ppp(5)	23	ppp(5)
4	ppp(5)	14	ppp(5)	24	ppp(5)
5	ppp(5)	15	ppp(5)	25	ppp(5)
6	ppp(5)	16	ppp(5)	26	ppp(5)
7	ppp(5)	17	ppp(5)	27	ppp(5)
8	ppp(5)	18	ppp(5)	28	ppp(5)
9	ppp(5)	19	ppp(5)	29	ppp(5)
10	ppp(5)	20	ppp(5)	30	ppp(5)

Figure 87. T1/E1 Channel Assignment

In the **Modify Channel Assignment** section of the **T1/E1 Link Configuration** window, you can change selected DS0 channels to carry in-band management information over Frame Relay or PPP links. You can use the buttons at the top of the window to modify all 30 timeslots at once. Or, you can use the 30 drop-down menus to modify selected timeslots individually. Click **Submit** to apply your changes for individual links.

View Line Status

There are two types of line status statistics that you may view in the T1/E1 Link Configuration window – **Near End Line Status** and **Far End Line Status**.

- **Near End Line Status** – Click on **Current Near End Line Status** to view statistics for current near end performance. Click on **Total Near End Line Status** to view statistics totals for near end performance.
- **Far End Line Status** – Click on **Current Far End Line Status** to view statistics for current far end performance. Click on **Total Far End Line Status** to view statistics totals for far end performance.

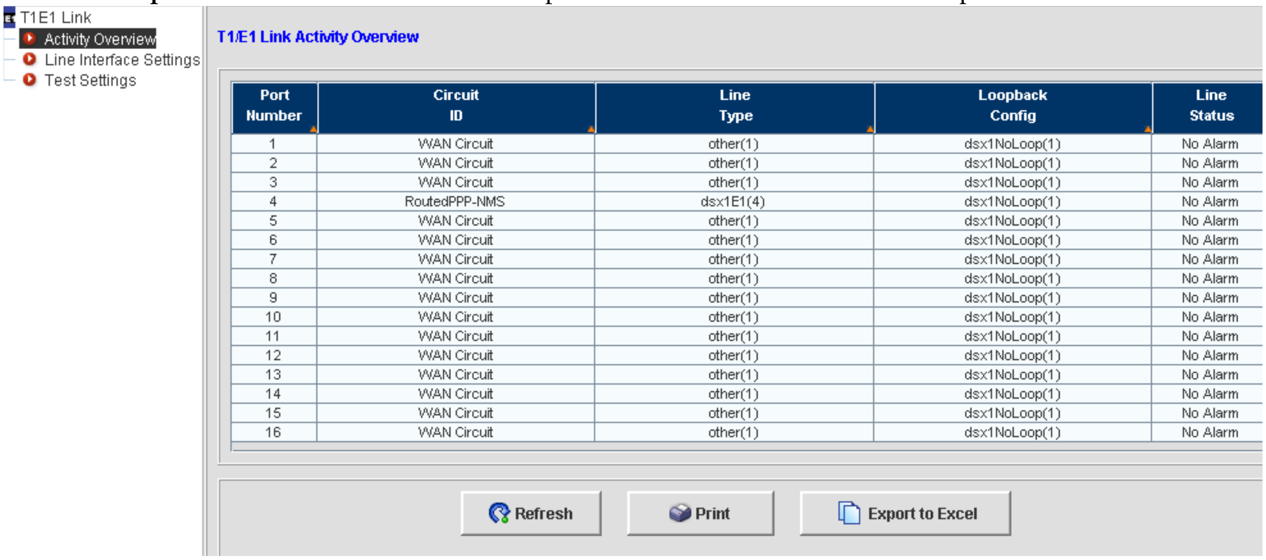
> **Note** Refer to the *3096RC Adminsitrator's Reference Guide* for detailed information about line status statistics.

Viewing T1/E1 Reports

Click on **T1E1 Reports** to view and print different reports about the activity, line interface settings, and test settings of T1/E1 links on the 3096RC card.

Click the **Print** button to send the report to a printer on your network.

Click the **Export to Excel** button to send the report to Microsoft Excel to save in a spreadsheet.



T1/E1 Link Activity Overview

Port Number	Circuit ID	Line Type	Loopback Config	Line Status
1	WAN Circuit	other(1)	dsx1NoLoop(1)	No Alarm
2	WAN Circuit	other(1)	dsx1NoLoop(1)	No Alarm
3	WAN Circuit	other(1)	dsx1NoLoop(1)	No Alarm
4	RoutedPPP-NMS	dsx1E1(4)	dsx1NoLoop(1)	No Alarm
5	WAN Circuit	other(1)	dsx1NoLoop(1)	No Alarm
6	WAN Circuit	other(1)	dsx1NoLoop(1)	No Alarm
7	WAN Circuit	other(1)	dsx1NoLoop(1)	No Alarm
8	WAN Circuit	other(1)	dsx1NoLoop(1)	No Alarm
9	WAN Circuit	other(1)	dsx1NoLoop(1)	No Alarm
10	WAN Circuit	other(1)	dsx1NoLoop(1)	No Alarm
11	WAN Circuit	other(1)	dsx1NoLoop(1)	No Alarm
12	WAN Circuit	other(1)	dsx1NoLoop(1)	No Alarm
13	WAN Circuit	other(1)	dsx1NoLoop(1)	No Alarm
14	WAN Circuit	other(1)	dsx1NoLoop(1)	No Alarm
15	WAN Circuit	other(1)	dsx1NoLoop(1)	No Alarm
16	WAN Circuit	other(1)	dsx1NoLoop(1)	No Alarm

Figure 88. 3096RC T1/E1 Reports

Viewing the T1/E1 Map Layer

Click on **Display T1E1 Map Layer** to show a map of all the T1/E1 ports on the card. Right-click on a port in the map to configure its link. See "Configuring the T1/E1 Ports" on page 99 for more details.

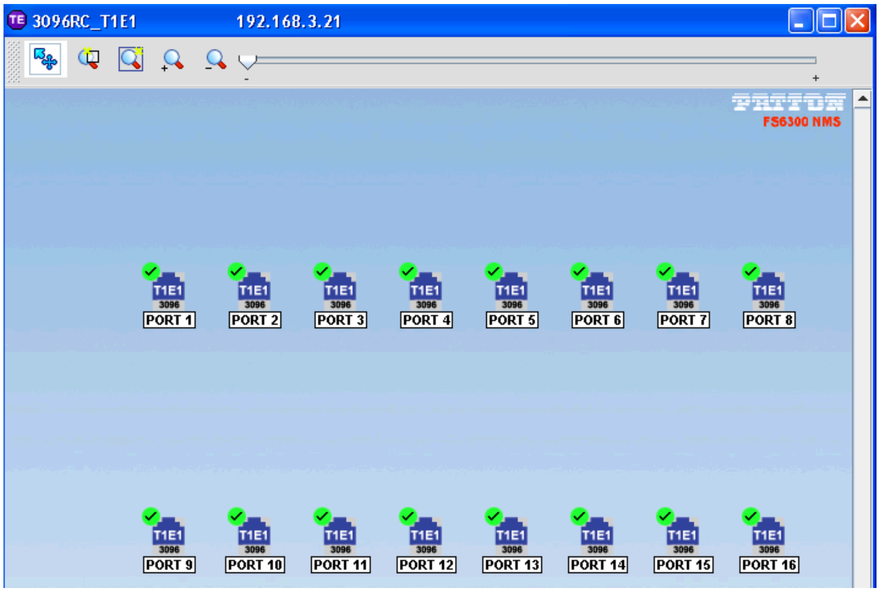


Figure 89. 3096RC T1/E1 Port Map

Viewing the G.SHDSL Map Layer

Click on **Display G.SHDSL Map Layer** to show a map of all the G.SHDSL ports on the card. Right-click on a port in the map to configure its link. See "Configuring G.SHDSL Ports" on page 88 for more details.

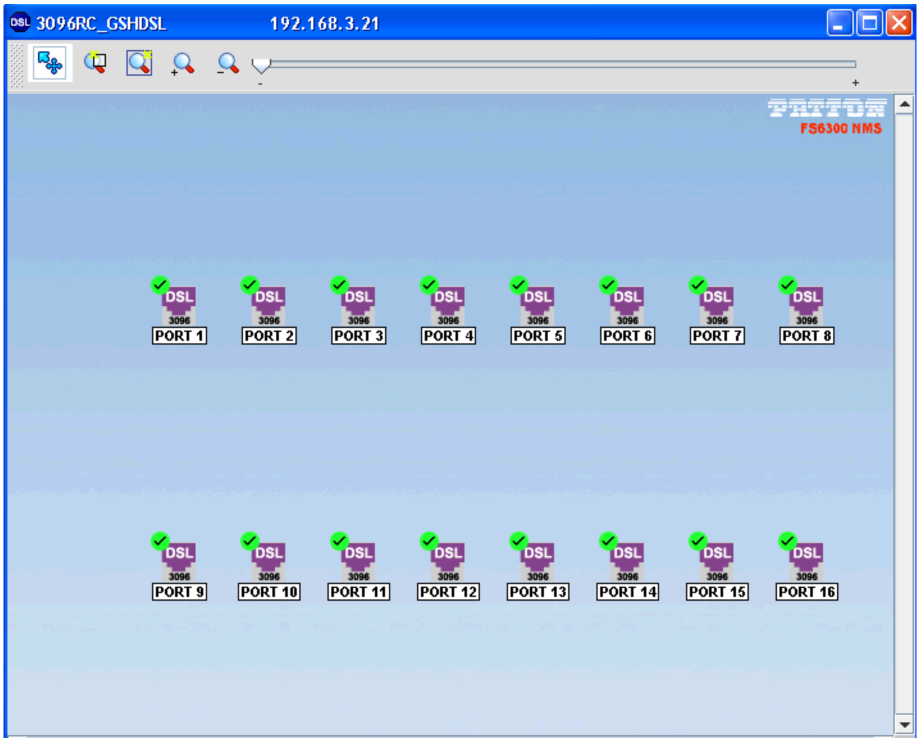


Figure 90. 3096RC G.SHDSL Port Map

Chapter 7 Configuring the 3196RC Card

Chapter contents

Introduction

The Patton Model 3196RC is a TDM concentrator with 16 iDSL ports. There are several ways to reach the configuration menu for the 3196RC card:

- Click on **Network Maps** in the main menu tree, then click on **Chassis.** Right-click on the 3196RC icon.
- Select the **3196RC** card from the main menu tree, then right-click on the card icon in the main window.
- Navigate to **Network Database** > **Managed Objects** > **Cards** in the main menu tree, then right-click on the IP address of the card in the table in the main window.

The best way to reach the configuration menu for a card is to select the card in the main menu tree, then right-click on the card's icon in the main window.

3196RC Configuration Menu

The following options are available in the pull-down menu for the 3196RC card:

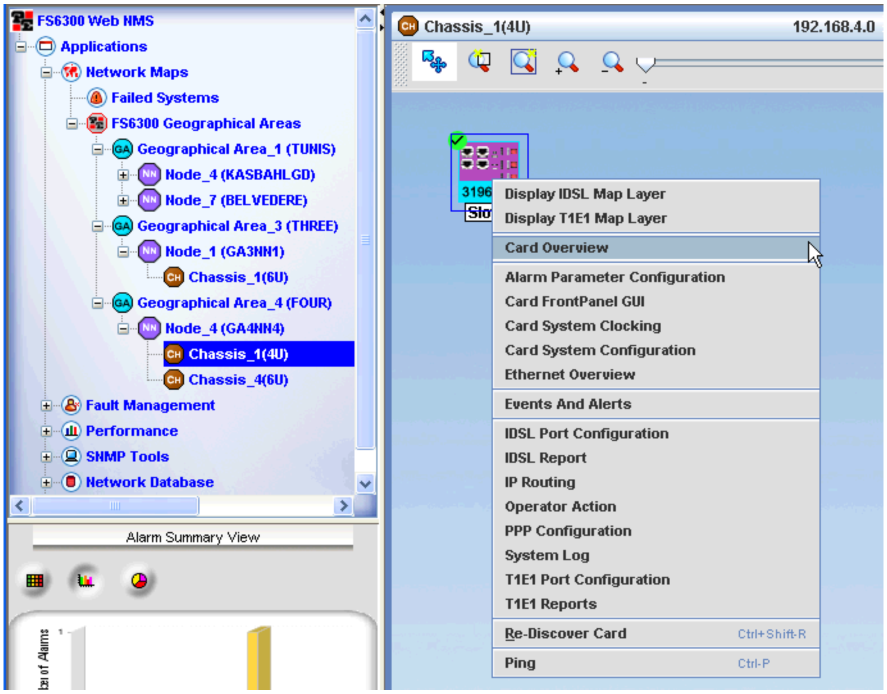


Figure 91. 3196RC Configuration Menu

- Display iDSL Map Layer – See "Viewing the iDSL Map Layer" on page 125
- Display T1E1 Map Layer – See "Viewing the T1/E1 Map Layer" on page 124
- Card Overview – Shows information for Box Status, Card Info, and Alarm Info
- Alarm Parameter Configuration – See "Configuring Alarms through a Card in the Chassis" on page 48
- Card Front Panel GUI – See "Viewing the Front Panel" on page 107
- Card System Clocking – See "Configuring Card System Clocking" on page 54
- Card System Configuration – See "Configuring the Card System" on page 107

- Ethernet Overview – See “Configuring Ethernet Settings” on page 109
- Events and Alerts – See “Viewing Events and Alerts” on page 62
- iDSL Port Configuration – See “Configuring iDSL Ports” on page 110
- iDSL Report – See “Viewing iDSL Reports” on page 113
- IP Routing – See “Configuring IP Routing” on page 114
- Operator Action – See “Managing Operator Actions” on page 60
- PPP Configuration – See “Configuring PPP” on page 116
- System Log – See “Viewing/Modifying System Log Configuration” on page 65
- T1E1 Port Configuration – See “Configuring the T1/E1 Ports” on page 120
- T1E1 Reports – See “Viewing T1/E1 Reports” on page 124
- Re-Discover Card – See “Re-Discovering Cards Manually” on page 38
- Ping – Displays a status message after pinging the interface.

Viewing the Front Panel

Click on **Card Front Panel GUI** to view the front panel of the card in real-time.

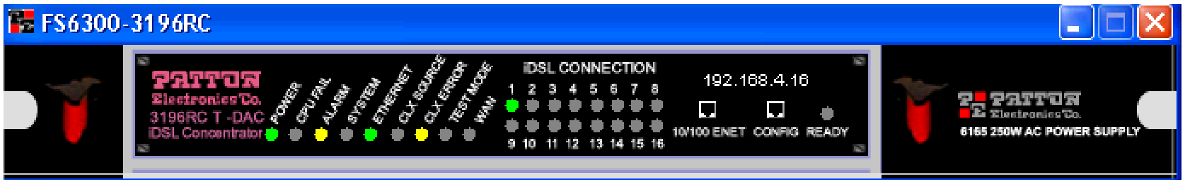


Figure 92. 3196RC Front Panel LEDs

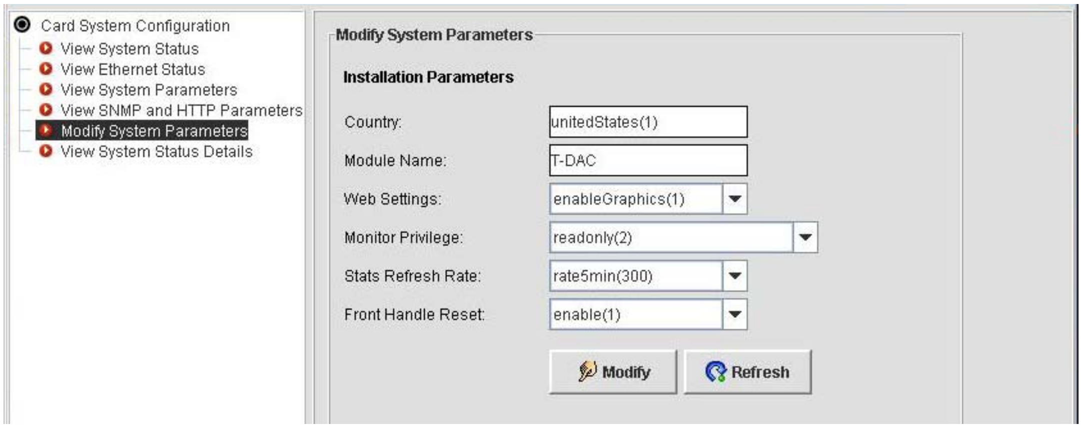
Configuring the Card System

Click on **Card System Configuration** to configure system parameters. You can also view the system status, ethernet status, system parameters, SNMP and HTTP Parameters, and system status details.

Modify System Parameters

If you only want to view the system parameters, click on **View System Parameters** in the Card System Configuration window.

To configure the card system, click on **Modify System Parameters** in the menu tree in the Card System Configuration window (see Figure 93 on page 108).



Modify System Parameters

Installation Parameters

Country: unitedStates(1)

Module Name: T-DAC

Web Settings: enableGraphics(1)

Monitor Privilege: readonly(2)

Stats Refresh Rate: rate5min(300)

Front Handle Reset: enable(1)

Figure 93. Modify Card System Parameters

1. Select to enable or disable graphics from the **Web Settings** drop-down menu.
2. Select a privilege option for configuring the card through the NMS from the **Monitor Privilege** drop-down menu.
3. Select how often you would like to refresh statistics information from the **Stats Refresh Rate** drop-down menu.
4. Select to enable or disable front handle reset from the **Front Handle Reset** drop-down menu.
5. Click **Modify** to save your changes. Click **Refresh**.

View System Status

Click on **View System Status** in the Card System Configuration window to see an overview of the physical status of the card and the system status. **View System Status** shows information about the handle switches, front/rear LEDs, alarm and clock LEDs, and the board temperature.

View System Status Details

Click on **View System Status Details** in the Card System Configuration window to see information on CPU statistics, Message Block statistics, Memory statistics, Manufacturer details, and the Enclosure System temperature.

View Ethernet Status

Click on **View Ethernet Status** in the Card System Configuration window to see the LEDs and speeds of the card's Ethernet ports.

View SNMP and HTTP Parameters

Click on **View SNMP and HTTP Parameters** in the Card System Configuration window to see the SNMP version and passwords.

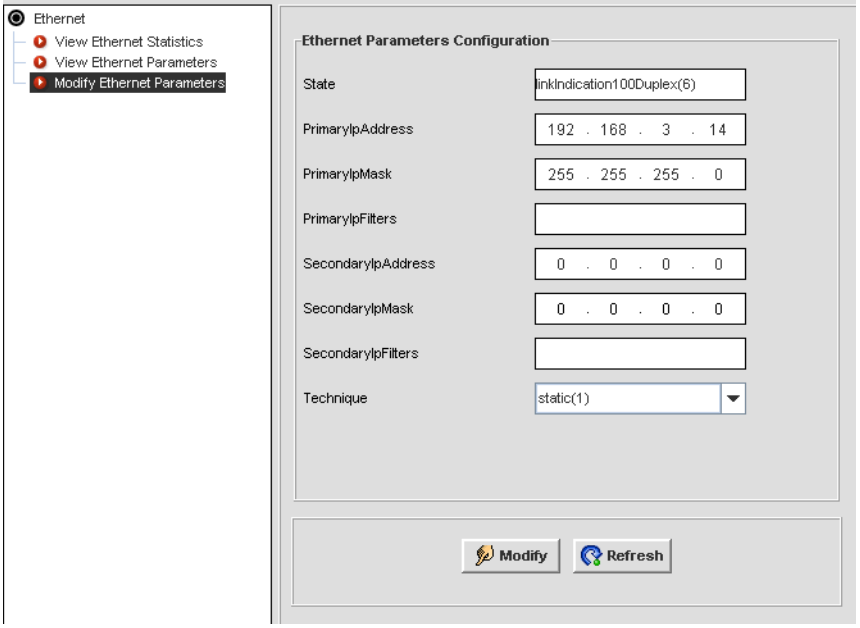
Configuring Ethernet Settings

Click on **Ethernet Overview** to configure Ethernet settings. You can also view Ethernet statistics.

Modify Ethernet Parameters

If you only want to view the Ethernet parameters, click on **View Ethernet Parameters** in the Ethernet Overview window.

To configure the Ethernet settings, click on **Modify Ethernet Parameters** in the menu tree in the Ethernet Overview window (see Figure 94).



Ethernet Parameters Configuration

State: inkIndication100Duplex(6)

PrimaryIpAddress: 192 . 168 . 3 . 14

PrimaryIpMask: 255 . 255 . 255 . 0

PrimaryIpFilters:

SecondaryIpAddress: 0 . 0 . 0 . 0

SecondaryIpMask: 0 . 0 . 0 . 0

SecondaryIpFilters:

Technique: static(1)

Figure 94. Modify Ethernet Parameters

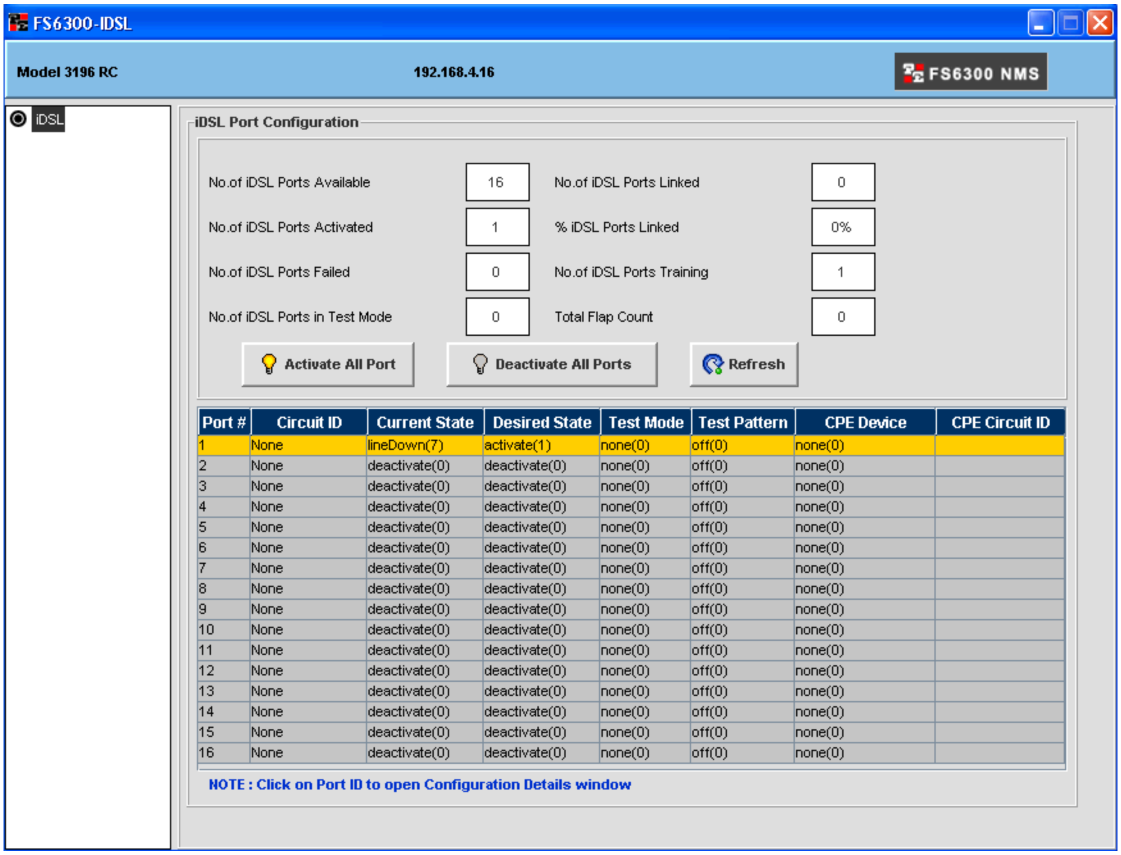
1. Enter the main address and mask for the card in the **Primary IP Address** and **IP Mask** fields.
2. The **IP Filter** needs to be provisioned through the card's configuration website. For more information on setting up IP Filters, refer to the *Model 3196RC Adminstrator's Reference Guide*.
3. From the **Technique** drop-down menu, select **static** if you want to statically assign the IP address, or select **disable** if you want to use DHCP to assign the IP address.
4. Click **Modify** to commit your changes. Click **Refresh**.

View Ethernet Statistics

Click on **View Ethernet Statistics** in the Ethernet Overview window to view statistics for the Ethernet ports on the device, such as errors and frame stats.

Configuring iDSL Ports

Click on **iDSL Port Configuration** in the pull-down menu to bring up the **iDSL** window. The iDSL window shows the number of iDSL ports available, linked ports, failed ports, training ports, and ports in test mode.



Model 3196 RC 192.168.4.16

iDSL Port Configuration

No.of iDSL Ports Available	16	No.of iDSL Ports Linked	0
No.of iDSL Ports Activated	1	% iDSL Ports Linked	0%
No.of iDSL Ports Failed	0	No.of iDSL Ports Training	1
No.of iDSL Ports in Test Mode	0	Total Flap Count	0

Port #	Circuit ID	Current State	Desired State	Test Mode	Test Pattern	CPE Device	CPE Circuit ID
1	None	lineDown(7)	activate(1)	none(0)	off(0)	none(0)	
2	None	deactivate(0)	deactivate(0)	none(0)	off(0)	none(0)	
3	None	deactivate(0)	deactivate(0)	none(0)	off(0)	none(0)	
4	None	deactivate(0)	deactivate(0)	none(0)	off(0)	none(0)	
5	None	deactivate(0)	deactivate(0)	none(0)	off(0)	none(0)	
6	None	deactivate(0)	deactivate(0)	none(0)	off(0)	none(0)	
7	None	deactivate(0)	deactivate(0)	none(0)	off(0)	none(0)	
8	None	deactivate(0)	deactivate(0)	none(0)	off(0)	none(0)	
9	None	deactivate(0)	deactivate(0)	none(0)	off(0)	none(0)	
10	None	deactivate(0)	deactivate(0)	none(0)	off(0)	none(0)	
11	None	deactivate(0)	deactivate(0)	none(0)	off(0)	none(0)	
12	None	deactivate(0)	deactivate(0)	none(0)	off(0)	none(0)	
13	None	deactivate(0)	deactivate(0)	none(0)	off(0)	none(0)	
14	None	deactivate(0)	deactivate(0)	none(0)	off(0)	none(0)	
15	None	deactivate(0)	deactivate(0)	none(0)	off(0)	none(0)	
16	None	deactivate(0)	deactivate(0)	none(0)	off(0)	none(0)	

NOTE : Click on Port ID to open Configuration Details window

Figure 95. 3196RC iDSL window

Activating/Deactivating All Ports

Click the **Activate All Ports** button to train all of the iDSL ports on the card.

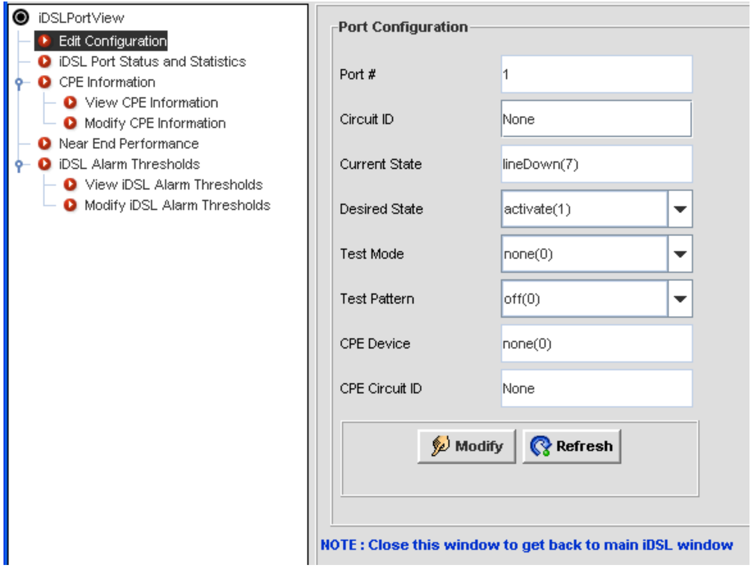
Click the **Deactivate All Ports** button to turn off all of the iDSL ports on the card.

Configuring Individual Ports

To configure an individual port, click on the port in the table to bring up the **Port Configuration** window. From the Port Configuration window, you can edit the port's configuration, view port information, edit CPE options, and modify alarm thresholds.

Edit Configuration

Click on **Edit Configuration** in the menu tree of the Port Configuration window. **Circuit ID**, **Desired State**, **Test Mode** and **Test Pattern** are configurable.



Port Configuration

Port # 1

Circuit ID None

Current State lineDown(7)

Desired State activate(1)

Test Mode none(0)

Test Pattern off(0)

CPE Device none(0)

CPE Circuit ID None

NOTE : Close this window to get back to main iDSL window

Figure 96. 3196RC Edit iDSL Configuration

1. Enter the **Circuit ID** (optional) in the text field.
2. Select an option from the **Desired State** drop-down menu:
   - Deactivated(0)—Select this option when the port is not currently connected to a remote CPE modem.
   - Activated(1)—Select this option to connect the port to a remote CPE modem for current active use.
   - Reset(2)—Select this option to reset the iDSL port.
3. Select an option from the **Test Mode** drop-down menu:
   - localLoop(1)—The T-DAC's iDSL port will operate in local loopback mode. Data transmitted through the 3196RC to the iDSL port is looped back to the transmitting port.
   - remoteLoop(2)—For a Patton CPE iDSL modem that provides a serial port (such as the model 1082), and that is remotely connected to this iDSL port, remoteLoop(2) changes the operating mode of the serial port. The 3196RC will cause the serial port on the remote CPE to operate in loopback mode.
   - lineLoop(3)—The 3196RC's iDSL port will operate in line loopback mode. For the CPE remotely connected to this port, you can use lineLoop(3) mode to test the iDSL link from the CPE to the 3196RC and back to the CPE.
   - none(0)— The default value for Test Mode.

4. Select an option from the **Test Pattern** drop-down menu. The Test Pattern parameter defines which test pattern the 3196RC will generate and transmit. The 3196RC will transmit the selected test pattern to the destination port defined by the option you selected for the Test Mode.
5. Click **Modify** to save your changes.

View Port Information

Click on **iDSL Port Status and Statistics** in the menu tree of the Port Configuration window to view erros and up times for the selected port.

Edit CPE Options

Click on **Modify CPE Information** in the menu tree of the Port Configuration window to edit the options for the CPE, such as the serial rate, DTE test mode, and front panel switches.

To edit the CPE options for a port:

1. Click on **Modify CPE Options** in the menu tree of the Port Configuration window.
2. Edit the desired, configurable options:
   – **Serial Rate:** Select from the following:

   rate19-2k(0) for serial rate of 19200 bps

   rate32k(1) for serial rate of 32000 bps

   rate56k(1) for serial rate of 56000 bps

   rate64k(1) for serial rate of 64000 bps

   rate128k(1) for serial rate of 128000 bps

   rate144k(1) for serial rate of 144000 bps

   – **Front Panel Switches:** Disable or enable front panel switches for the CPE.

   – **DTE Test Mode:** Enable or disable the CPE from initiating and responding to test patterns.

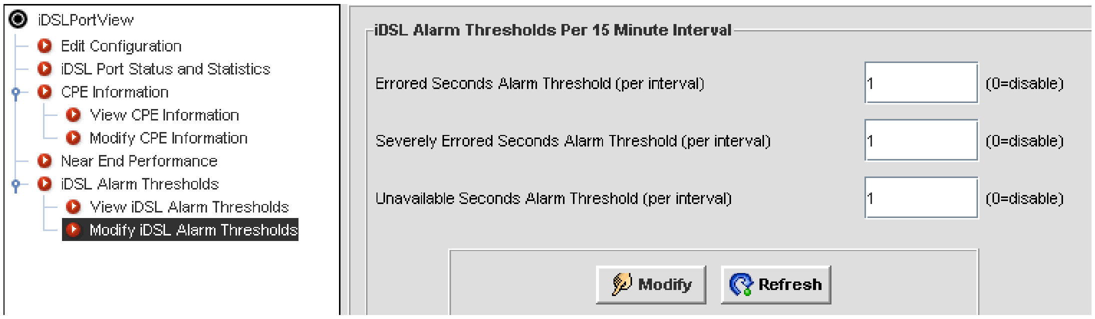
   – **User ID:** Enter a new User ID for the remote CPE.
3. Click **Modify** to save your changes.

Modify iDSL Alarm Thresholds

You may modify the number of errored seconds and unavailable seconds for which an alarm condition will be triggered for a selected iDSL port on the 3196RC.

To modify the iDSL alarm threshold:

1. Click on **Modify iDSL Alarm Thresholds** in the menu tree of the Port Configuration window.



iDSL Alarm Thresholds Per 15 Minute Interval

Errored Seconds Alarm Threshold (per interval) 1 (0=disable)

Severely Errored Seconds Alarm Threshold (per interval) 1 (0=disable)

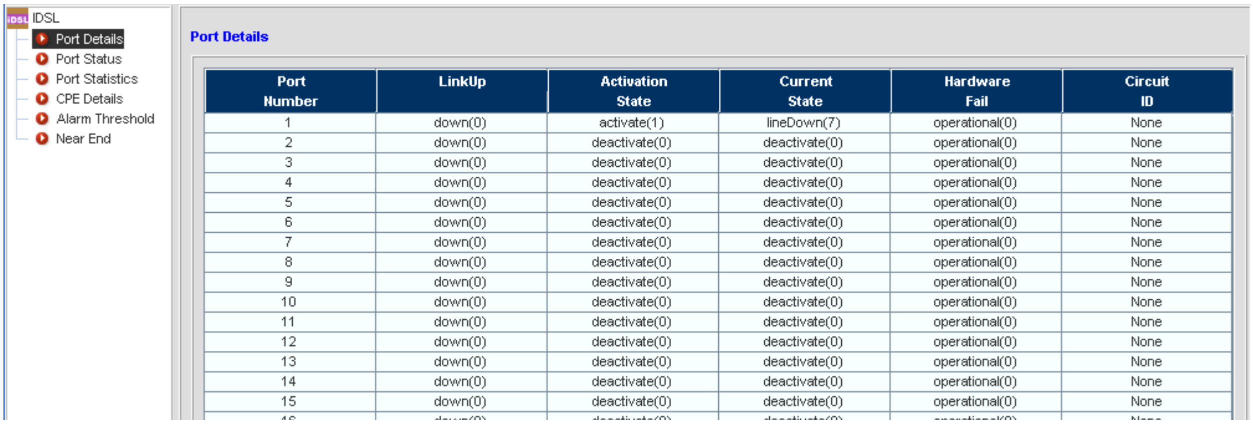
Unavailable Seconds Alarm Threshold (per interval) 1 (0=disable)

Figure 97. 3196RC Modify iDSL Alarm Thresholds

2. Edit the desired options:
   - **Errored Seconds Alarm Threshold (per interval)**—Enter a number of errored seconds that will trigger an alarm.
   - **Severely Errored Seconds Alarm Threshold (per interval)** - Enter a number of errored seconds that will trigger an alarm.
   - **Unavailable Seconds Alarm Threshold (per interval)** - Enter a number of unavailable seconds that will trigger an alarm.
3. Click **Modify** to apply your changes.

Viewing iDSL Reports

Click on **iDSL Report** to view different reports about port details, status, statistics, alarm threshold, and CPE details for the iDSL ports on the 3196RC card. Click the **Print** button to send the report to a printer on your network. Click the **Export to Excel** button to send the report to Microsoft Excel to save in a spreadsheet.



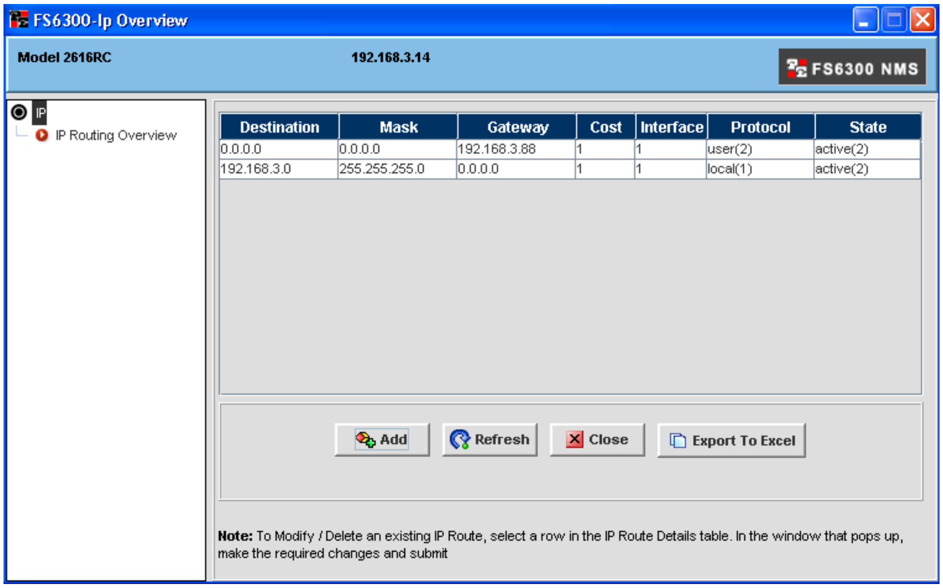
Port Details

Port Number	LinkUp	Activation State	Current State	Hardware Fail	Circuit ID
1	down(0)	activate(1)	lineDown(7)	operational(0)	None
2	down(0)	deactivate(0)	deactivate(0)	operational(0)	None
3	down(0)	deactivate(0)	deactivate(0)	operational(0)	None
4	down(0)	deactivate(0)	deactivate(0)	operational(0)	None
5	down(0)	deactivate(0)	deactivate(0)	operational(0)	None
6	down(0)	deactivate(0)	deactivate(0)	operational(0)	None
7	down(0)	deactivate(0)	deactivate(0)	operational(0)	None
8	down(0)	deactivate(0)	deactivate(0)	operational(0)	None
9	down(0)	deactivate(0)	deactivate(0)	operational(0)	None
10	down(0)	deactivate(0)	deactivate(0)	operational(0)	None
11	down(0)	deactivate(0)	deactivate(0)	operational(0)	None
12	down(0)	deactivate(0)	deactivate(0)	operational(0)	None
13	down(0)	deactivate(0)	deactivate(0)	operational(0)	None
14	down(0)	deactivate(0)	deactivate(0)	operational(0)	None
15	down(0)	deactivate(0)	deactivate(0)	operational(0)	None

Figure 98. 3196RC iDSL Reports

Configuring IP Routing

ou may configure a host and routes for the 3196RC through the FS6300 NMS. The **IP Overview** window shows details for routing destinations, and includes information for gateway, cost, interface, protocol, and state of each route.



Destination	Mask	Gateway	Cost	Interface	Protocol	State
0.0.0.0	0.0.0.0	192.168.3.88	1	1	user(2)	active(2)
192.168.3.0	255.255.255.0	0.0.0.0	1	1	local(1)	active(2)

Note: To Modify / Delete an existing IP Route, select a row in the IP Route Details table. In the window that pops up, make the required changes and submit

Figure 99. 3196RC IP Overview

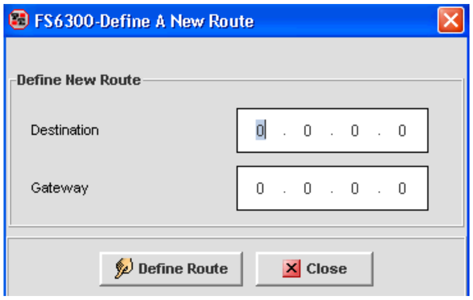
The table in the **IP Overview** window shows a list of defined routes for the 3196RC, and includes the following information for each entry:

- **Destination:** The destination IP address of this route. An entry with a value of 0.0.0.0 is considered a default route.
- **Mask:** The mask that is logical-ANDed with the destination address before being compared to the value in the Destination field.
- **Gateway:** The IP address where the packets should be forwarded.
- **Cost:** The cost of the route as defined by RIP standards. Cost is sometimes considered to be number of hops.
- **Interface:** The index value that uniquely identifies the local interface through which the next hop of this route should be reached.
- **Protocol:** The routing mechanism via which this route was learned.
  - *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 managemen tools.
  - *rip(4)*—Learned via reception of RIP packet.
  - *icmp(5)*—Learned via reception of ICMP packet
- **State:** Shows if a route is valid/in use.

Add Routes

To add an IP route to the 3196RC:

1. In the **IP Overview** window for the 3196RC, click the **Add** button to define a new route.



FS6300-Define A New Route

Define New Route

Destination 0 . 0 . 0 . 0

Gateway 0 . 0 . 0 . 0

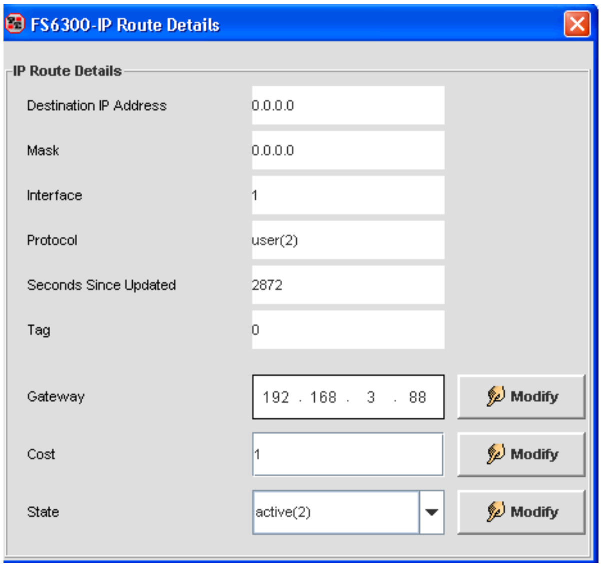
Figure 100. Add a New Route for 3196RC

2. Enter a **Destination** address for the new route. An entry with a value of 0.0.0.0 is considered a default route.
3. Enter a **Gateway** address for the new route. The gateway address specifies the IP address where the packets should be forwarded.
4. Click **Define Route**.

Modify Routes

To modify an existing IP route for the 3196RC:

1. In the **IP Overview** window for the 3196RC, select the entry in the table of the route you want to modify.



FS6300-IP Route Details

IP Route Details

Destination IP Address 0.0.0.0

Mask 0.0.0.0

Interface 1

Protocol user(2)

Seconds Since Updated 2872

Tag 0

Gateway 192 . 168 . 3 . 88

Cost 1

State active(2)

Figure 101. Modifying a Route for 3196RC

2. The **IP Route Details** window displays. You may only modify the gateway address, cost, and state of the route.
3. Enter your desired changes and click **Modify** for each change. A confirmation message displays.

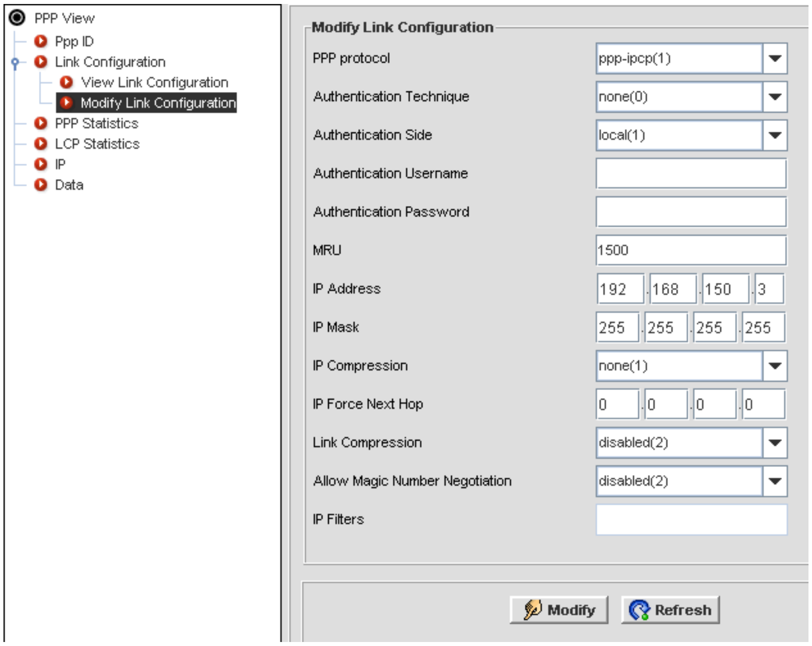
Configuring PPP

Click on **PPP Configuration** to view PPP links for the card. You may also modify the link configuration and default packet settings for PPP links.

Modify PPP Link Configuration

To configure PPP links for the card:

1. Right-click on the card in the main window and select **PPP Configuration**. The **PPP3196** window displays.
2. Click on **PPP View** and select an entry to edit from the table. The **FS6300-PPP** window displays.
3. Select **Modify Link Configuration**..



Modify Link Configuration

PPP protocol	ppp-ipcp(1)
Authentication Technique	none(0)
Authentication Side	local(1)
Authentication Username	
Authentication Password	
MRU	1500
IP Address	192 .168 .150 .3
IP Mask	255 .255 .255 .255
IP Compression	none(1)
IP Force Next Hop	0 .0 .0 .0
Link Compression	disabled(2)
Allow Magic Number Negotiation	disabled(2)
IP Filters	

Figure 102. PPP Link Configuration

4. Edit the desired options:

   – **PPP Protocol:** The desired kind of PPP protocol.

   • ppp-ipcp(1) —point-to-point protocol

   • ppp-bcp(2)—bridge control protocol

   – **Authentication Technique:** The login technique to use for authentication.

   • none(0)—No authentication will be used

   • pap(3)—password authentication protocol will be used

   • chap(4)—challenge handshake authentication protocol will be used

   • chapORpap(5)—chap will be negotiated first, if that fails, pap will be attempted

- **Authentication Side:** The side of the link which will be authenticating.
  - local(1)—local server will be authenticating. Remote needs to log into local server.
  - remote(2)—remote server will be authentication. Local needs to log into remote server.
- **Authentication Username and Password:** The username and password that will be sent to the remote side if the remote machine is authenticating.
- **MRU:** The setting for Maximum Receive Unit (MRU), used for the PPP negotiation.
- **IP Address:** The IP address that will be used for the PPP link.
- **IP Mask:** The IP mask that will be used for the PPP link.
- **IP Compression:** Set whether Van Jacobson (*vj-tcp(2)*) header compression is used or not (*none(1)*).
- **IP Force Next Hop:** The IP address of the interface, which should be the next hop for the packets—fast routing
- **Link Compression:** Enables the PPP link layer address and protocol field compression. When enabled the PPP negotiations will desire link compression but may disable the compression due the other end of the link not accepting link compression. When disabled the PPP negotiations will force no compression on the PPP link.
  - enabled(1)—enable link compression
  - disabled(2)—disable link compression
- **Allow Magic Number Negotiation:** Determines if magic number negotiation should be done.
  - enabled(1)—enable magic number negotiation
  - disabled(2)—disable magic number negotiation
- **IP Filters:** This option is not modifiable through the FS6300 NMS. Refer to the *3196RC Administrator's Reference Guide* for more information on IP filtering.

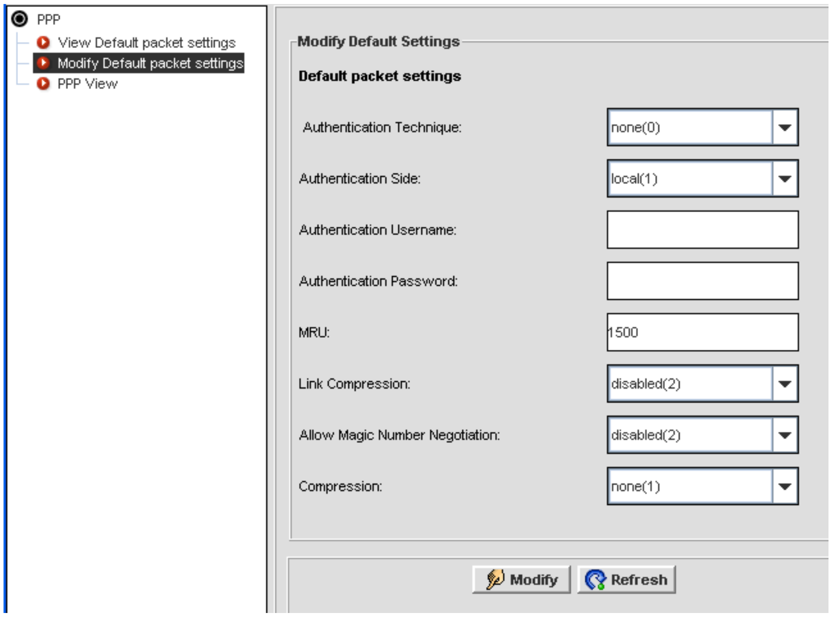
5. Click **Modify** to apply your changes.

Modify Default Packet Settings

You may modify the default PPP settings that each PPP link will take when first initialized. See "Modify PPP Link Configuration" on page 116 for modifying settings for individual links.

To modify default packet settings for PPP links:

1. Right-click on the card in the main window and select **PPP Configuration**. The **PPP2616** window displays.
2. Select **Modify Link Configuration**.



Modify Default Settings

Default packet settings

Authentication Technique: none(0)

Authentication Side: local(1)

Authentication Username:

Authentication Password:

MRU: 1500

Link Compression: disabled(2)

Allow Magic Number Negotiation: disabled(2)

Compression: none(1)

Figure 103. PPP Default Packet Settings

3. Edit the desired options:
   - **Authentication Technique:** The login technique to use for authentication.
     - none(0)—No authentication will be used
     - pap(3)—password authentication protocol will be used
     - chap(4)—challenge handshake authentication protocol will be used
     - chapORpap(5)—chap will be negotiated first, if that fails, pap will be attempted
   - **Authentication Side:** The side of the link which will be authenticating.
     - local(1)—local server will be authenticating. Remote needs to log into local server.
     - remote(2)—remote server will be authentication. Local needs to log into remote server.
   - **Authentication Username and Password:** The username and password that will be sent to the remote side if the remote machine is authenticating.
   - **MRU:** The setting for Maximum Receive Unit (MRU), used for the PPP negotiation.

– **Link Compression:** Enables the PPP link layer address and protocol field compression. When enabled the PPP negotiations will desire link compression but may disable the compression due the other end of the link not accepting link compression. When disabled the PPP negotiations will force no compression on the PPP link.

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

– **Allow Magic Number Negotiation:** Determines if magic number negotiation should be done.

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

– **Compression:** If none(1), then the local node will not attempt to negotiate any IP compression option. Otherwise, the local node will attempt to negotiate compression mode. Changing this option will have effect when the link restarts.

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

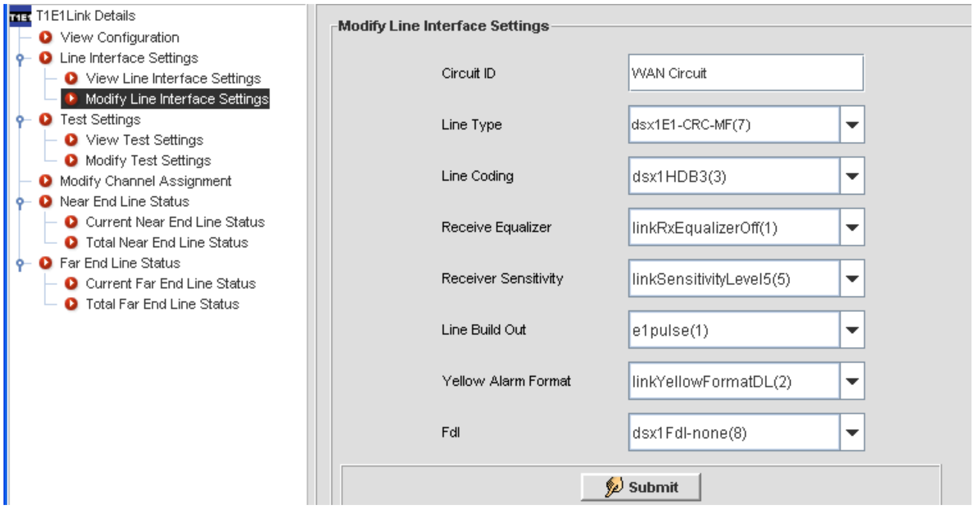
Configuring the T1/E1 Ports

Click on **T1E1 Port Configuration** to view T1/E1 links for the card. Select an entry in the table to configure line interfaces, test settings, and channel assignments for T1/E1 ports.

View Configuration

In the **T1-E1 Port Configuration** window for the selected link, click on **View Configuration**. If there are alarms for the link, click on **Alarms Present** to view the alarm details for the link.

Modify Line Interface Settings


T1E1Link Details
View Configuration
Line Interface Settings
View Line Interface Settings
Modify Line Interface Settings
Test Settings
View Test Settings
Modify Test Settings
Modify Channel Assignment
Near End Line Status
Current Near End Line Status
Total Near End Line Status
Far End Line Status
Current Far End Line Status
Total Far End Line Status
Modify Line Interface Settings
Submit

Circuit ID	WAN Circuit
Line Type	dsx1E1-CRC-MF(7)
Line Coding	dsx1HDB3(3)
Receive Equalizer	linkRxEqualizerOff(1)
Receiver Sensitivity	linkSensitivityLevel5(5)
Line Build Out	e1pulse(1)
Yellow Alarm Format	linkYellowFormatDL(2)
Fdl	dsx1Fdl-none(8)

Figure 104. T1/E1 Link Configuration window

1. In the **T1-E1 Port Configuration** window for the selected link, click on **Modify Line Interface Settings**.
2. Edit the desired options:

   – **Circuit ID:** The transmission vendor's circuit identifier, for the purpose of facilitating troubleshooting.

   – **Line Type:** the type of DS1 Line implemented on this circuit. The type of circuit affects the number of bits per second that the circuit can reasonably carry, as well as the interpretation of the usage and error statistics. Select fromt he following values:

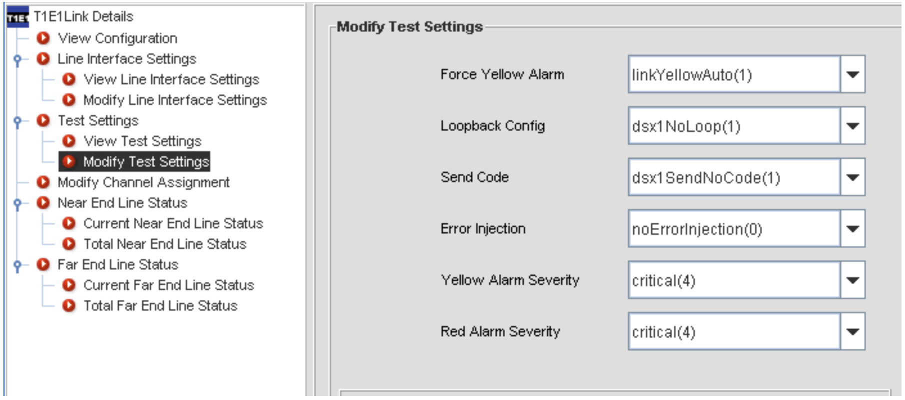
   - other(1)—Link is disabled
   - dsx1ESF(2)—Extended Superframe DS1
   - dsx1D4(3)—AT&T D4 format DS1
   - dsx1E1(4)—Based on CCITT/ITU G.704 without CRC (Cyclical Redundancy Check)
   - dsx1E1-CRC(5)—Based on CCITT/ITU G.704 with CRC (Cyclical Redundancy Check)
   - dsx1E1-MF(6)—Based on CCIT/ITU G.704 without CRC (bit oriented signaling)
   - dsx1E1-CRC-MF(7)—Based on CCIT/ITU G.704 with CRC (bit oriented signaling)
   - dsx1E1-Transparent(8)—Based on CCIT/ITU G.703 without CRC (Cyclical Redundancy Check)

- **Line Coding:** The type of Zero Code Suppression used on the link.
  - dsx1JBZS(1)—Jammed Bit Zero Suppression, in which the AT&T specification of at least one pulse every 8 bit periods is literally implemented by forcing a pulse in bit 8 of each channel. Thus, only seven bits per channel, or 1.344 Mbps, is available for data. This feature is not currently implemented.
  - dsx1B8ZS(2)—The use of a specified pattern of normal bits and bipolar violations which are used to replace a sequence of eight zero bits. The most common coding for T1 circuits.
  - dsx1HDB3(3)—This line coding is used with most E1 circuits today.
  - dsx1ZBTSI(4)—May use dsx1ZBTSI, or Zero Byte Time Slot Interchange. This feature is not currently implemented.
  - dsx1AMI(5)—Refers to a mode wherein no zero code suppression is present and the line encoding does not solve the problem directly. In this application, the higher layer must provide data which meets or exceeds the pulse density requirements, such as inverting HDLC data.
  - other(6)—This feature is not currently supported.
- **Receive Equalizer:** The equalization used on the received signal. Long haul signals should have the equalization set for more. Short haul signals require less equalization.
- **Receiver Sensitivity:** The minimum voltage at which the WAN port will sense that the signal is available. This variable is only used if the **Receiver Equalization** is set to **ON**.
- **Line Build Out:** The T1 or E1 pulse levels used by the T1/E1 ports:
  - triState(0)—When the T1/E1 port is not in use, you may want to place the port in tri-state mode. While in this setting, the input lines to the port are placed in high impedance protection mode.
  - e1pulse(1)—Used when connecting the T1/E1 port to E1 lines.
  - t1pulse0dB(2)—Strong T1 pulse amplitude.
  - t1pulse-7dB(3)—Medium T1 pulse amplitude.
  - t1pulse-15dB(4)—Weak T1 pulse amplitude.
- **Yellow Alarm Format:** The standard used to transmit and identify the Yellow Alarm.
  - link YellowFormatBit2(1)—Bit-2 equal zero in every channel
  - link YellowFormatDL(2)—FF00 pattern in the Data Link
  - link YellowFormatFrame12FS(3)—FS bit of frame 12
- **Fdl:** implementation of FDL is being used, if any. FDL applies only to T1 circuits.
  - other(1)—Indicates that a protocol other than one following is used.
  - dsx1Ansi-T1-403(2)—Refers to the FDL exchange recommended by ANSI.
  - dsx1Att-54016(3)—Refers to ESF FDL exchanges.
  - dsx1Fdl-none(4)—Indicates that the device does not use the FDL.

  If one of the E1 line types has been selected, set **Fdl** to **dsx1Fdl-none**(**8**).

3. Click **Submit** to commit your changes.

Modify Test Settings


T1E1Link Details
View Configuration
Line Interface Settings
View Line Interface Settings
Modify Line Interface Settings
Test Settings
View Test Settings
Modify Test Settings
Modify Channel Assignment
Near End Line Status
Current Near End Line Status
Total Near End Line Status
Far End Line Status
Current Far End Line Status
Total Far End Line Status

Modify Test Settings

Force Yellow Alarm: linkYellowAuto(1)

Loopback Config: dsx1NoLoop(1)

Send Code: dsx1SendNoCode(1)

Error Injection: noErrorInjection(0)

Yellow Alarm Severity: critical(4)

Red Alarm Severity: critical(4)

Figure 105. T1/E1 Test Settings

1. In the **T1-E1 Port Configuration** window for the selected link, click on **Modify Test Settings**.
2. Edit the desired options:

   – **Force Yellow Alarm:** The standard used to transmit and identify the Yellow Alarm.

   - linkYellowAuto—Do not force the transmission of a yellow alarm. But, yellow alarm may be automatically transmitted.
   - linkYellowOn—Force the transmission of a yellow alarm even if the received signal is in frame.
   - linkYellowDisable—Do NOT transmit a yellow alarm even if the received signal is out of frame.

   – **Loopback Configuration:** The loopback configuration of the DS1 interface.

   - dsx1NoLoop(1)—Not in the loopback state. A device that is not capable of performing a loopback on the interface shall always return this as it's value.
   - dsx1PayloadLoop(2)—The received signal at this interface is looped through the device. Typically the received signal is looped back for retransmission after it has passed through the device's framing function.
   - dsx1LineLoop(3)—The received signal at this interface does not go through the device (minimum penetration) but is looped back out.
   - dsx1OtherLoop(4)—Loopbacks that are not defined here.

   – **Send Code:** The type of code is being sent across the DS1 interface by the device.

   - dsx1SendNoCode(1)—Sending looped or normal data
   - dsx1SendLineCode(2)—Sending a request for a line loopback
   - dsx1SendResetCode(4)—Sending a loopback termination request

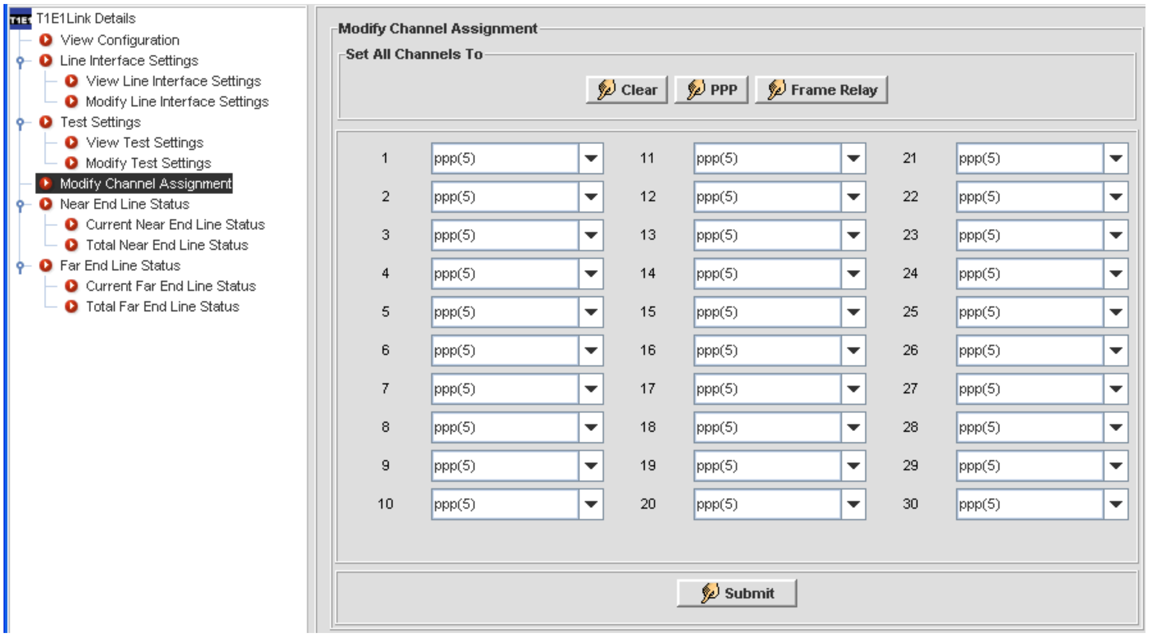
   – **Error Injection:** Force an output error to see if the other end detects it.

   – **Yellow Alarm Severity:** Critical / Major / Minor / Info / Ignore

   – **Red Alarm Severity:** Critical / Major / Minor / Info / Ignore

3. Click **Submit** to commit your changes.

Modify Channel Assignments


T1E1Link Details
View Configuration
Line Interface Settings
View Line Interface Settings
Modify Line Interface Settings
Test Settings
View Test Settings
Modify Test Settings
Modify Channel Assignment
Near End Line Status
Current Near End Line Status
Total Near End Line Status
Far End Line Status
Current Far End Line Status
Total Far End Line Status
Modify Channel Assignment
Set All Channels To
Clear
PPP
Frame Relay
Submit

1	ppp(5)	11	ppp(5)	21	ppp(5)
2	ppp(5)	12	ppp(5)	22	ppp(5)
3	ppp(5)	13	ppp(5)	23	ppp(5)
4	ppp(5)	14	ppp(5)	24	ppp(5)
5	ppp(5)	15	ppp(5)	25	ppp(5)
6	ppp(5)	16	ppp(5)	26	ppp(5)
7	ppp(5)	17	ppp(5)	27	ppp(5)
8	ppp(5)	18	ppp(5)	28	ppp(5)
9	ppp(5)	19	ppp(5)	29	ppp(5)
10	ppp(5)	20	ppp(5)	30	ppp(5)

Figure 106. T1/E1 Channel Assignment

In the **Modify Channel Assignment** section of the **T1/E1 Link Configuration** window, you can change selected DS0 channels to carry in-band management information over Frame Relay or PPP links. You can use the buttons at the top of the window to modify all 30 timeslots at once. Or, you can use the 30 drop-down menus to modify selected timeslots individually. Click **Submit** to apply your changes for individual links.

View Line Status

There are two types of line status statistics that you may view in the T1/E1 Link Configuration window – **Near End Line Status** and **Far End Line Status**.

- **Near End Line Status** – Click on **Current Near End Line Status** to view statistics for current near end performance. Click on **Total Near End Line Status** to view statistics totals for near end performance.
- **Far End Line Status** – Click on **Current Far End Line Status** to view statistics for current far end performance. Click on **Total Far End Line Status** to view statistics totals for far end performance.

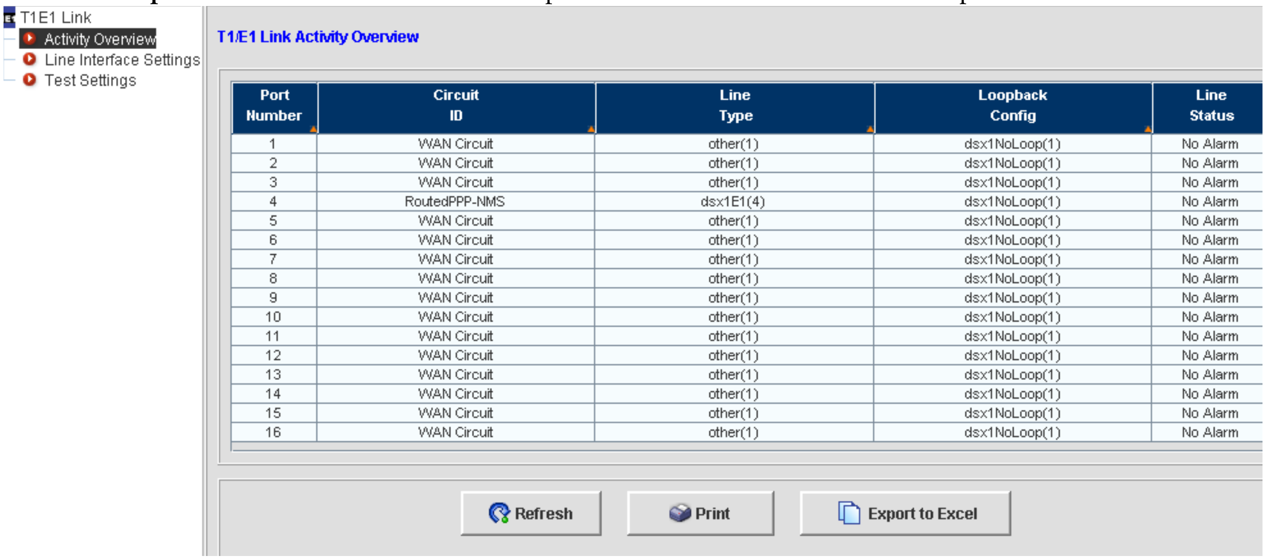
Note Refer to the *3196RC Adminsitrator's Reference Guide* for detailed information about line status statistics.

Viewing T1/E1 Reports

Click on **T1E1 Reports** to view and print different reports about the activity, line interface settings, and test settings of T1/E1 links on the 3196RC card.

Click the **Print** button to send the report to a printer on your network.

Click the **Export to Excel** button to send the report to Microsoft Excel to save in a spreadsheet.



T1/E1 Link Activity Overview

Port Number	Circuit ID	Line Type	Loopback Config	Line Status
1	WAN Circuit	other(1)	dsx1NoLoop(1)	No Alarm
2	WAN Circuit	other(1)	dsx1NoLoop(1)	No Alarm
3	WAN Circuit	other(1)	dsx1NoLoop(1)	No Alarm
4	RoutedPPP-NMS	dsx1E1(4)	dsx1NoLoop(1)	No Alarm
5	WAN Circuit	other(1)	dsx1NoLoop(1)	No Alarm
6	WAN Circuit	other(1)	dsx1NoLoop(1)	No Alarm
7	WAN Circuit	other(1)	dsx1NoLoop(1)	No Alarm
8	WAN Circuit	other(1)	dsx1NoLoop(1)	No Alarm
9	WAN Circuit	other(1)	dsx1NoLoop(1)	No Alarm
10	WAN Circuit	other(1)	dsx1NoLoop(1)	No Alarm
11	WAN Circuit	other(1)	dsx1NoLoop(1)	No Alarm
12	WAN Circuit	other(1)	dsx1NoLoop(1)	No Alarm
13	WAN Circuit	other(1)	dsx1NoLoop(1)	No Alarm
14	WAN Circuit	other(1)	dsx1NoLoop(1)	No Alarm
15	WAN Circuit	other(1)	dsx1NoLoop(1)	No Alarm
16	WAN Circuit	other(1)	dsx1NoLoop(1)	No Alarm

Figure 107. 3196RC T1/E1 Reports

Viewing the T1/E1 Map Layer

Click on **Display T1E1 Map Layer** to show a map of all the T1/E1 ports on the card. Right-click on a port in the map to configure its link. See “Configuring the T1/E1 Ports” on page 120 for more details.

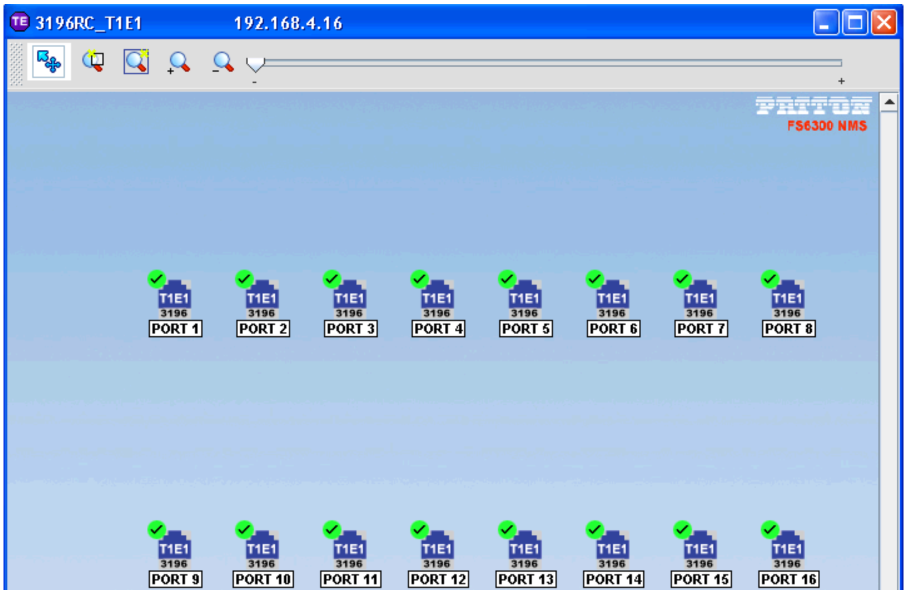


Figure 108. 3196RC T1/E1 Port Map

Viewing the iDSL Map Layer

Click on **Display iDSL Map Layer** to show a map of all the iDSL ports on the card. Right-click on a port in the map to configure its link. See "Configuring iDSL Ports" on page 110 for more details.

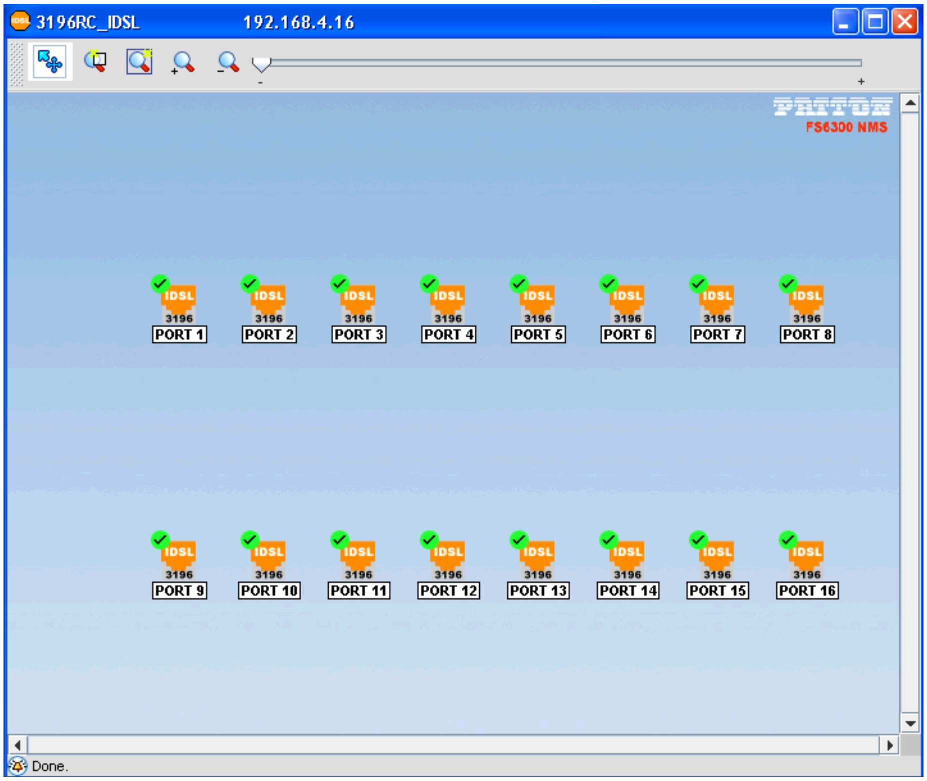


Figure 109. 3196RC iDSL Port Map

Chapter 8 Configuring the 6511RC Card

Chapter contents

Introduction

The Patton Model 6511RC is a matrix switch with Gigabit Ethernet. There are several ways to reach the configuration menu for the 6511RC card:

- Click on **Network Maps** in the main menu tree, then click on **Chassis.** Right-click on the 6511RC icon.
- Navigate to **Network Database** > **Managed Objects** > **Cards** in the main menu tree, then right-click on the IP address of the card in the table in the main window.

The best way to reach the configuration menu for a card is to select the card in the main menu tree, then right-click on the card's icon in the main window.

6511RC Configuration Menu

The following options are available in the pull-down menu for the 6511RC card:

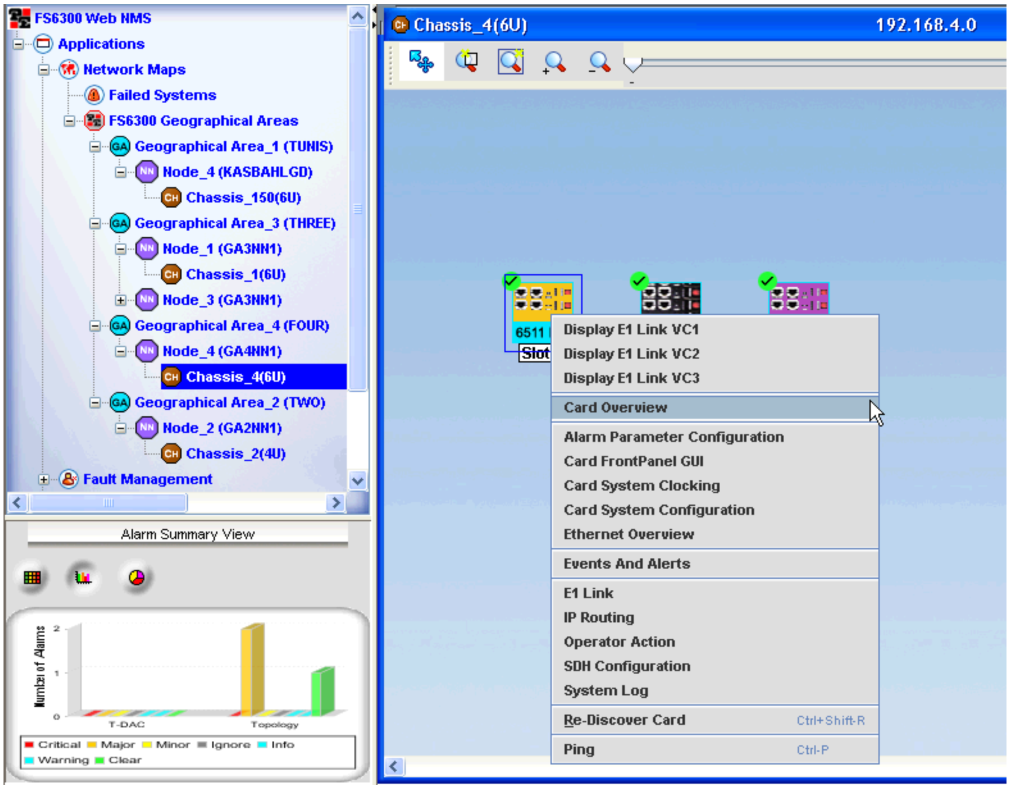


Figure 110. 6511RC Configuration Menu

- Display E1Link VC*x* – See "Viewing E1Link Layers" on page 138
- Card Overview – Shows information for Box Status, Card Info, and Alarm Info
- Alarm Parameter Configuration – See "Configuring Alarms through a Card in the Chassis" on page 48
- Card Front Panel GUI – See "Viewing the Front Panel" on page 128
- Card System Clocking – See "Configuring Card System Clocking" on page 54
- Card System Configuration – See "Configuring the Card System" on page 128

- Ethernet Overview – See "Configuring Ethernet Settings" on page 130
- Events and Alerts – See "Viewing Events and Alerts" on page 62
- E1 Link – See "Configuring E1 Links" on page 131
- IP Routing – See "Configuring IP Routing" on page 133
- Operator Action – See "Managing Operator Actions" on page 60
- SDH Configuration – "Configuring SDH" on page 135
- System Log – See "Viewing/Modifying System Log Configuration" on page 65
- Re-Discover Card – See "Re-Discovering Cards Manually" on page 38
- Ping – Displays a status message after pinging the interface.

Viewing the Front Panel

Click on **Card Front Panel GUI** to view the front panel of the card in real-time.

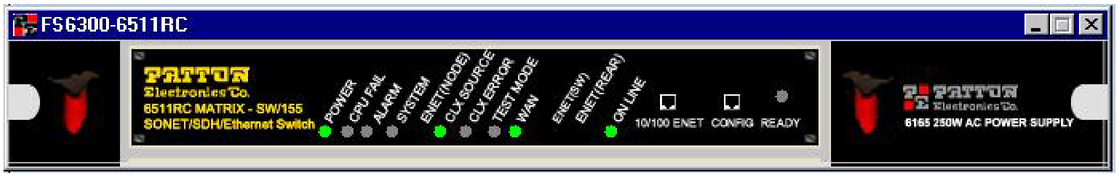


Figure 111. 6511RC Front Panel LEDs

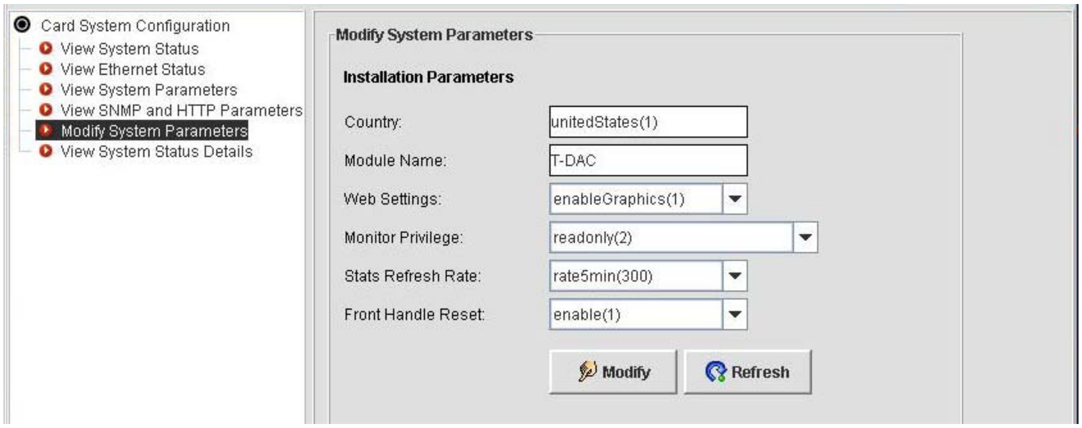
Configuring the Card System

Click on **Card System Configuration** to configure system parameters. You can also view the system status, ethernet status, system parameters, SNMP and HTTP Parameters, and system status details.

Modify System Parameters

If you only want to view the system parameters, click on **View System Parameters** in the Card System Configuration window.

To configure the card system, click on **Modify System Parameters** in the menu tree in the Card System Configuration window (see Figure 112 on page 129).



Installation Parameters

Country: unitedStates(1)

Module Name: T-DAC

Web Settings: enableGraphics(1)

Monitor Privilege: readonly(2)

Stats Refresh Rate: rate5min(300)

Front Handle Reset: enable(1)

Figure 112. Modify Card System Parameters

1. Select to enable or disable graphics from the **Web Settings** drop-down menu.
2. Select a privilege option for configuring the card through the NMS from the **Monitor Privilege** drop-down menu.
3. Select how often you would like to refresh statistics information from the **Stats Refresh Rate** drop-down menu.
4. Select to enable or disable front handle reset from the **Front Handle Reset** drop-down menu.
5. Click **Modify** to save your changes. Click **Refresh**.

View System Status

Click on **View System Status** in the Card System Configuration window to see an overview of the physical status of the card and the system status. **View System Status** shows information about the handle switches, front/rear LEDs, alarm and clock LEDs, and the board temperature.

View System Status Details

Click on **View System Status Details** in the Card System Configuration window to see information on CPU statistics, Message Block statistics, Memory statistics, Manufacturer details, and the Enclosure System temperature.

View Ethernet Status

Click on **View Ethernet Status** in the Card System Configuration window to see the LEDs and speeds of the card’s Ethernet ports.

View SNMP and HTTP Parameters

Click on **View SNMP and HTTP Parameters** in the Card System Configuration window to see the SNMP version and passwords.

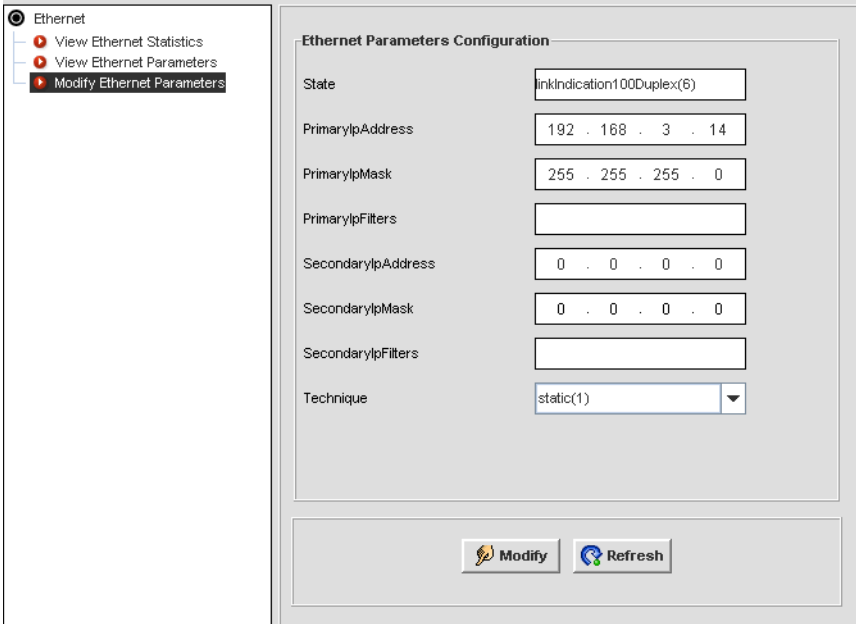
Configuring Ethernet Settings

Click on **Ethernet Overview** to configure Ethernet settings. You can also view Ethernet statistics.

Modify Ethernet Parameters

If you only want to view the Ethernet parameters, click on **View Ethernet Parameters** in the Ethernet Overview window.

To configure the Ethernet settings, click on **Modify Ethernet Parameters** in the menu tree in the Ethernet Overview window (see Figure 113).



Ethernet Parameters Configuration

State: linkIndication100Duplex(6)

PrimaryIpAddress: 192 . 168 . 3 . 14

PrimaryIpMask: 255 . 255 . 255 . 0

PrimaryIpFilters:

SecondaryIpAddress: 0 . 0 . 0 . 0

SecondaryIpMask: 0 . 0 . 0 . 0

SecondaryIpFilters:

Technique: static(1)

Figure 113. Modify Ethernet Parameters

1. Enter the main address and mask for the card in the **Primary IP Address** and **IP Mask** fields.
2. The **IP Filter** needs to be provisioned through the card's configuration website. For more information on setting up IP Filters, refer to the *Model 6511RC Adminstrator's Reference Guide*.
3. From the **Technique** drop-down menu, select **static** if you want to statically assign the IP address, or select **disable** if you want to use DHCP to assign the IP address.
4. Click **Modify** to commit your changes. Click **Refresh**.

View Ethernet Statistics

Click on **View Ethernet Statistics** in the Ethernet Overview window to view statistics for the Ethernet ports on the device, such as errors and frame stats.

Configuring E1 Links

Click on **E1 Link** to configure the line interface, alarm status, DS0 settings, and test settings.

Edit Line Interface Settings

Click on **Line Interface** (under Current Configuration) in the menu tree for the E1 Link window, then select the links you want to edit from the **TUG3**, **TUG2**, and **TU** drop-down menus. Make the desired changes, then click **Submit**.

View Alarm Status

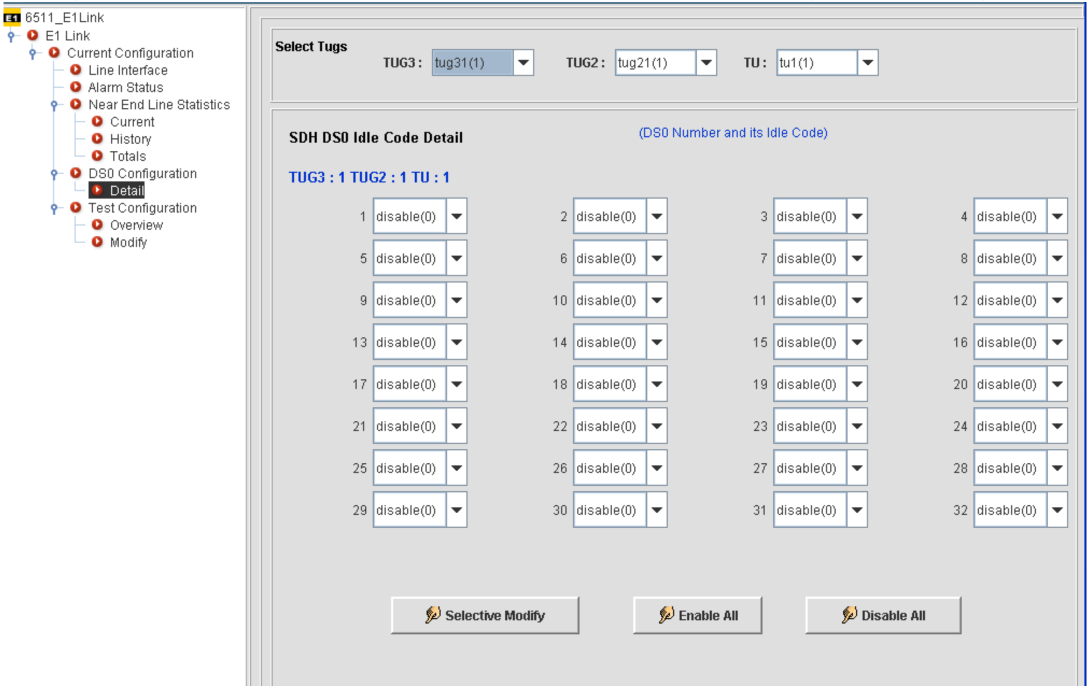
Click on **Alarm Status** (under Current Configuration) in the menu tree for the E1 Link window, then select the links you want to view alarms for from the **TUG3**, **TUG2**, and **TU** drop-down menus.

View Line Statistics

You can view Current, Past, and Total Line Statistics for a link. Navigate to **Near End Line Statistics > Current**, **Near End Line Statistics > History**, or **Near End Line Statistics > Totals** in the menu tree for the E1 Link window, then select the links you want to view from the **TUG3**, **TUG2**, and **TU** drop-down menus.

Configure DS0 Settings

Click on **DS0 Configuration > Details** in the menu tree for the E1 Link window, then select the links you want to configure from the **TUG3**, **TUG2**, and **TU** drop-down menus (see Figure 114 on page 131).



Select Tugs

TUG3 : tug31(1) TUG2 : tug21(1) TU : tu1(1)

SDH DS0 Idle Code Detail (DS0 Number and its Idle Code)

TUG3 : 1 TUG2 : 1 TU : 1

1	disable(0)	2	disable(0)	3	disable(0)	4	disable(0)
5	disable(0)	6	disable(0)	7	disable(0)	8	disable(0)
9	disable(0)	10	disable(0)	11	disable(0)	12	disable(0)
13	disable(0)	14	disable(0)	15	disable(0)	16	disable(0)
17	disable(0)	18	disable(0)	19	disable(0)	20	disable(0)
21	disable(0)	22	disable(0)	23	disable(0)	24	disable(0)
25	disable(0)	26	disable(0)	27	disable(0)	28	disable(0)
29	disable(0)	30	disable(0)	31	disable(0)	32	disable(0)

Figure 114. 6511RC DS0 Details

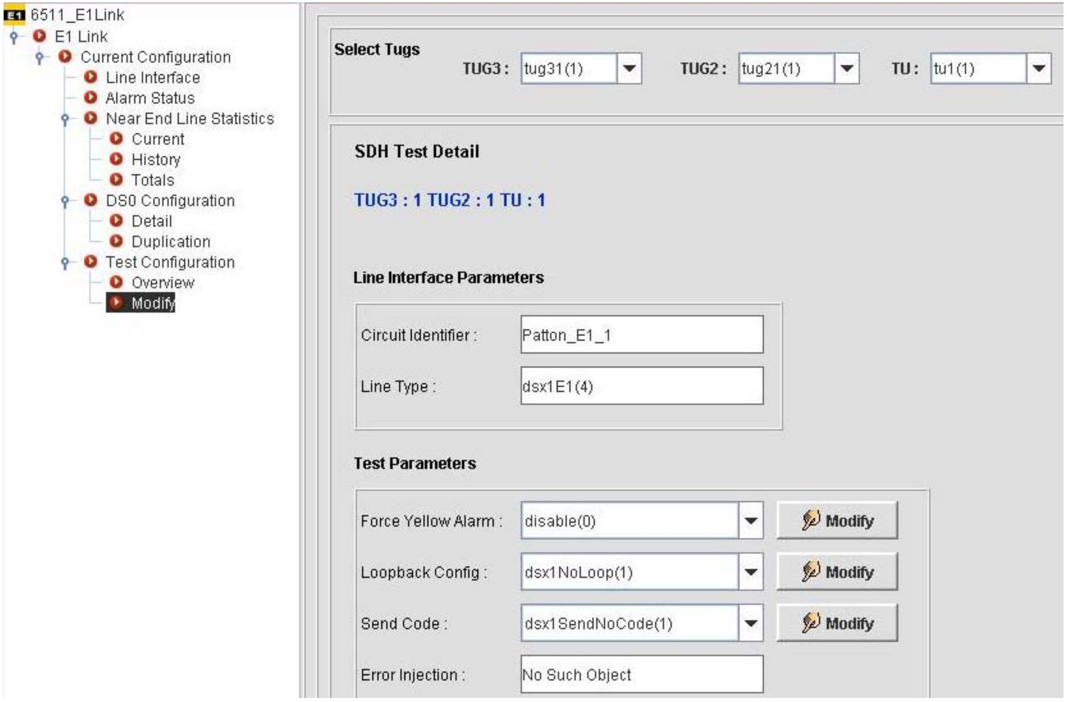
If you only want to enable or disable a few DS0 numbers, select the status from the drop-down menu for each DS0 number you want to change, then click **Selective Modify**.

If you want to activate all DS0 numbers, click **Enable All**. If you want to deactivate all DS0 numbers, click **Disable All**. A status emssage will display. Click **OK**.

Edit Test Settings

Click on **Test Configuration** in the menu tree for the E1 Link window, then select the links you want to configure from the **TUG3**, **TUG2**, and **TU** drop-down menus. **Test Configuration** > **Overview** shows information for SDH, including test settings, line parameters, and test parameters.

Click on **Test Configuration** > **Modify** to configure test parameters (see Figure 115 **on page 132**).



Select Tugs

TUG3 : tug31(1) TUG2 : tug21(1) TU : tu1(1)

SDH Test Detail

TUG3 : 1 TUG2 : 1 TU : 1

Line Interface Parameters

Circuit Identifier : Patton_E1_1

Line Type : dsx1E1(4)

Test Parameters

Force Yellow Alarm : disable(0)

Loopback Config : dsx1NoLoop(1)

Send Code : dsx1SendNoCode(1)

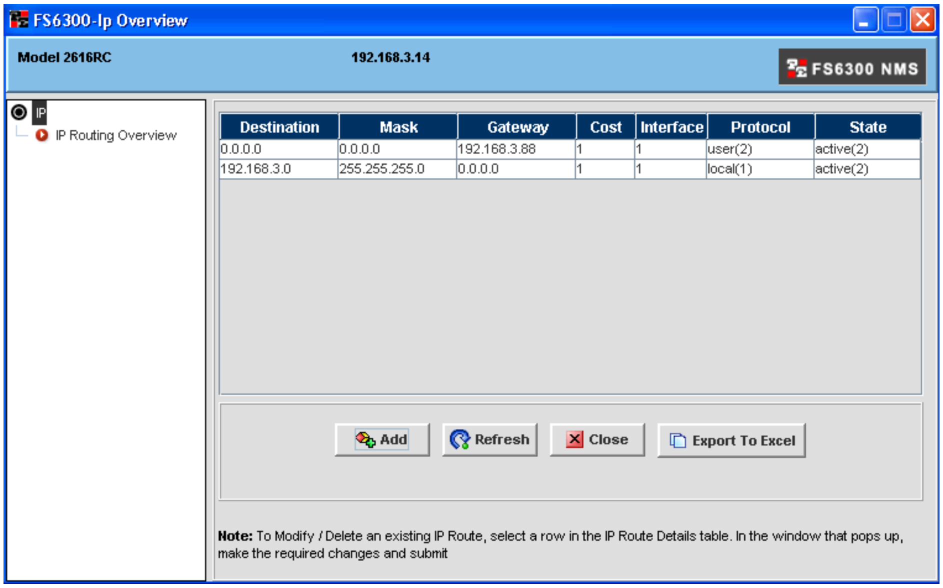
Error Injection : No Such Object

Figure 115. 6511RC E1 Link Test Settings

1. Select enable or disable from the **Force Yellow Alarm** drop-down menu, then click **Modify**. Selecting **enable**(1) forces the transmission of a yellow alarm even if the received signal is in frame.
2. Select a loop test from the **Loopback Config** drop-down menu, then click **Modify**. Select from the following loopback options:
   - 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.
3. Select a code from the **Send Code** drop-down menu, then click **Modify**.
   Code options include: Line Code, Payload Code, Reset Code, QRS, 511 Pattern, 3in24 Pattern, Other Test Pattern, and No Code.

Configuring IP Routing

ou may configure a host and routes for the 6511RC through the FS6300 NMS. The **IP Overview** window shows details for routing destinations, and includes information for gateway, cost, interface, protocol, and state of each route.



Destination	Mask	Gateway	Cost	Interface	Protocol	State
0.0.0.0	0.0.0.0	192.168.3.88	1	1	user(2)	active(2)
192.168.3.0	255.255.255.0	0.0.0.0	1	1	local(1)	active(2)

Note: To Modify / Delete an existing IP Route, select a row in the IP Route Details table. In the window that pops up, make the required changes and submit

Figure 116. 6511RC IP Overview

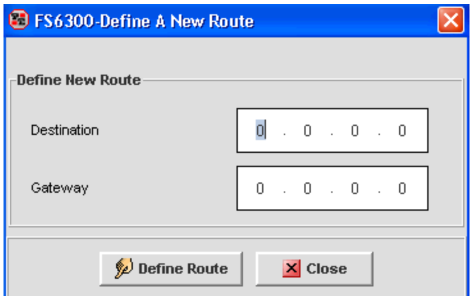
The table in the **IP Overview** window shows a list of defined routes for the 6511RC, and includes the following information for each entry:

- **Destination:** The destination IP address of this route. An entry with a value of 0.0.0.0 is considered a default route.
- **Mask:** The mask that is logical-ANDed with the destination address before being compared to the value in the Destination field.
- **Gateway:** The IP address where the packets should be forwarded.
- **Cost:** The cost of the route as defined by RIP standards. Cost is sometimes considered to be number of hops.
- **Interface:** The index value that uniquely identifies the local interface through which the next hop of this route should be reached.
- **Protocol:** The routing mechanism via which this route was learned.
  - *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 managemen tools.
  - *rip(4)*—Learned via reception of RIP packet.
  - *icmp(5)*—Learned via reception of ICMP packet
- **State:** Shows if a route is valid/in use.

Adding Routes

To add an IP route to the 6511RC:

1. In the **IP Overview** window for the 6511RC, click the **Add** button to define a new route.



FS6300-Define A New Route

Define New Route

Destination: 0 . 0 . 0 . 0

Gateway: 0 . 0 . 0 . 0

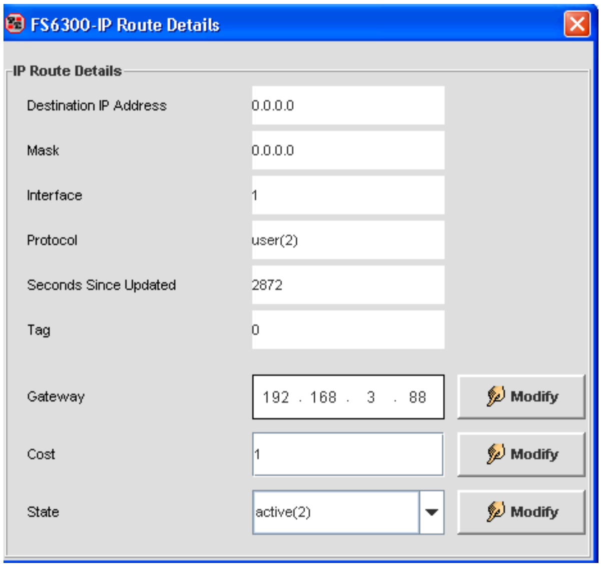
Figure 117. Add a New Route for 6511RC

2. Enter a **Destination** address for the new route. An entry with a value of 0.0.0.0 is considered a default route.
3. Enter a **Gateway** address for the new route. The gateway address specifies the IP address where the packets should be forwarded.
4. Click **Define Route**.

Modifying Routes

To modify an existing IP route for the 6511RC:

1. In the **IP Overview** window for the 6511RC, select the entry in the table of the route you want to modify.



FS6300-IP Route Details

IP Route Details

Destination IP Address: 0.0.0.0

Mask: 0.0.0.0

Interface: 1

Protocol: user(2)

Seconds Since Updated: 2872

Tag: 0

Gateway: 192 . 168 . 3 . 88

Cost: 1

State: active(2)

Figure 118. Modifying a Route for 6511RC

2. The **IP Route Details** window displays. You may only modify the gateway address, cost, and state of the route.
3. Enter your desired changes and click **Modify** for each change. A confirmation message displays.

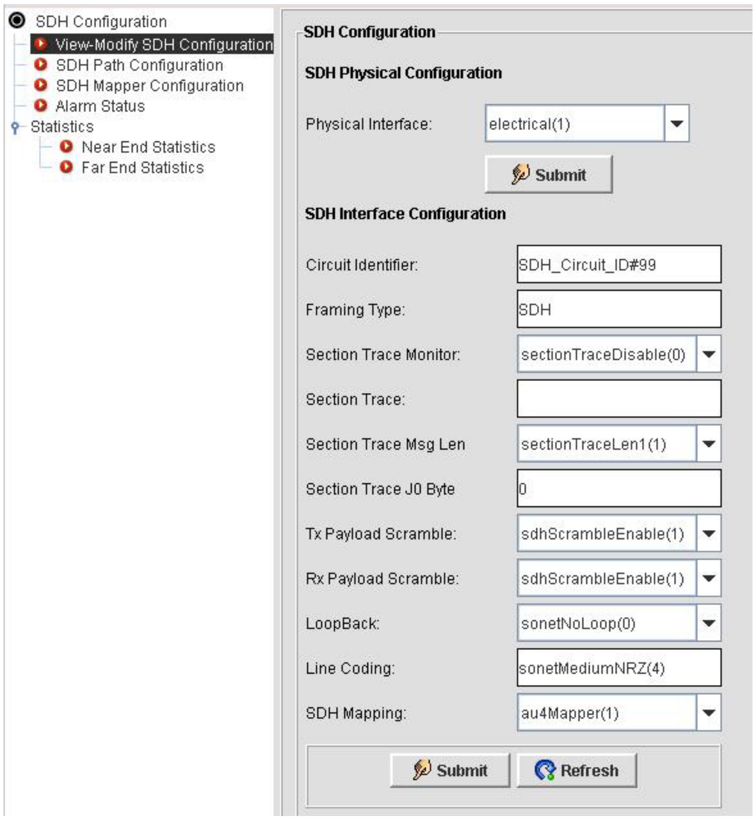
Configuring SDH

Click on **SDH Configuration** to bring up the SDH Configuration window to view and modify SDH interfaces and paths.

Configuring SDH Interfaces

To configure SDH interfaces:

1. Click on **View/Modify SDH Configuration** in the menu tree of the SDH Configuration window.



SDH Configuration

SDH Physical Configuration

Physical Interface: electrical(1)

SDH Interface Configuration

Circuit Identifier: SDH_Circuit_ID#99

Framing Type: SDH

Section Trace Monitor: sectionTraceDisable(0)

Section Trace:

Section Trace Msg Len sectionTraceLen1(1)

Section Trace J0 Byte 0

Tx Payload Scramble: sdhScrambleEnable(1)

Rx Payload Scramble: sdhScrambleEnable(1)

LoopBack: sonetNoLoop(0)

Line Coding: sonetMediumNRZ(4)

SDH Mapping: au4Mapper(1)

Figure 119. 6511RC SDH Interface Configuration

2. Select a **Physical Interface** from the drop-down menu under SDH Physical Configuration, and click **Submit**. The **Physical Interface** corresponds to the physical cabling atatched to the STM-1 interface ports.
   Select **Optical** if you are using fiber-optic cable connected to the rear-card SC connectors.
   Select **Electrical** if you are using coaxial cables connected to the rear-card BNC connectors.
3. If desired, enter an alphanumeric name for the STM-1 link in the **Circuit Identifier** field.
4. If section trace is enabled in your connected SDH network, select **sectionTraceEnable** from the **Section Trace Monitor** drop-down menu. Otherwise, select **sectionTraceDisable**, and go to Step 8 on page 136.
5. If the Section Trace Monitor is Enabled, enter the alphanumeric name your connected SDH network uses for the **Section Trace** message in the SDH frame.

6. Select the message length used by the SDH network –1-byte, 16-byte, or 64-byte– from the **Section Trace Message Len** drop-down menu.

7. Enter the value the connetced SDH network uses for the J0 byte in the **Section Trace J0 Byte** field.

> **Note** J0 Byte only applies to the 1-byte Section Trace Messages. For 16-byte or 64-byte, the J0 value is ignored and the trace message value applies.

8. If the SDH network transmits a scrambled payload, select **Enable** from the **Tx Payload Scramble** drop-down menu. Otherwise, select **Disable**.

9. If the SDH network expects to receive a scrambled payload, select **Enable** from the **Rx Payload Scramble** drop-down menu. Otherwise, select **Disable**.

10. Select a diagnostic loop type from the **Loopback** drop-down menu. Choose from the following options:
    - 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.

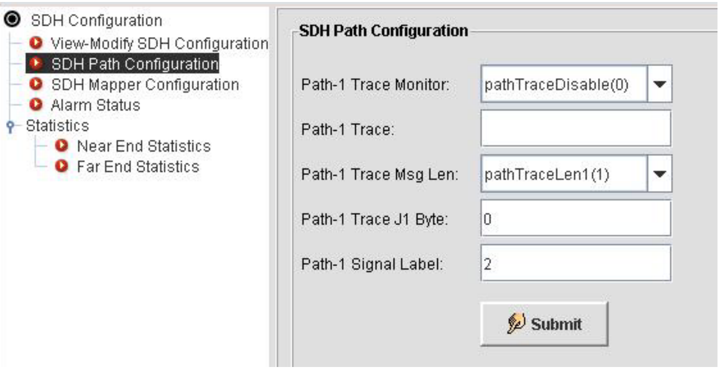
11. For **SDH Mapping,** select the type of AU that corresponds to the SDH multiplexing path you want to use. Select **au4Mapper** if you want to multiplex three TUG-3s into an AU-4. Select **au3Mapper** if you want to multiplex seven TUG-2s into an AU-3.

12. Click **Submit** to save your changes.

Configuring SDH Paths

To configure SDH paths:

1. Click on **SDH Path Configuration** in the menu tree of the SDH Configuration window. Path Trace settings will vary, depending on which type of SDH mapping is being used– AU-3 or AU-4.



SDH Path Configuration

Path-1 Trace Monitor: pathTraceDisable(0)

Path-1 Trace:

Path-1 Trace Msg Len: pathTraceLen1(1)

Path-1 Trace J1 Byte: 0

Path-1 Signal Label: 2

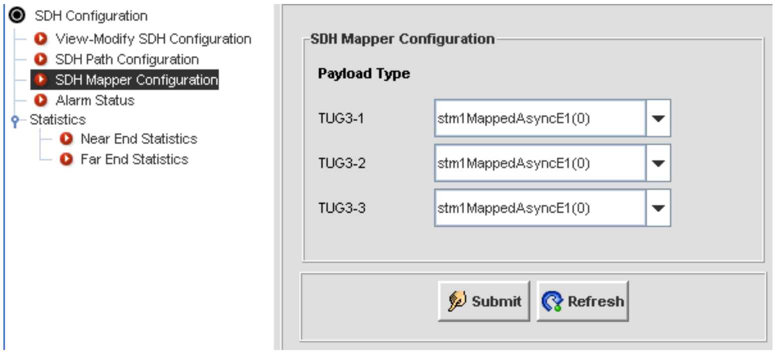
Figure 120. 6511RC SDH Path Configuration

2. Select **Enable** from the **Trace Monitor** drop-down menu if Path Trace is enabled in the connected SDH network.
3. Enter the alphanumeric name your SDH network uses for the Path-1 Trace Message in the **Trace** field. This only applies to 16-byte and 64-byte section trace messages.
4. Select the message length value your SDH network uses from the **Trace Message Len** drop-down menu.
5. For **Trace J1 Byte**, enter the value your connected SDH network uses for the J1 byte in the SDH frame. J1 only applies to 1-byte trace messages.
6. In the **Signal Label** field, enter the value your connected SDH network uses for the path signal label in the SDH frame.
7. Click **Submit**.

Configuring SDH Mapper

The SDH Mapper allows you to configure the E1 payload timing with regard to SDH timing.To configure the SDH Mapper:

1. Click on **SDH Mapper Configuration** in the menu tree of the SDH Configuration window.



TUG3-1 stm1MappedAsyncE1(0)
TUG3-2 stm1MappedAsyncE1(0)
TUG3-3 stm1MappedAsyncE1(0)

Figure 121. 6511RC SDH Mapper Configuration

2. Select **AsyncE1** or **ByteSyncE1** to configure the payload type for the SDH Mapper. The payload type indicates whether the E1 signals are asynchronous or synchronous with respect to SDH. Select **stm1MappedAsyncE1(0)** so that the E1 2 Mbits signals are not synchronized to the SDH signal. Select **stm1MappedBytesincE1(1)** so that rate and framing of E1 signals are synchronized to the SDH signal.
3. Click **Submit**.

Viewing Alarm Status

To view SDH alarms, click on **Alarm Status** in the menu tree of the SDH Configuration window. Hover the mouse pointer over an LED (Section, Line, or Path) to view the alarm status.

Viewing Statistics

To view SDH statistics, click on **Near End Statistics** or **Far End Statistics** in the menu tree of the SDH Configuration window. Click on an LED in the Current column to edit the Stats Refresh Rate. Click on an LED in the History column to view past details.

Viewing E1Link Layers

Click on **Display E1 Link VC**(#) to show a map of all the E1 links on a TUG. To edit a link, right-click on the E1 link icon that you want to edit and select **E1 Port Link Configuration**. (See "Configuring E1 Links" on page 131).

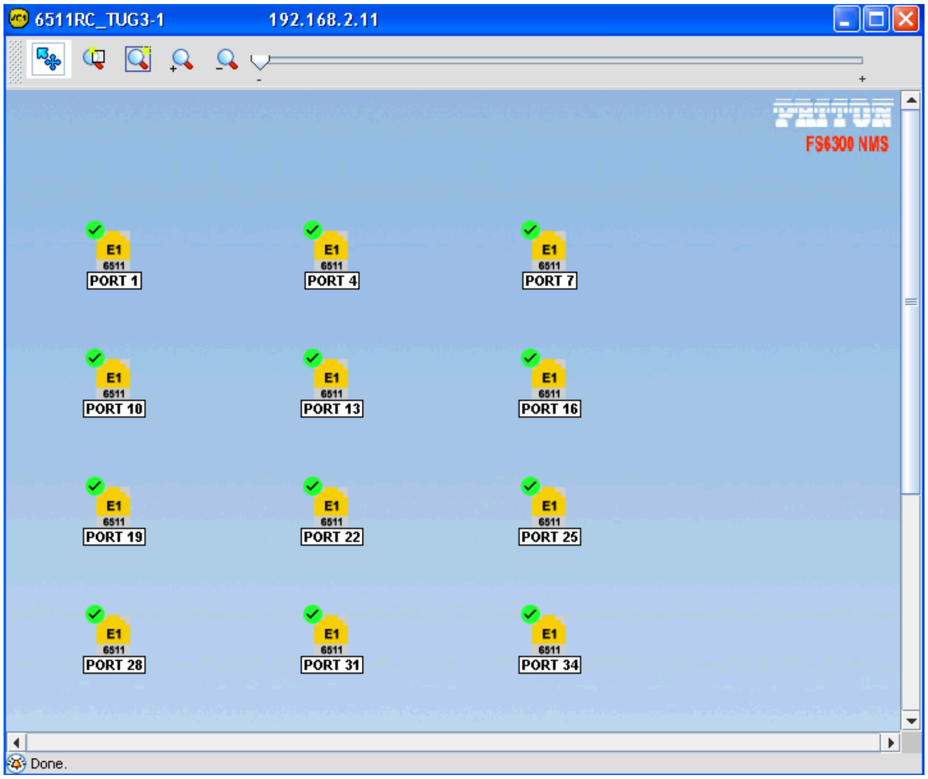


Figure 122. 6511RC E1 Link Map

Chapter 9 **Configuring Chassis**

Chapter contents

Introduction

To configure a chassis, navigate to **Network Maps** > **Geographical Area** > **Network Node** in the menu tree on the left side of the screen. Right-click on a chassis icon in the main window to display the configuration menu for the chassis.

Chassis Configuration Menu

The following options are available in the pull-down menu for a chassis:

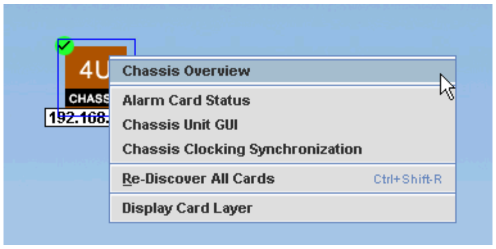


Figure 123. Chassis Configuration Menu

- Chassis Overview – Shows information for the chassis, including Area ID and Network Node, Chassis ID, Name, and Type, Network IP, Number of Cards, and Alarm Status
- Alarm Card Status – View information about the card on the chassis that is monitoring alarms
- Chassis Unit GUI – See "Viewing the Chassis LEDs" on page 141
- Chassis Clocking Synchronization – See "Configuring Clocking Synchronization" on page 53
- Re-Discover Card – See "Re-Discovering Cards Manually" on page 38
- Display Card Layer – See "Viewing the Card Layer Map" on page 142

Viewing the Chassis LEDs

Click on **Chassis Unit GUI** to view the front panels of all of the cards in the chassis in real-time.

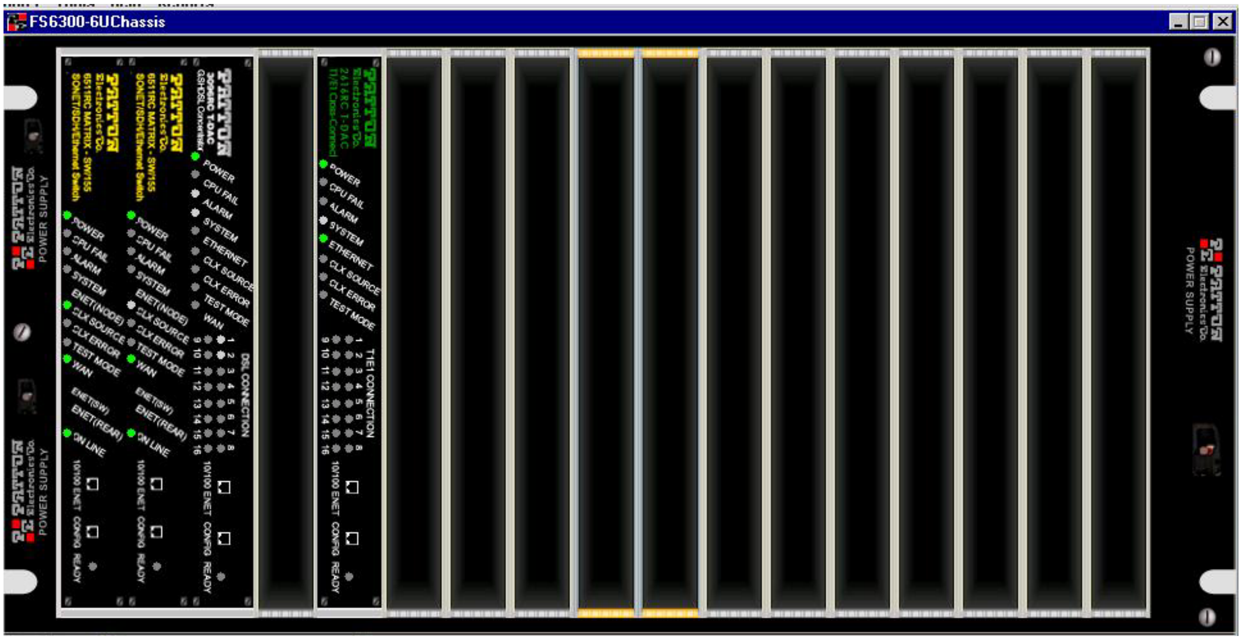


Figure 124. Chassis LEDs

Viewing the Card Layer Map

Click on **Display Card Layer** to view a map of all of the cards in the chassis. Right-click on a card to configure to view it's configuration menu.

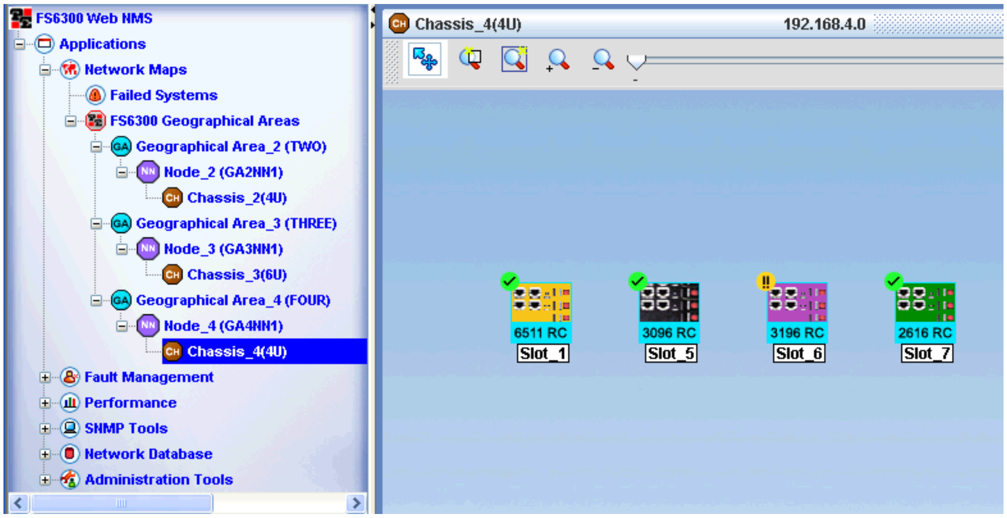


Figure 125. Chassis Card Layer Map

Chapter 10 Contacting Patton for assistance

Chapter contents

Introduction

This chapter contains the following information:

- "Contact information"—describes how to contact Patton technical support for assistance.
- "Warranty Service and Returned Merchandise Authorizations (RMAs)"—contains information about the warranty and obtaining a return merchandise authorization (RMA).

Contact information

Patton Electronics offers a wide array of free technical services. If you have questions about any of our other products we recommend you begin your search for answers by using our technical knowledge base. Here, we have gathered together many of the more commonly asked questions and compiled them into a searchable database to help you quickly solve your problems.

Patton support headquarters in the USA

- Online support: available at **www.patton.com**
- E-mail support: e-mail sent to **support@patton.com** will be answered within 1 business day
- Telephone support: standard telephone support is available five days a week—from **8:00 am** to **5:00 pm** EST (**1300** to **2200** UTC/GMT)—by calling **+1 (301) 975-1007**
- Fax: **+1 (253) 663-5693**

Alternate Patton support for Europe, Middle East, and Africa (EMEA)

- Online support: available at **www.patton-inalp.com**
- E-mail support: e-mail sent to **support@patton-inalp.com** will be answered within 1 business day
- Telephone support: standard telephone support is available five days a week—from **8:00 am** to **5:00 pm** CET (**0900** to **1800** UTC/GMT)—by calling **+41 (0)31 985 25 55**
- Fax: **+41 (0)31 985 25 26**

Warranty Service and Returned Merchandise Authorizations (RMAs)

Patton Electronics is an ISO-9001 certified manufacturer and our products are carefully tested before shipment. All of our products are backed by a comprehensive warranty program.

Note If you purchased your equipment from a Patton Electronics reseller, ask your reseller how you should proceed with warranty service. It is often more convenient for you to work with your local reseller to obtain a replacement. Patton services our products no matter how you acquired them.

Warranty coverage

Our products are under warranty to be free from defects, and we will, at our option, repair or replace the product should it fail within one year from the first date of shipment. Our warranty is limited to defects in workmanship or materials, and does not cover customer damage, lightning or power surge damage, abuse, or unauthorized modification.

Out-of-warranty service

Patton services what we sell, no matter how you acquired it, including malfunctioning products that are no longer under warranty. Our products have a flat fee for repairs. Units damaged by lightning or other catastrophes may require replacement.

Returns for credit

Customer satisfaction is important to us, therefore any product may be returned with authorization within 30 days from the shipment date for a full credit of the purchase price. If you have ordered the wrong equipment or you are dissatisfied in any way, please contact us to request an RMA number to accept your return. Patton is not responsible for equipment returned without a Return Authorization.

Return for credit policy

- Less than 30 days: No Charge. Your credit will be issued upon receipt and inspection of the equipment.
- 30 to 60 days: We will add a 20% restocking charge (crediting your account with 80% of the purchase price).
- Over 60 days: Products will be accepted for repairs only.

RMA numbers

RMA numbers are required for all product returns. You can obtain an RMA by doing one of the following:

- Completing a request on the RMA Request page in the *Support* section at **www.patton.com**
- By calling **+1 (301) 975-1007** and speaking to a Technical Support Engineer
- By sending an e-mail to **returns@patton.com**

All returned units must have the RMA number clearly visible on the outside of the shipping container. Please use the original packing material that the device came in or pack the unit securely to avoid damage during shipping.

Shipping instructions

The RMA number should be clearly visible on the address label. Our shipping address is as follows:

Patton Electronics Company
RMA#: xxxx
7622 Rickenbacker Dr.
Gaithersburg, MD 20879-4773 USA

Patton will ship the equipment back to you in the same manner you ship it to us. Patton will pay the return shipping costs.