Viewing the Alarms Report

To access the **Current Alarms** report, in the System Menu bar, click **System Information** > **Get Information**, and then in the **Reports** panel **Type** list, select **Alarms**.

System Information > Get Information

Reports

Type [Alarms ▼] [Download]

Current Alarms

Severity	Ack'd	Alarm Code	Alarm Name	⊟ Timestamp	Unit Id	Unit Type	Unit Name	Module	Module Name	RF Band	Extended Info
Minor	☐	AC31	DART Under Drive	2011/02/12 14:17:41	SciencesBldg1 1	Host	SciencesBldg1	DART 2	ASTRNY1_Floor4	AWS ABC	Click
Major	☐	AC83	Optical Transmitter Fault	2011/02/11 15:14:11	SciencesBldg1 1-1	PRU	UNKNOWN_REMOTENAME	SFP 1	UNKNOWN_SFPNAME	NA	Click
Major	☐	AC114	RF Power Low	2011/02/11 15:01:45	SciencesBldg1 1-1	PRU	UNKNOWN_REMOTENAME	Power Detector 2	NA	NA	Click
Major	☐	AC114	RF Power Low	2011/02/11 15:01:45	SciencesBldg1 1-1	PRU	UNKNOWN_REMOTENAME	Power Detector 4	NA	NA	Click
Major	☐	AC77	Fan Under Speed	2011/02/11 15:01:43	SciencesBldg1 1-1	PRU	UNKNOWN_REMOTENAME	SeRF	NA	NA	Click

[Refresh]

The **Current Alarms** table provides the following information:

- **Severity**—whether alarm is classified as Major or Minor.

- **Ack'd**—whether the alarm has been acknowledged, as indicated by a checkmark.

- **Alarm Code**—system-assigned alarm code. See "Troubleshooting Alarms" on page 185 or use the "Index of Alarms" on page 313 to find the page number for a specific alarm description, which includes the alarm code.

- **Alarm Name**—descriptive name of alarm.

- **Timestamp**—date and time when the alarm occurred (**YYYY:MM:DD:HH:MM:SS**)

- **Unit Id**—identifies the unit within the system; see "Unit Identification" on page 43.

- **Unit Type**—what the unit is, such as Host or Remote

- **Unit Name**—name assigned to the unit

- **Module**—type of module within the specified unit that is experiencing the alarm (SeRF, DART, Power Detector, SFP)

- **Module Name**—user-assigned name for the module that assists in identifying modules when troubleshooting

- **RF Band**—type of passband provided by the DART (if applicable)

- **Extended Info**—link that provides further information on the alarm, including troubleshooting information.

IFEU + RAU Report

The **IFEU + RAU** report pertains to an InterReach Spectrum system and is not applicable to this release.

Viewing the All Report

The All Report consolidates all available reports into a single web page.

System Information > Get Information

Reports

Type [All ▼] [Download]

Network Statistics

Unit Id	Port	Rx Bytes	Rx Packets	Rx FCS Errors	Tx Bytes	Tx Packets
SciencesBldg1 1	Switch Port	139777411	809147	0	139777411	9566
SciencesBldg1 1	Craft Port	0	0	0	0	9
SciencesBldg1 1	Network Port	139710842	8260	0	139710842	8273
SciencesBldg1 1-1	Switch Port	137580733	800023	0	439957	1348

Hardware Inventory

SciencesBldg1 1(155.226.45.16)Backplane II					
Module Type	Id	Date Code	Hardware Version	Serial Number	Part Number
DART-ASTRNY1_Floor4	2	34/2008	21	224894186	1433212
DART-UNKNOWN_DARTNAME	1	47/2008	11	225364536	1448080
DART-UNKNOWN_DARTNAME	4	23/2009	11	225858576	1465070
DART-UNKNOWN_DARTNAME	5	48/2007	0	00003021	1410689
DART-UNKNOWN_DARTNAME	6	08/2010	21	TR2208YW	1448073
SeRF-I	NA	28/2008	21	224992774	1433780
System Card-I	NA	33/2008	31	225014558	1397156

SciencesBldg1 1-1: LawrenceLab (169.254.48.104)					
Module Type	Id	Date Code	Hardware Version	Serial Number	Part Number
DART-Grizzly4	7	17/2010	11	TR220ACH	1456329
DART-UNKNOWN_DARTNAME	1	24/2008	11	224868062	1432419
DART-UNKNOWN_DARTNAME	3	08/2009	11	225558429	1461877

Downloading a Report

CAUTION! The All Report or Analog Units Report can take several minutes to download.

You can download the reports to your laptop in Windows Excel format.

Do the following to download a report to your computer:

1 In the System Menu bar, click **System Information** > **Get Information**.

2 On the **Get Information** page, in the **Reports** panel **Type** list, select the name of the report that you want to download.

3 Click **Download**.

4 In the **File Download** window, click **Save**.
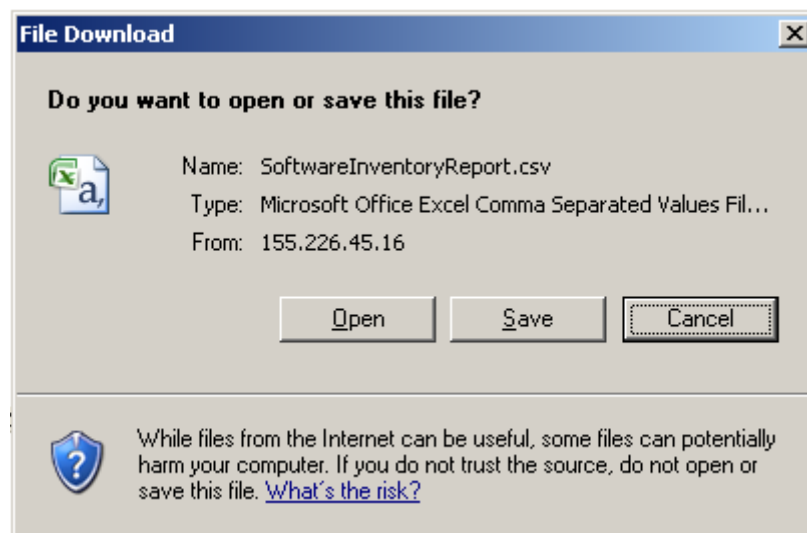
5 In the **Save As** window, navigate to where you want the report file saved, and then click **Save**.
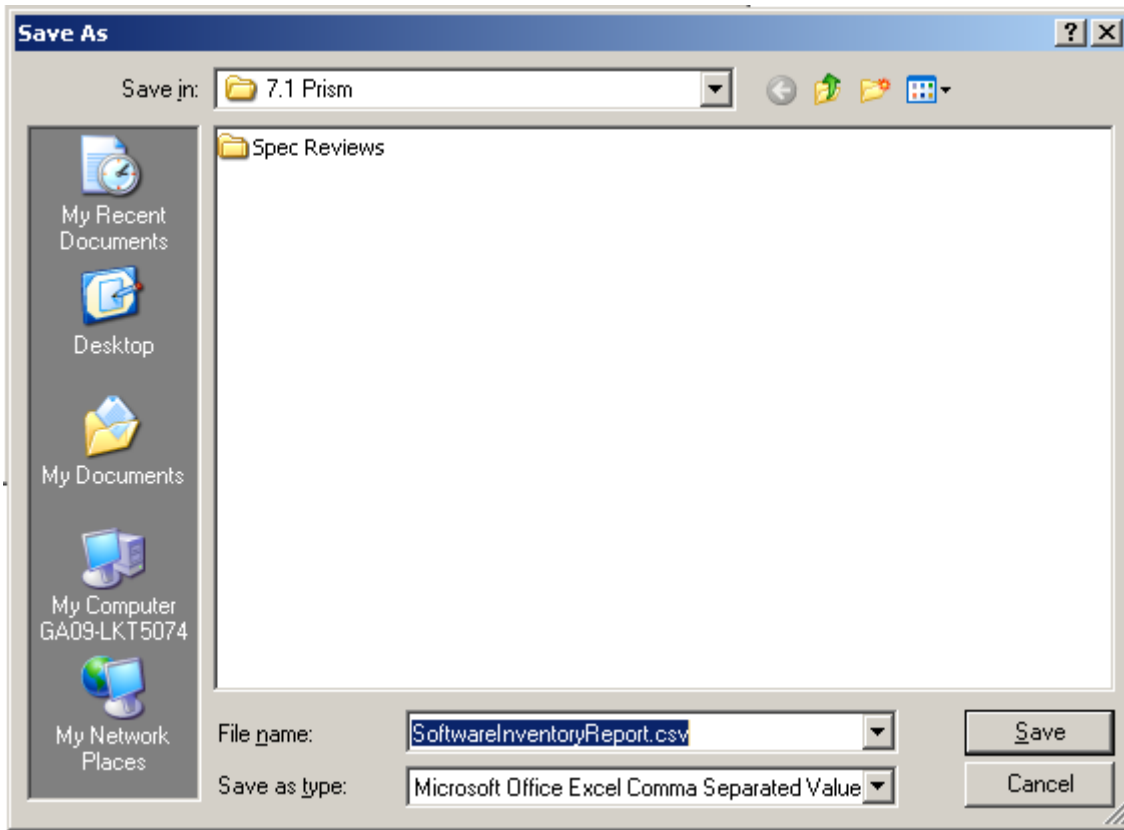
The file is saved as specified.
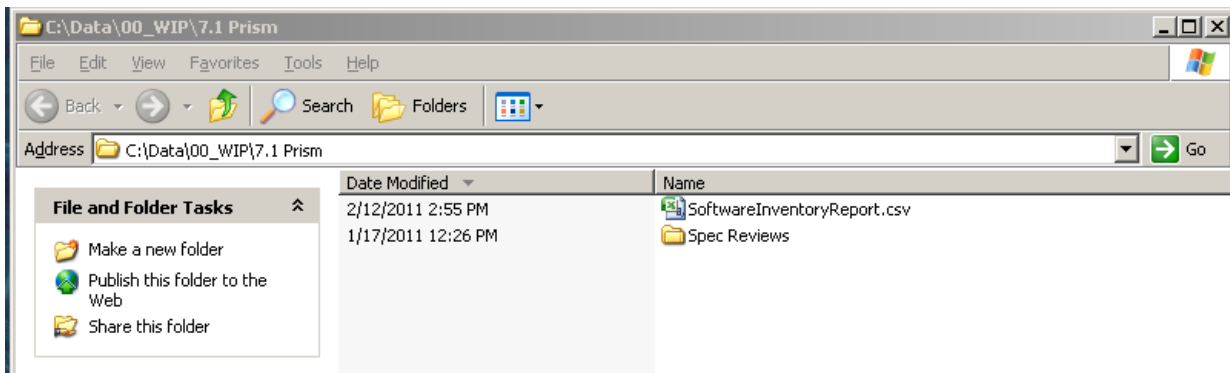
6 Go to the directory where the file was saved to open the file.

NOTE: **While Excel is often used to view this file, Excel uses characters such as hyphens and slashes to create formulas. If discrepancies are seen in this report, use a text editor to verify the report's content.**

GET OPTICS INFORMATION

The **Get Optics Information** page allows you to view information on the fiber.

To access the **Get Optics Information** page, in the System Menu bar, click **System Information** > **Get Optics Information**.

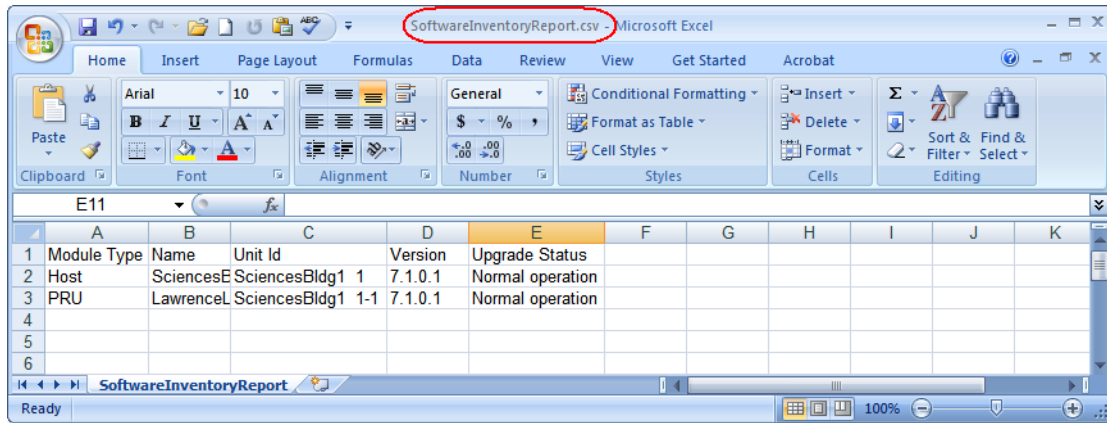|	Unit Type	Unit Name	SFP Number	SFP Name	Optics Type	Wavelength (nm)	Tx Power (dBm)	Rx Power (dBm)	Remote Name	Alarm Status
	Host	SciencesBldg1	1	Astronomy1	Long Range	1310	2.8	-16.1	LawrenceLab	Clear
	Remote	LawrenceLab	1	Astronomy1_PRU	Long Range	1310	3.0	-15.3	SciencesBldg1	Clear

System Information > Get Optics Information

Filter — View [None ▼] contains [ ] [Filter]

[Refresh]

The **Filter** panel has the following elements:

- **View** list—allows you to select a filter to be applied to the page
- **contains** box—allows you to enter filter criteria
- **Filter** button—click to apply the filter

The **Get Optics Information** table has the following elements:
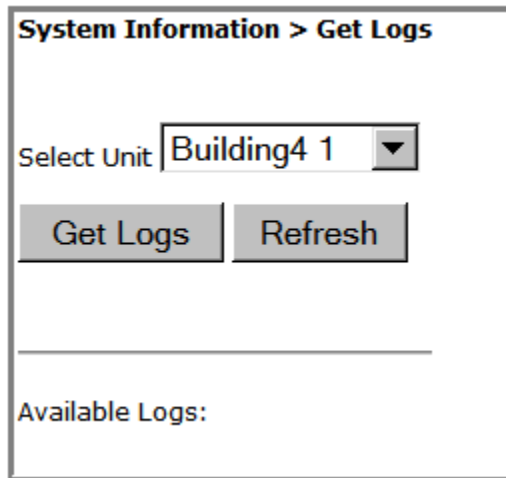
- **Unit Type**—whether the unit is a Host or Remote
- **Unit Name**—user defined name of the unit
- **SFP Number**—system assigned number (from **1** to **8**) for the Optical ports
- **SFP Name**—user entered port name or **UNKNOWN_SFPNAME**, which indicates that a name has not been entered.
- **Optics Type**
  - **LongRange**—26 dB
  - **IntermediateRange**—18 dB).

- **Wavelength (nm)**—number displayed is the wavelength transmitted through this port:
  - Non-duplex and WDM configurations
    - 1550 nm fwd
    - 1310 nm rev
  - CWDM configurations can be one of eight wavelengths:

▪ 1470 nm	▪ 1550 nm
▪ 1490 nm	▪ 1570 nm
▪ 1510 nm	▪ 1590 nm
▪ 1530 nm	▪ 1610 nm

- **Tx Power (dBm)**—launch power level in dBm of forward path signal. The minimum FWD launch power is -2 dBm, and the maximum is 3 dBm.

- **Rx Power (dBm)**—Receive power level in dBm of reverse path signal, which incorporates the launch power of the Remote Unit SFP plus all optical losses (insertion losses, fiber cable loss, and so forth).

- **Remote Name**—name of the Remote connected to this Optics port.

- **Alarm Status**—whether an alarm is active. If an alarm is active, there will be a **Minor** or **Major** link that you click to open a dialog that defines the active alarm, as described in "Viewing Alarm Details" on page 45. The background color of the **Alarm Status** cell also indicates the alarm level (see "Alarm Color Codes" on page 44).
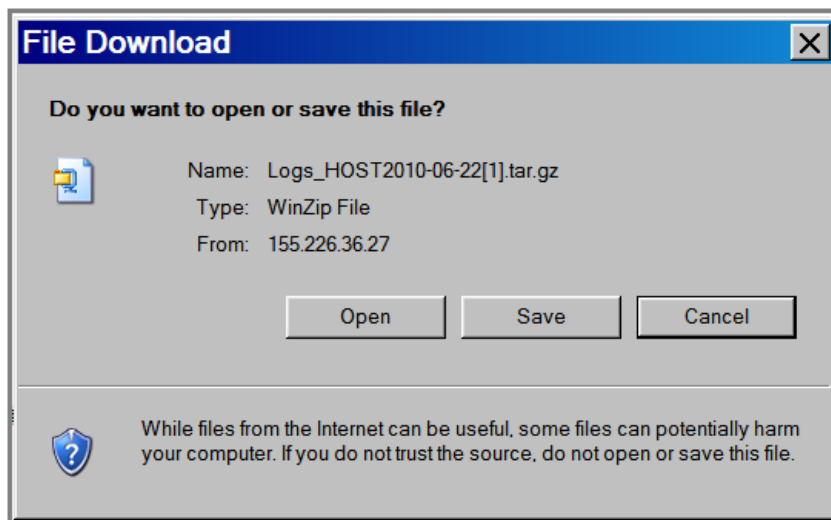
GET LOGS

The **Get Logs** page allows you to save compressed tar archive files of Prism logs. This feature is primarily used by ADC personnel when troubleshooting a system. However, you should know how to create a log so you can email the log to ADC if requested to do so.

1 To access the **Get Logs** page, in the System Menu bar, click **System Information** > **Get Logs**.

```
System Information > Get Logs


Select Unit │Building4 1     ▼│

     Get Logs        Refresh
   _____

   _____

Available Logs:
```

2 Click **Get Logs**.

3 In the **File Download** dialog, click **Save**.

```
File Download                                    ✕

Do you want to open or save this file?

          Name:   Logs_HOST2010-06-22[1].tar.gz
          Type:   WinZip File
          From:   155.226.36.27

              Open          Save          Cancel

     While files from the Internet can be useful, some files can potentially harm
     your computer. If you do not trust the source, do not open or save this file.
```

4 In the **Save As** dialog, navigate to where you want to save the log file.
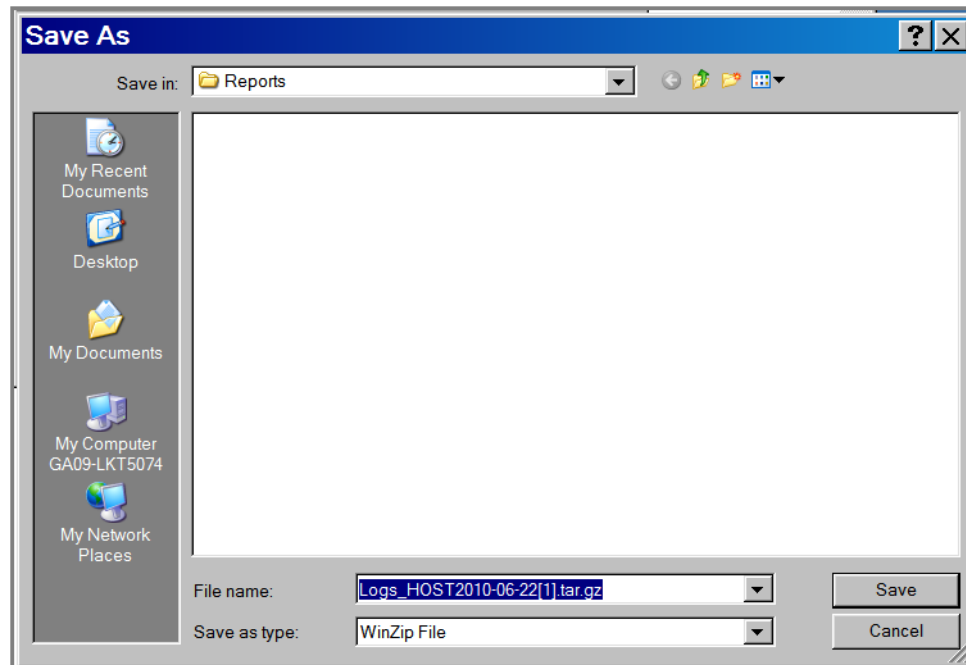
After a log has been created, it is listed as an **Available Log** in the **Get Logs** page.
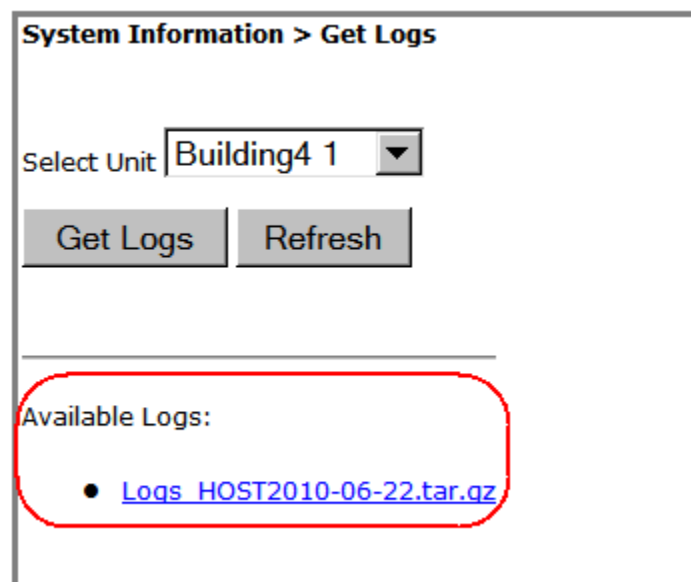
5 In Windows, navigate to where you saved the log zip file on your hard drive.

6 Double-click on the tar file to access the logs.

Intentionally Blank Page

SYSTEM MANAGEMENT

The EMS views and parameters discussed in this section affect the entire Prism system, as opposed to affecting an individual unit or module.

MOVING OR RECONFIGURING FIBERS

If you need to move or reconfigure fibers during troubleshooting, follow the steps below.

1 Move Host SFPs and fibers to their new locations.

2 Do the following if a previously filled SFP position is now empty:

    a There will still be a GUI representation of a Remote on that SFP. To remove this ghost representation, follow the steps in "Clear All Disconnect Alarms" on page 184.

    b To delete fiber and SFP alarms attributed to the abandoned SFP positions, follow the steps in "Clear Current Alarms" on page 170.

3 **Complete this step only for moved DARTs now in an alarmed state.** If the configuration of a Remote Unit DART originally connected to an SFP does not match the configuration of the DART moved to the SFP, the new DART will have an alarm state such as **Module Missing Fault** or **DART Hardware Mismatch**. In this instance, follow the steps in "Clearing DART Configurations" on page 161 to clear the configuration of the DART in the alarmed state.

EDIT THE PROPERTIES OF ALL UNITS IN THE SYSTEM

The **Edit Unit Properties** page that is accessible through the System Menu bar allows you to edit basic information and optionally provide notes for all the units in the system at one time.

To access the **Edit Unit Properties** page, in the System Menu bar, click **System Configuration** > **Edit Unit Properties**.

System Configuration > Edit Unit Properties					
Unit Id	**Unit Name**	**IP Address**	**Contact Alarms**	**Notes**	
SciencesBldg1 1	SciencesBldg1	155.226.45.16	--	Science Building 1, Basement	
SciencesBldg1 1-1	LawrenceLab	169.254.48.104	--	Centennial and Grizzly Peak	

Apply   Refresh

The **Edit Unit Properties** page has the following elements, where each row in the **Edit Unit Properties** table correspond to the unit identified in the **Unit Id** column.

- **Unit Id** column—identifies the unit within the system; see "Unit Identification" on page 43.

- **Unit Name** column—provides a text box that allows you to enter a unique name for the Host and each connected Remote. Each **Unit Name** must start with an alphabetical character, be between 5 and 40 characters (alphanumeric or underscore only), and contain no spaces.

- **IP Address** column—the IP address of the unit

NOTE: An IP address of the type 169.254.x.y will only be communicable if the connected laptop also has a 169.254.x.y address.

- **Contact Alarms** column—identifies active contact alarms, if any. For information on contact alarms, see any of the following:
  - "Contact Alarms—Host System Card" on page 201
  - "Contact Alarms—Remote Unit" on page 201

- **Notes** column—provides a text box that allows you to enter notes specific to the unit. You can enter up to 256 characters; all keyboard characters can be used.

RESET ALL UNITS TO FACTORY DEFAULT

This procedure resets the Host and all connected Remote Units (PRU or URU) to their factory default settings.

This procedure does not clear commanded Out of Service and Band Lockout settings (see Table on page 42).

1 Document all configuration data, as everything except user IDs and IP configuration will have to be re-entered. To record the current configuration:

   a Follow the procedures in "Viewing the All Report" on page 112 to access the system configuration reports.

   b Follow the procedures in "Downloading a Report" on page 113 to download the system configuration reports to a hard drive.

2 In the System Tree, click on the Host icon.

3 In the Unit Menu bar, click **Unit Configuration** > **Edit Properties**, to open the **Unit Configuration > Edit Properties** page.

```
Unit Configuration > Edit Properties [SciencesBldg1 1]

┌─Edit Host Properties────────────────────────────────────────────┐
│                                                                  │
│  Name                    SciencesBldg1                           │
│                                                                  │
│  10 MHz Reference        Internal  ▼                             │
│  Clock                                                           │
│                                                                  │
│  System Card Output      10 MHz     ▼                            │
│  Clock                                                           │
│                                                                  │
│  Notes                   Science Building 1,  ▲                  │
│  (Max 256 chars)         Basement             ▼                  │
│  ┌────────┐ ┌─────────┐ ┌──────────────────────────────────────┐│
│  │ Apply  │ │ Refresh │ │   Reset all units to factory defaults ││
│  └────────┘ └─────────┘ └──────────────────────────────────────┘│
└──────────────────────────────────────────────────────────────────┘
```
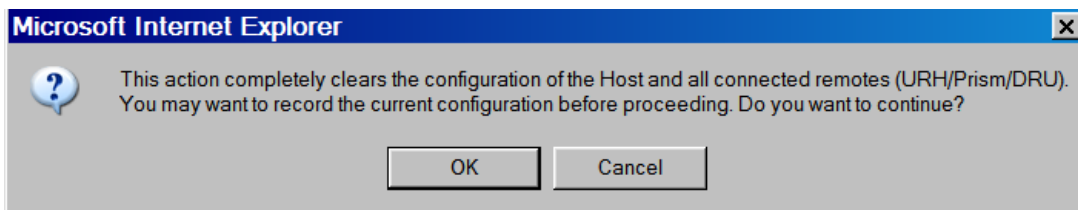
4 Click **Reset all units to factory defaults**.

5 In the confirmation dialog, click **OK**.

```
Microsoft Internet Explorer                                    [x]

  ?   This action completely clears the configuration of the Host and all connected remotes (URH/Prism/DRU).
      You may want to record the current configuration before proceeding. Do you want to continue?

              ┌────────┐      ┌────────┐
              │   OK   │      │ Cancel │
              └────────┘      └────────┘
```

The system configuration is cleared, and you are logged out of your current EMS session.

6 Log back into the EMS to reconfigure the system.

NOTE: **It may take a few minutes for the EMS to recognize the Host and connected remotes.**

BACKING UP A SYSTEM CONFIGURATION

The **Backup** page allows you to backup the system configuration. A backup file size is typically less than 1 MB, and a new backup overwrites the pre-existing backup. You use the backup file to restore the configuration as described in .

Do the following to backup a system configuration:

1 In the System Menu bar, click **System Configuration** > **Backup**.

2 Click **Backup**. If the back up procedure fails, the following error message displays: **Failed to create Back Up**. At the end of a successful backup, a link to the downloaded file appears.

System Configuration > Backup

Click Backup to continue.

Backup

3 To download the back-up file, click the link that appears, the name for which is in the format of **HOSTNAME_<DATETIME>.tgz**. Only one file will be available.
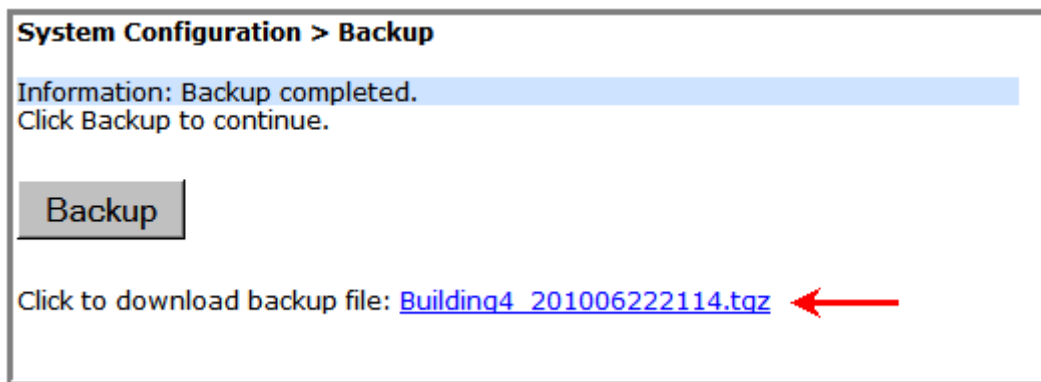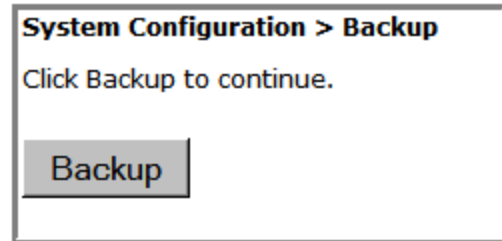
System Configuration > Backup

Information: Backup completed.
Click Backup to continue.

Backup

Click to download backup file: Building4_201006222114.tgz

4 In the **File Download** window, click **Save**.
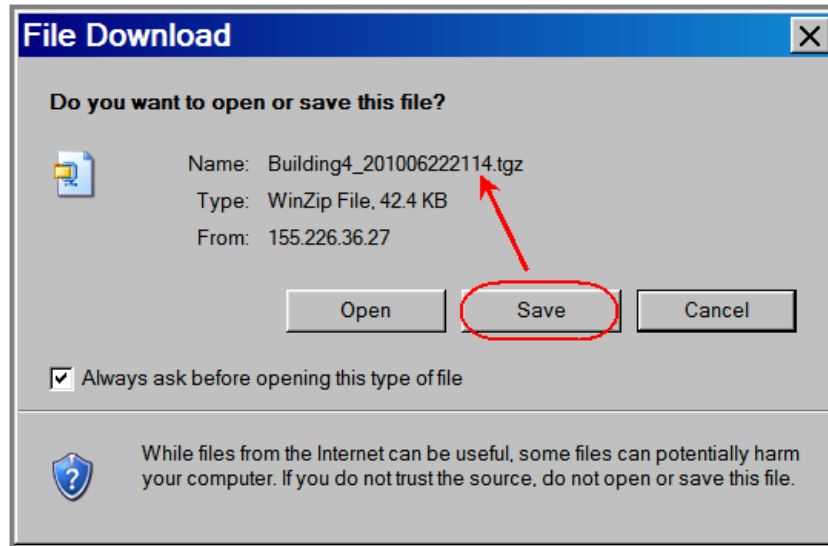
5 In the **Save As** window, navigate to where you want the backup file saved, and then click **Save**.
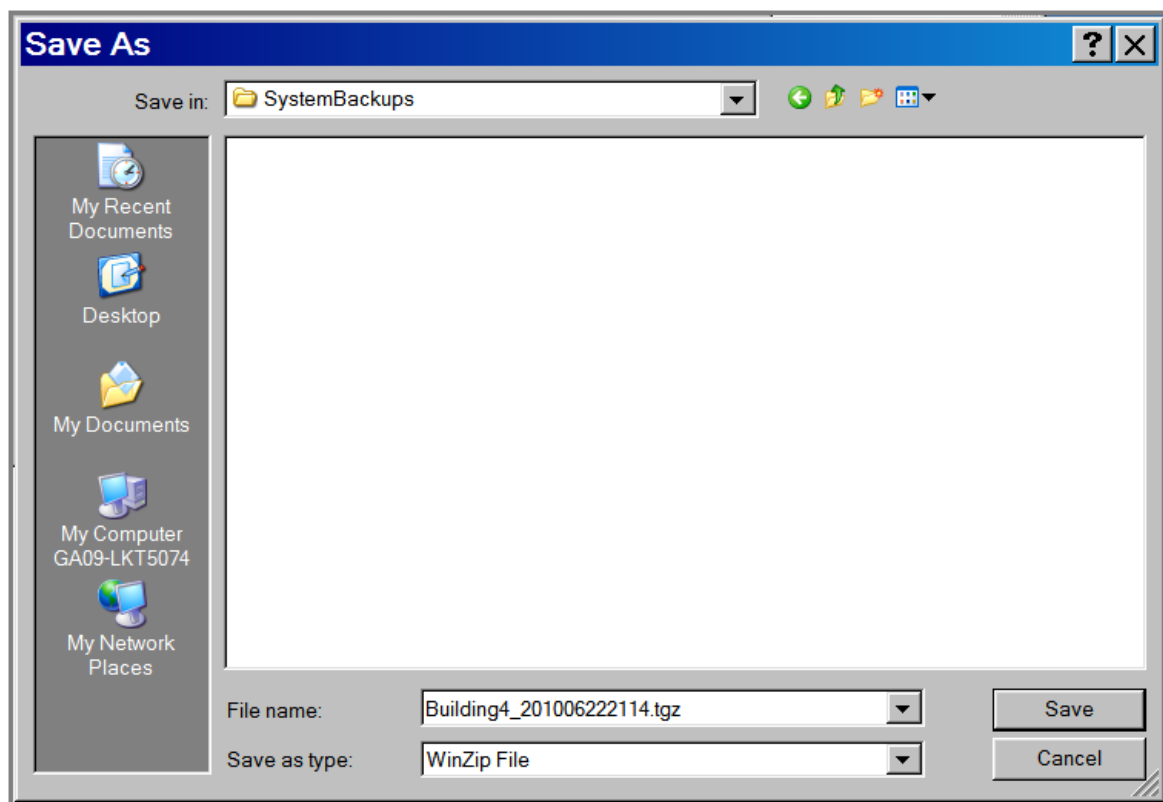
RESTORING A BACKED UP SYSTEM CONFIGURATION

CAUTION!   A System Restore can only occur if a previous system configuration has been backed up as described in "Backing Up a System Configuration" on page 126.

CAUTION!   A system restore requires that you log back into the system. Once you click the Restore button, the system will be unavailable for approximately two minutes. Perform this procedure during a maintenance window.

NOTE: A System Restore can only be performed by a user logged in as admin user or by a user with Network Manager rights. A user assigned only Network User rights will not see the System Restore node in the Function System Tree.

The **System Restore page** allows for a restoration of a backed up system configuration, as follows:

- The Restore function assumes that the same or comparable replacement hardware components are in place as when the Backup function occurred. If hardware component changes have occurred, alarms that point to the differences will arise.

- If a Remote has been added (that is, was not part of the original system hardware setup), then the newly added Remote will not be restored since it was not present during the system configuration backup.

Do the following to restore a system backup:

1   Make sure there is sufficient disk space for the backed up system configuration that you want to restore.

2   In the System Menu bar, click **System Configuration** > **Restore**.

3   Click the **Browse** button next to the **File** box to browse to the location of the backup file.
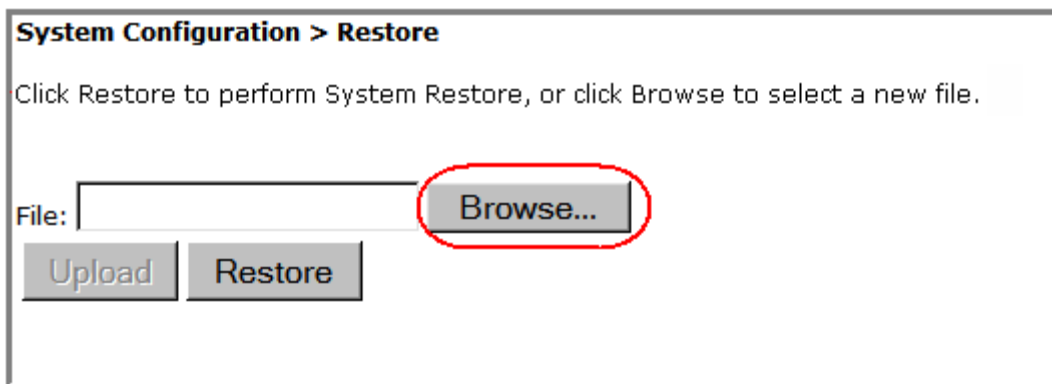
4 In the **Choose File** window, click on the back-up file to select it (the backup filename is in the format of **HOSTNAME_<DATETIME>.tgz**, and then click **Open**.
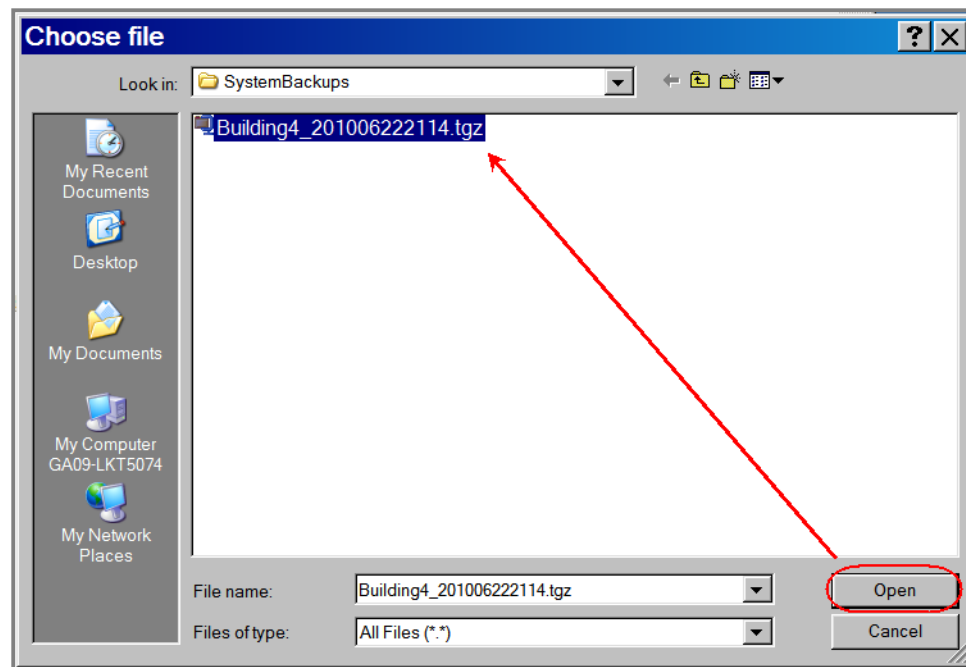
5 In the **Restore** page, wait for the file name and path to display in the **File** box and for the ennoblement of the **Upload** button, and then click **Upload**.
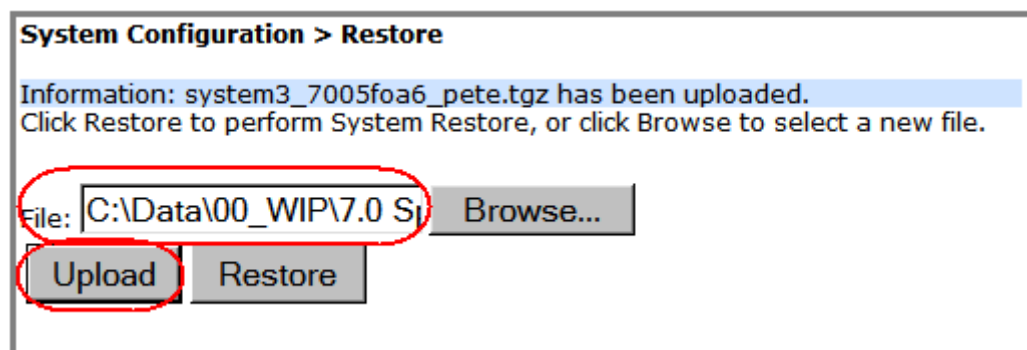
6 In the **Restore** page, wait for the file upload message to display and for the ennoblement of the **Upload** and **Restore** buttons, and then click **Restore**.
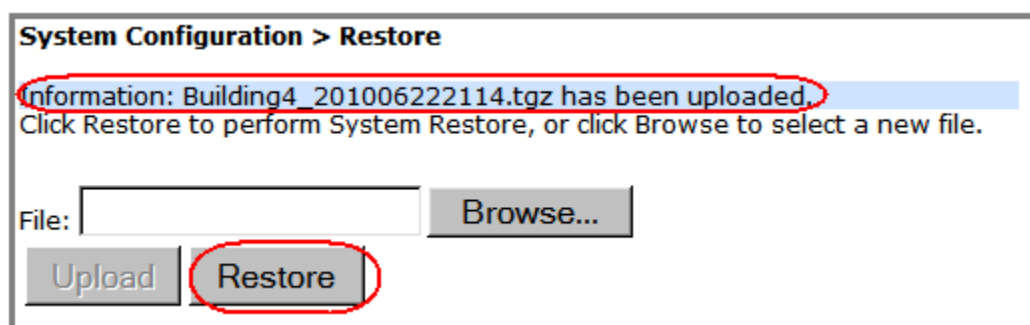
7 In the confirmation dialog, click **OK**.
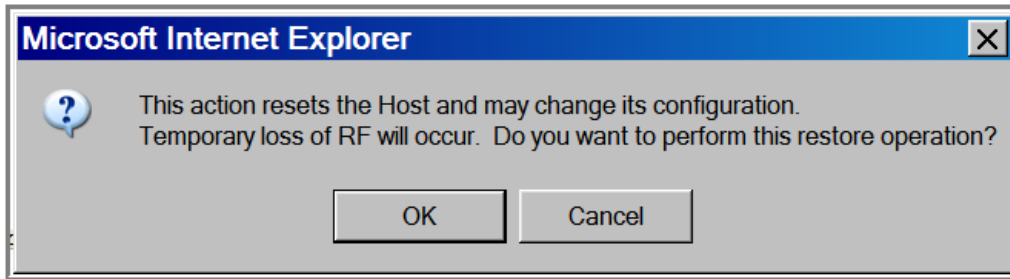
Status messages display to notify you if the restoration failed or completed successfully.

After a successful restoration, you are logged out of the system.

8 Log back in to the EMS to continue management activities.

PERFORM SYSTEM TEST

System Test performs an RF integrity check of the system. Certain alarms (such as the RAU **Antenna Disconnect** alarm) can only be set or cleared by running System Test.

CAUTION! **Running System Test (System Configuration > Perform System Test) with un-terminated Host DARTs may cause a false RLM Upconvert Fault. Ensure that all Host DARTs are terminated before running System Test.**

CAUTION! **System Test interrupts RF transmission; System Test should therefore only be run during a normal maintenance window.**

CAUTION! **Do not make any software or hardware configuration changes during System Test, as changes made during the test will make the test results unreliable.**

1 In the System Menu bar, click **System Configuration** > **Perform System Test**.

System Configuration > Perform System Test											

Do not make any configuration changes during System Test as this causes test results to be unreliable.
System Test takes down the RF signal for ALL bands and DARTs for up to two minutes per band.
Do you want to continue?

Bands [All ▼] DART [All ▼]

[Perform System Test]   [Refresh]

Last Test Results
Click Here to download

Last Test Run Time: 2011/03/30 09:42:33

Severity	Ack'd	Alarm Code	Alarm Name	▼ Timestamp	Unit Id	Unit Type	Unit Name	Module	Module Name	RF Band	Extended Info
Major	☐	AC114	RF Power Low	2011/03/29 10:22:35	mhost 1-5	URU	UNKNOWN_REMOTENAME	Power Detector 2	NA	NA	Click
Major	☐	AC114	RF Power Low	2011/03/29 10:22:35	mhost 1-5	URU	UNKNOWN_REMOTENAME	Power Detector 3	NA	NA	Click
Major	☐	AC114	RF Power Low	2011/03/29 10:23:14	mhost 1-7	URU	UNKNOWN_REMOTENAME	Power Detector 2	NA	NA	Click
Major	☐	AC114	RF Power Low	2011/03/29 10:23:14	mhost 1-7	URU	UNKNOWN_REMOTENAME	Power Detector 3	NA	NA	Click
Major	☐	AC114	RF Power Low	2011/03/29 10:44:31	mhost 1-7	URU	mhRemote7	Power Detector 1	NA	Cellular AA1A2	Click
Major	☐	AC114	RF Power Low	2011/03/29 10:46:40	mhost 1-5	URU	mhRemote5	Power Detector 1	NA	Cellular AA1A2	Click
Minor	☐	AC31	DART Under Drive	2011/03/30 09:42:48	mhost 1	Host	mhost	DART 1	host850_1	Cellular AA1A2	Click
Minor	☐	AC31	DART Under Drive	2011/03/30 09:42:48	mhost 1	Host	mhost	DART 2	host900_2	SMR High	Click
Minor	☐	AC31	DART Under Drive	2011/03/30 09:42:48	mhost 1	Host	mhost	DART 3	host800_3	SMR Low	Click
Minor	☐	AC31	DART Under Drive	2011/03/30 09:42:48	mhost 1	Host	mhost	DART 5	host1900_5	PCS ADB	Click
Minor	☐	AC31	DART Under Drive	2011/03/30 09:42:48	mhost 1	Host	mhost	DART 6	host1900_6	PCS C	Click

NOTE: **The table at the bottom of the Perform System Test page presents the results of the last System Test, if any, as shown above.**

2 In the **Bands** list, select the passbands for which you want to perform System Test. Only configured passbands will be listed in the **Bands** list.

3 In the **DART** list, select the DART you want to perform System Test. Only those DARTS that are available will be listed in the **DART** list.

CAUTION! Regardless if only 1 DART or all DARTs are selected for System Test, System Test temporarily shuts down the RF to all DARTs in the system.

4 Click **Perform System Test**. A **System Test has started** message displays.

This message should be followed by one of these messages. You may need to click **Refresh** to see these messages.

- **System Test passed.**
- **System Test failed.**
- **System Test not available.**
- **System Test passed – exceptions noted in log file.**

After a few seconds, the **Last Test Results** panel updates with a list of major and minor alarms with a corresponding timestamp for when System Test was run.

5 (Optional) Do the following to download the results of System Test (to make the file available for later use, such as troubleshooting).

a Click the **Click Here to Download** link.

b In the **File Download** dialog, click **Save**.
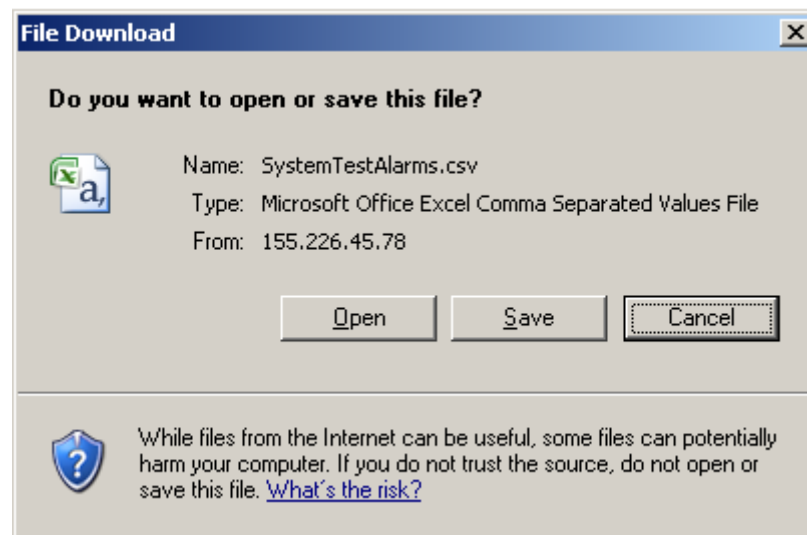
    c In the Save As dialog, navigate to where you want to save the file, and then click Save.
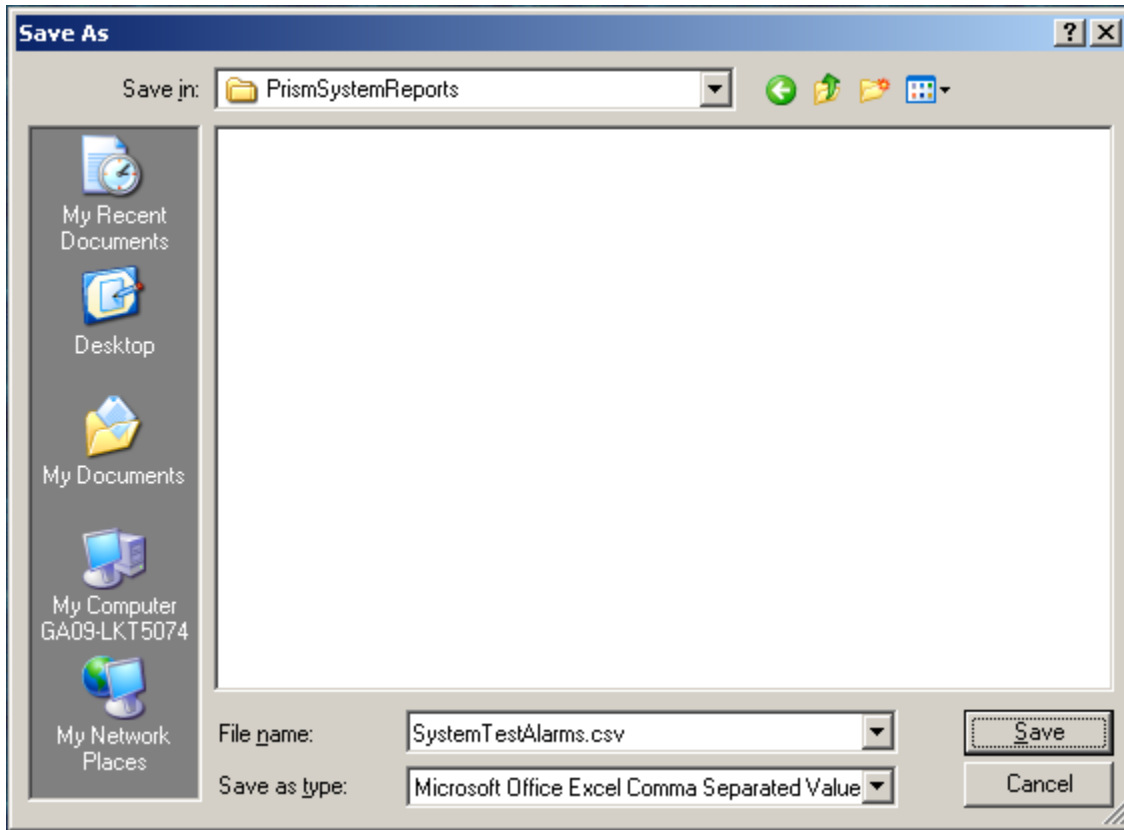
The file is saved in Excel format.

	A	B	C	D	E	F	G	H	I	J
1	Severity	Alarm Code	Alarm Name	Timestamp	Unit Id	Remote Ty	Remote Name	Module	Module Name	RF Band
2	Major	114	RF Power Low	3/29/2011 10:22	5	URU		Power Detector 2	UNKNOWN_REMOTENAME	Undefined(NA)
3	Major	114	RF Power Low	3/29/2011 10:22	5	URU		Power Detector 3	UNKNOWN_REMOTENAME	Undefined(NA)
4	Major	114	RF Power Low	3/29/2011 10:23	7	URU		Power Detector 2	UNKNOWN_REMOTENAME	Undefined(NA)
5	Major	114	RF Power Low	3/29/2011 10:23	7	URU		Power Detector 3	UNKNOWN_REMOTENAME	Undefined(NA)
6	Major	114	RF Power Low	3/29/2011 10:44	7	URU		Power Detector 1	mhRemote7	800 SMR Classic
7	Major	114	RF Power Low	3/29/2011 10:46	5	URU		Power Detector 1	mhRemote5	800 SMR Classic
8	Minor	31	DART Under Drive	3/30/2011 9:42	1	Host		DART 1	mhost	800 SMR Classic
9	Minor	31	DART Under Drive	3/30/2011 9:42	1	Host		DART 2	mhost	Undefined(94)
10	Minor	31	DART Under Drive	3/30/2011 9:42	1	Host		DART 3	mhost	Undefined(93)
11	Minor	31	DART Under Drive	3/30/2011 9:42	1	Host		DART 5	mhost	Undefined(85)
12	Minor	31	DART Under Drive	3/30/2011 9:42	1	Host		DART 6	mhost	Undefined(48)
13										
14										

SCHEDULE SYSTEM TEST

You can schedule a System Test to run on a specific date and time, as described in:

- "Schedule System Tests by Date and Time" on page 135
- "Disable a Scheduled System Test" on page 137

Schedule System Tests by Date and Time

CAUTION! **Running System Test (System Configuration > Perform System Test) with un-terminated Host DARTs may cause a false RLM Upconvert Fault. Ensure that all Host DARTs are terminated before running System Test.**

CAUTION! **System Test interrupts RF transmission; System Test should therefore only be run during a normal maintenance window.**

CAUTION! **Do not make any software or hardware configuration changes during System Test, as changes made during the test will make the test results unreliable.**

Do the following to schedule a single or recurring System Test:

1 In the System Menu bar, click **System Configuration** > **Schedule System Test**.

> **System Configuration > Schedule System Test**
>
> Warning: A system test will take the system offline.
>
> **Enable** ☐
> **Bands** [All ▼]
> **DART** [All ▼]
> **Date (YYYY/MM/DD)** [   ] [...]
> **Time (HH:MM:SS)** [   ]
>
> **Recurrence** ◉ Day(s) (1-30) [   ]
>   ○ Week(s) (1-4) [   ]
>
> [Apply] [Refresh]

2 Select **Enable** to enable the scheduled System Test (see also "Disable a Scheduled System Test" on page 137).

3 In the **Bands** list, select the band(s) that you want to test.

4 In the **DART** list, select the DART(s) that you want to test.

5 Click the icon to the right of the **DATE** box to schedule on which date the System Test will run. If you enter the date manually, use the `YYYY/MM/DD` format. For example, to run a System Test on 14 June 2011, enter: `2011/06/14`.

6 In the **Time** box, enter the time that the System Test is to run. Use the 24-hour timeclock format of `HH:MM:SS`.

7 (Optional) Use the **Recurrence** radio buttons to set up a recurring System Test.

- To have the System Test recurrence interval be counted by days, select the **Day(s) (1-30)** radio button, and then in the corresponding box, enter how many days should pass between each occurrence of this System Test.

- To have the System Test recurrence interval be counted by weeks, select the **Week(s) (1-4)** radio button, and then in the corresponding box, enter how many weeks should pass between each occurrence of this System Test.

8 Click **Apply**.

NOTE: If you leave either the DATE or TIME parameter empty and then click Apply, Schedule System Test will not run. However, if you leave both the DATE and TIME parameters empty and then click Apply, the System Test starts immediately.

The following example has scheduled a System Test for 850 Classic passbands on 850 Classic DARTs installed in Host1 to occur on 2 April 2011 at 1:00 AM. This System Test will occur in one-week intervals.

```
System Configuration > Schedule System Test

Warning: A system test will take the system offline.

Enable              ☑

Bands               [850 Classic         ▼]

DART                [1-host850_1-850 Classic ▼]

Date ( YYYY/MM/DD ) [2011/04/02            ] [...]

Time ( HH:MM:SS )   [01:00:00              ]

                    ○ Day(s) (1-30) [        ]
Recurrence
                    ⊙ Week(s) (1-4) [1       ]

[Apply]  [Refresh]
```

Disable a Scheduled System Test

When you disable a scheduled System Test, the **Bands**, **DART**, **Date**, and **Time** setting remain, but the test will not be run again until enabled.

1 In the System Menu bar, click **System Configuration** > **Schedule System Test**.

2 Deselect **Enable**.

3 Click **Apply**.

System Configuration > Schedule System Test

Warning: A system test will take the system offline.

Enable	☐
Bands	850 Classic
DART	1-host850_1-850 Classic
Date (YYYY/MM/DD)	2011/04/02 ...
Time (HH:MM:SS)	01:00:00
Recurrence	○ Day(s) (1-30)
	⦿ Week(s) (1-4) 1

Apply   Refresh

SET SNMP TRAP MANAGERS

The **Set SNMP Trap Managers** page allows you to add, delete, and modify SNMP Trap Managers.

The **Registered Trap Manager** table, at the top of the page, details any existing SNMP Trap Managers, where:

- **Select** radio button—allows you to select an existing SNMP Trap Manager to modify or delete it.

- **IP Address**—shows the IP address of registered trap managers

- **Port**—shows the port number for registered trap managers

- **Community**—shows the Community password for registered trap managers

- **Version**—shows the trap version for registered trap managers

If a Trap Manager has not been created, the table is empty:

Adding an SNMP Trap Manager

1 In the System Menu bar, click **System Configuration** > **Set SNMP Trap Managers**.

2 In the **Add New Trap Manager** panel, do the following:

a In the **IP Address** box enter the IP address of the device that you want to add as a trap receiver. The address must be in the xxx.xxx.xxx.xxx format.

b In the **Port** box, enter the port on the device that will receive the traps. The normal and recommended SNMP Trap port is 162.

c In the **Community** box, enter a password that will allow access to the device. The **Community** password must be between 6 and 20 alphanumeric characters (usually `public` or `private`).

d In the **Version** list, select the trap version for the SNMP Trap Manager that you are registering (**V1** or **V2c**).

3 Click **Add**.

The **Registered Trap Managers** table updates with the new SNMP Trap Manager.

Modifying an SNMP Trap Manager

1 In the System Menu bar, click **System Configuration** > **Set SNMP Trap Managers**. The **Registered Trap Managers** table lists existing SNMP Trap Managers.

2 In the **Registered Trap Managers** table, select the trap manager that you want to modify.

3 In the **Add New Trap Manager** panel, do any of the following:

- In the **IP Address** box enter a new IP address. The address must be in the **xxx.xxx.xxx.xxx** format.

- In the **Port** box, enter the port on the device that will receive the traps. The normal and recommended SNMP trap port is 162.

- In the **Community** box, enter a password that allows access to the device (usually public or private). The Community password is limited to 20 characters.

- In the **Version** list, select the trap version for the SNMP Trap Manager that you are registering.

4 Click **Modify**.

The **Registered Trap Managers** table updates with the modified SNMP Trap Manager.

Deleting an SNMP Trap Manager

1   In the System Menu bar, click **System Configuration** > **Set SNMP Trap Managers**. The **Registered Trap Managers** table lists existing SNMP Trap Managers.

2   In the **Registered Trap Managers** table, select the trap manager that you want to delete.

3   Click **Delete**.

4   In the confirmation window, click **OK**.

The deleted SNMP Trap Manager is removed from the **Registered Trap Managers** table and will no longer receive traps.

System Configuration > Set SNMP Trap Managers

Information: Operation completed.
Registered Trap Manager

Select	IP Address	Port	Community	Version
○	155.226.36.13	162	public	V2c

Delete

Add New Trap Manager

IP Address

Port

Community

Version V1

Add   Modify   Refresh

SETUP SNMP

1 To access the **Setup SNMP** page, in the System Menu bar, click **System Configuration > Setup SNMP**.

```
System Configuration > Setup SNMP

┌─SNMP V1 Agent Override──────────────────────┐
│                                             │
│  Mode              [Disabled ▼]             │
│                                             │
│  Address           [_____]   │
│                                             │
│  SNMP Port Number  [161      ]              │
│                                             │
│  [ Apply ]  [ Refresh ]                     │
└─────────────────────────────────────────────┘
```

2 In the **SNMP V1 Agent Override** panel, do the following.

  a In the **Mode** list, select the SNMP V1 Agent Override mode:

  - **Enabled**
  - **Disabled**

  b In the **Address** box, enter the SNMP V1 Agent Override address. If the SNMP Agent Override **Mode** is not **Disabled**, the system uses this address as the source address in the traps.

3 In the **SNMP Port Number** box, enter the SNMP port number for `sets` and `gets`.

4 Click **Apply** to modify the SNMP settings.

ACTIVATE OPTIONAL FEATURES

The **Activate Optional Features** page allows you to activate optional features available in the system that are purchased after the Host Unit has been shipped.

NOTE: **Activation Codes are supplied by ADC Technical Assistance (see** "Appendix C: Contacting ADC/TE Connectivity" on page 297**).**

1 To access the **Activate Optional Features** page, in the System Menu bar, click **System Configuration** > **Activate Optional Features**.

2 In the **Activation Code** box that corresponds to the feature that you want to activate, enter the activation code provided by ADC.

3 Click **Activate**. The following **Information** message displays.

Intentionally Blank Page

MANAGING UNITS

This section describes the Prism EMS parameters whose settings affect the individual units within a Prism system.

BASIC UNIT VIEWS

When you click on a device icon in the System Tree, the following view opens in the EMS View Frame, in which there are three places where the selected device is identified. Notice also the indicators for active alarms. In this instance the alarm overlays on the Host and Remote Unit icons indicate that an alarm is active on each device, and the Alarm Counter shows the count of active alarms.

The following graphic identifies the components in a basic unit view.
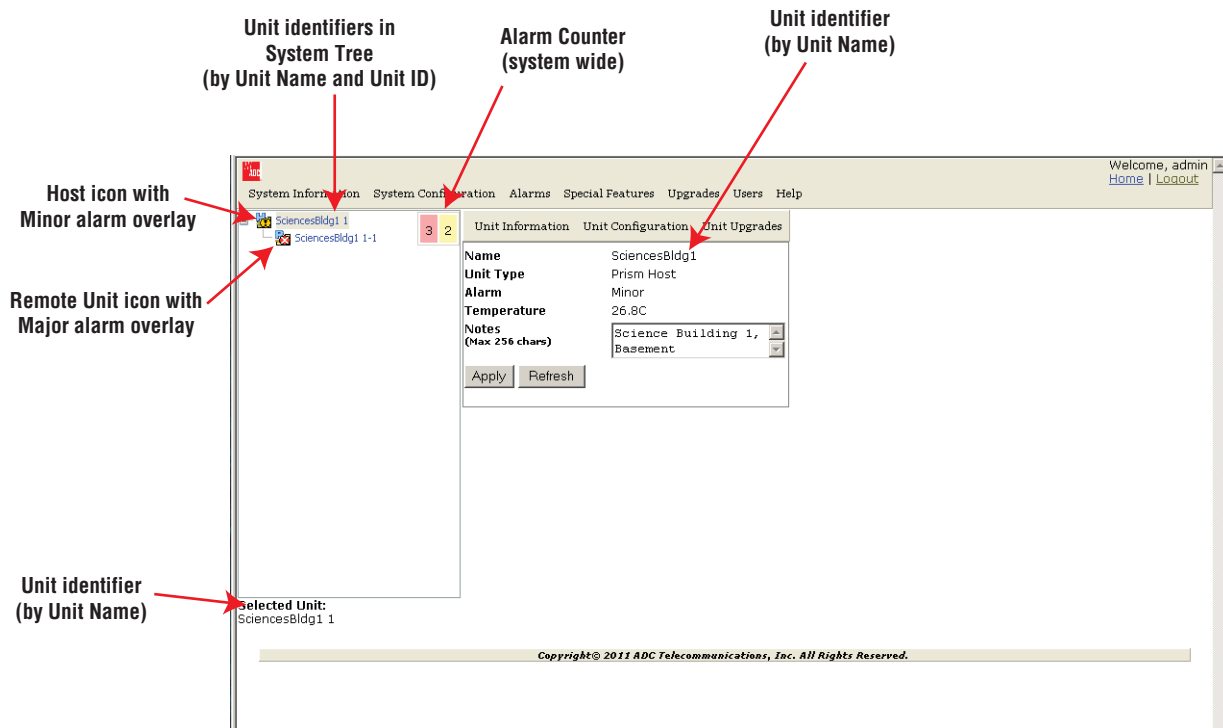
Figure 22. Overview of Components in a Basic Unit View

The Unit view provides the following information:

- **Name**—user-defined or system name of the selected unit.

- **Unit Type**—the type of device that the selected unit is:
  - **Host**
  - **PRU**—Prism Remote Unit
  - **URU**—URH Remote Unit

- **Alarm**—highest level of alarm occurring on the selected unit. Notice that in this example, the Alarm indicators show that there are four Minor alarms active on this system. The Unit view lets you know that at least one of the alarms is active on the Host.

- **Temperature**—internal temperature of the selected unit.

- **Notes**—text box that allows you to enter notes specific to the selected unit. You can enter up to 256 characters; all keyboard characters can be used.

VIEW OPTICAL PORTS

The **View Optical Ports** page shows the current usage and alarm status of the optical ports on a Host or a PRU/URU plus the current values of key operating parameters. The Host and PRU/URU chassis have eight optical ports, but the **View Optical Ports** page only shows active ports (those physically connected to a Host or PRU/URU). Each port in the page represents one set of forward and reverse paths between a Host and Remote.

1   In the System Tree, click on an icon for a Host or Remote Unit.

2   In the Unit Menu bar, click **Unit Information** > **View Optical Ports**.

The **View Optical Ports** table has the following components:

- **SFP Number**—System assigned port number.

- **SFP Name**—user entered port name or **UNKNOWN_SFPNAME**, which indicates that no name has been entered.

- **In/Out**—used for cascading, which is not supported in this release. The Host will therefore always be set as **Out** (indicates that the forward link for the connected SFP is going away from the Host) and the SFPs for all Remote Units will always be set as **In**.

- **Optics Type**
    - **LongRange**—26 dB
    - **IntermediateRange**—18 dB.

- **Wavelength (nm)**—wave length transmitted through this port:
  – Non-duplex and WDM configurations: 1550 nm fwd or 1310 nm rev
  – CWDM configurations can be one of eight wavelengths:

▪ 1470 nm	▪ 1510 nm	▪ 1550 nm	▪ 1590 nm
▪ 1490 nm	▪ 1530 nm	▪ 1570 nm	▪ 1610 nm

- **Tx Power (dBm)**—launch power level in dBm of forward path signal. The minimum FWD launch power is -2 dBm, and the maximum is 3 dBm.

- **Rx Power (dBm)**—receive power level in dBm of reverse path signal, which incorporates the launch power of the Remote Unit SFP plus all optical losses (insertion losses, fiber cable loss, and so forth).

- **Host Name/Remote Name**—dependent on the unit selected in Step 1 on page 149:
  – If a Host Unit was selected, then the column is labeled **Remote Name** and the data in the column pertains to the Remote connected to this Optical port identified in **SFP Number** and **SFP Name**.
  – If a Remote Unit was selected, then the column is labeled **Host Name** and the data in the column pertains to the Host (for selected PRU/URU) connected to this Optical port identified in **SFP Number** and **SFP Name**.

- **Alarm Status**—whether an alarm is active. If an alarm is active, there will be a **Minor** or **Major** link that you click to open a dialog that defines the active alarm, as described in "Viewing Alarm Details" on page 45. The background color of the **Alarm Status** cell also indicates the alarm level (see "Alarm Color Codes" on page 44).

VIEWING DARTS

1 In the System Tree, click on the icon of the Host or PRU/URU for which you want to view information on its DARTs.

2 In the Unit Menu bar, click **Unit Information** > **View DARTs** to open the **View DARTs** page.

Unit Information > View DARTs [SciencesBldg1 1-1]				
▼ **DART Number**	**DART Name**	**Band Type**	**Passband**	**Alarm Status**
1	UNKNOWN_DARTNAME	850 Classic	Cellular A2ABA1B1	Clear
3	UNKNOWN_DARTNAME	1900 PCS DL SuperDART	NA	Clear
7	Grizzly4	2100 AWS Classic	AWS ABC	Clear

Refresh

The table in the **View DARTs** page provides the following information:

- **DART Number**—identifies any installed DARTs by the slot number in which it is installed in the Host or PRU/URU chassis

- **DART Name**—system or user-assigned name; default is **UNKNOWN_DARTNAME**.

- **Band Type**—which DART model is installed, and the band type that it is providing

- **Passband**—type of passband

- **Alarm Status**—whether an alarm is active. If an alarm is active, there will be a **Minor** or **Major** link that you click to open a dialog that defines the active alarm, as described in "Viewing Alarm Details" on page 45. The background color of the **Alarm Status** cell also indicates the alarm level (see "Alarm Color Codes" on page 44).

VIEWING NETWORK STATISTICS

1 In the System Tree, click on an icon for a Host or Remote Unit.

2 In the Unit Menu bar, click **Unit Information** > **View Network Statistics** to open the **View Network Statistics** page.

Port	Rx Bytes	Rx Packets	Rx FCS Errors	Rx BroadCast Pkts	Rx MultiCast Pkts	Rx Fragmented Frames	Rx Jabber Frames	Tx Byte Counter	Tx Pkt Counter	Tx BroadCast Pkts	Tx MultiCast Pkts
Craft Port	0	0	0	0	0	0	0	654	9	4	5
OptEnetPort2	0	0	0	0	0	0	0	234365644	738	734329	628405
OptEnetPort3	0	0	0	0	0	0	0	234365880	738	734330	628407
OptEnetPort4	0	0	0	0	0	0	0	234365880	738	734330	628407
OptEnetPort5	0	0	0	0	0	0	0	234365880	738	734330	628407
OptEnetPort6	0	0	0	0	0	0	0	234366018	738	734330	628409
OptEnetPort7	0	0	0	0	0	0	0	234366278	738	734332	628410
OptEnetPort8	0	0	0	0	0	0	0	234366278	738	734332	628410
Network Port	0	0	0	0	0	0	0	0	0	0	0
Management Port	1425707	3713	0	81	10	0	0	234816063	4344	734251	628400
Switch Port	234814064	1366973	0	734246	628389	0	0	1389667	3761	67	5
OptEnetPort1	234814526	4341	0	734246	628391	0	0	1393499	3689	81	10

Reset Counter

The **View Network Statistics** table has the following components:

• **Port**—Identifies the ports in the network.

• **Rx Bytes**—Receive byte counter that increments by the byte count of frames received, including those in bad packets, excluding preamble and SFD but including FCS bytes.

• **Rx Packets**—Receive packet counter that increments for each frame received packet (including bad packets, all unicast, broadcast, and multicast packets).

• **RX FCS Errors**—Receive FCS error counter that increments for each frame received that has an integral 64 to 1518 length and contains a frame check sequence error.

• **Rx Broadcast Pkts**—Receive broadcast packet counter that increments for each broadcast good frame of lengths 64 to 1518 (non VLAN) or 1522 (VLAN), excluding multicast frames. Does not include range/length errors.

• **Rx Multicast Pkts**—Receive multicast packet counter that increments for each multicast good frame of lengths 64 to 1518 (non VLAN) or 1522 (VLAN), excluding broadcast frames. This count does not include range/length errors.

• **Rx Fragmented Frames**—Receive fragments counter that increments for each frame received that contains an invalid FCS and is less than 64 bytes. This includes integral and non-integral lengths.

• **Rx Jabber Frames**—Receive jabber counter that increments for frames received that exceed 1518 (non VLAN) or 1522 (VLAN) bytes and contain an invalid FCS. This includes alignment errors.

- **Tx Byte Counter**—Transmit byte counter that increments by the number of bytes that were put on the wire including fragments of frames that were involved with collisions. This count does not include preamble/SFD or jam bytes. This counter does not count if the frame is truncated.

- **Tx Pkt Counter**—Transmit packet counter that increments for each transmitted packet (including bad packets, excessive deferred packets, excessive collision packets, late collision packets, all unicast, broadcast, and multicast packets).

- **Tx Broadcast Pkts**—Transmit broadcast packet counter that increments for each broadcast frame transmitted (excluding multicast frames).

- **Tx Multicast Pkts**—Transmit multicast packet counter that increments for each multicast valid frame transmitted (excluding broadcast frames).

- **Reset Counter** button—click to clear the statistics in the **Network Statistics** page.

EDITING UNIT PROPERTIES

Unit properties are set during initial setup, but can be changed at any time. See one of the following:

- "Configure Basic Host Unit Properties" on page 64
- "Label the PRU/URU" on page 66.

CONFIGURING OPTICAL PORTS

Optical port configurations are set during initial setup, but can be changed at any time. See one of the following:

- See "Label the Host Optical Ports" on page 67.
- See "Label PRU/URU Optical Ports" on page 70.

VIEWING THE STATUS OF THE HOST UNIT

1   In the System Tree, click on the Host icon.

2   In the Unit Menu bar, click **Unit Information** > **View Status**.

The **Unit Information > View Status** page provides the following information for the selected Host. The background of each table cell is color coded to the level of the alarm; see "Viewing Parameters and Alarms" on page 44. For further information on these faults and alarms, see "Troubleshooting Alarms" on page 185.

- **Module Status** table—provides status information for installed DARTs, where columns 1 through 8 correspond to the slot in which the DART resides (Column 1 = Slot 1, and so forth). If a DART column has no background color, a DART is not installed in that slot.

    – **DART Fault**—Summary of DART Downconverter 1 Synthesizer Unlocked, Downconverter 2 Synthesizer Unlocked, Upconverter Synthesizer Unlocked, DC Supply Fault alarms, and DART FPGA status.

    – **DART Over Drive Fault**—Red indicates that the RF signal received from the BTS/BDA is too strong. Fault threshold is +19 dBm.

    – **DART Under Drive Fault**—DART forward RF input signal below the normal operating limit. Fault threshold is +5 - Fwd Gain - 20

    – **Module Missing Fault**—One of the Host pluggable modules is missing (DART/SFP).

    – **DART Hardware Mismatch**—Host DART does not support the selected passband. Fault occurs when a Host DART is replaced with another DART of the incorrect type.

- **Optical Status** table—shows the current usage and alarm status of the optical ports on the Host plus the current values of some key operating parameters.

The Host has eight optical ports, but the **Optical Status** table only shows active ports (physically connected to a Remote). Each port in the table (where SFP 1 is column 1, SFP 2 is column 2, and so forth) represents one set of forward and reverse paths between a Host and Remote. Physically, this may have been accomplished with a dual-connector through that port. Each physical port contains an SFP transceiver with two connectors.

The **Optical Status** table only shows the Receive power level from the Remote Unit (REV path). To see the Receive power level in the FWD path (from the Host to the Remote), you must open the **Unit Information > View Status** page for the desired Remote as described in "Viewing the Status of a Remote Unit" on page 156.

- **Optical RX High BER**—High bit error rate (BER) detected by fiber optic receiver. Fault threshold is **0.00001**. Threshold cannot be changed.
- **Optical RX No Light**—No signal detected by optical receiver.
- **Optical Transmitter Fault**—SFP optical transmitter failed.
- **Optical Over Drive**—SFP optical receive input power above specification. The fault threshold cannot be changed, and is
  - **1 dBm** for IR
  - **-9 dBm** for LR.
- **Optical Under Drive**—SFP optical receive input power below specification. The fault threshold cannot be changed, and is
  - **-18 dBm** for IR
  - **-27 dBm** for LR.
- **Module Missing Fault**—One of the Host SFPs is missing.

• **Host Status** table—shows the current overall status of the Host.

- **Host Major Contact Alarm Output Active**—Major Contact Alarm Output active.
- **Host Minor Contact Alarm Output Active**—Minor Contact Alarm Output active.
- **Remote Major Contact Alarm Output Active**—Red indicates NO/NC major alarm contacts are in an alarm position. These connections are typically wired to a local alarm alert system. This status indicator is red when a major alarm is present on any Remote connected to the Host.
- **Remote Minor Contact Alarm Output Active**—Yellow indicates that NO/NC minor alarm contacts are in an alarm position. These connections are typically wired to a local alarm alert system. This status indicator is yellow when a minor alarm is present on any Remote connected to Host.
- **SeRF Fault**—state of the SeRF. Red indicates that either the SeRF clock source is unacceptable or the SeRF card FPGA is not programmed.
- **Fan Fault**—state of the Host chassis fan. Red indicates that the Host chassis fan is spinning too slowly.
- **Temperature High**—Red indicates that the current temperature of the Host interior is above its operating limits. Fault threshold is **62° C**.
- **Temperature Low**—Yellow indicates that the current temperature of the Host interior is below its operating limits. Fault threshold is **0° C**.

• **Temperature**—Gives the current temperature of the Host chassis interior in degrees Centigrade, as detected by the Host.

VIEWING THE STATUS OF A REMOTE UNIT

For further information on the faults listed in the View Status page for Remote Units, see "Troubleshooting Alarms" on page 185.

1   In the System Tree, click on the icon of the PRU/URU for which you want to view its status.

2   In the Unit Menu bar, click **Unit Information** > **View Status**.

The **Unit Information > View Status** page provides the following information for the selected Remote Unit. The background of each table cell is color coded to the level of the alarm; see "Viewing Parameters and Alarms" on page 44. For more information on the faults and alarms, see "Troubleshooting Alarms" on page 185.

Module Status Table

The **Module Status** table provides status information for PRU/URU modules where columns 1 through 8 correspond to the slot in which a DART resides (see "RF Module Capabilities and GUI Representation" on page 21).

The following sections describe the different sections within the **Module Status** table.

DART Status Table

The **DART Status** table presents status of the DARTs in a Remote Unit. There can be between 1 and 8 DARTs installed in a Remote Unit. If a DART column has no background color, a DART is not installed in that slot, as shown below.

DART is not installed in slots 2, 4, 5, 6

The **DART Status** table has the following elements.

- **DART Fault**—Summary of DART Downconverter 1 Synthesizer Unlocked, Downconverter 2 Synthesizer Unlocked, Upconverter Synthesizer Unlocked, DC Supply Fault alarms, and DART FPGA status.

- **DART DC Supply Fault**—DART Module DC supply voltages outside specification.

- **DART Hardware Mismatch**—Host DART does not support the selected passband. Fault occurs when a Host DART is replaced with another DART of the incorrect type.

- **DART Temperature High**—DART temperature above operating limit. Threshold is 85°C.

- **Delay Out Of Range**—PRU/URU delay settings outside the valid range.

- **DART Temperature Low**—DART temperature below operating limit. Threshold is -40°C.

- **Module Missing Fault**—DART module is missing.

LNA Status Table

LNA->	1	2	3	4	5	6	7	8
LNA Power Fault	🟩							
Module Missing Fault	🟩							

The **LNA Status** table presents status information for the Low Noise Amplifiers in a Remote Unit. There can be between 1 and 8 LNAs installed in a Prism Remote Unit.

- **LNA Power Fault**—PRU/URU Low Noise Amplifier Power fault.

- **Module Missing Fault**—LNA module is missing.

LPA Status Table

The **LPA Status** table presents status information for the Linear Power Amplifiers in a Remote Unit. There can be between 1 and 4 LPAs installed in a Prism Remote Unit.

LPA->	1	2	3	4
LPA Disabled	🟩			
LPA VSWR Fault	🟩			
LPA DC Fault	🟩			
LPA Loop Fault	🟩			
LPA Over Power	🟩			
LPA Low Power Fault	🟩			
LPA Missing	🟩			
LPA Over Temperature	🟩			

- L**PA Disabled**—PRU/URU Linear Power Amplifier (LPA) disabled due to an internally detected problem. (VSWR, DC, Loop Fault, Low Power, or Temperature High alarm).

- **LPA VSWR Fault**—PRU/URU Linear Power Amplifier (LPA) VSWR fault.

- **LPA DC Fault**—PRU/URU Linear Power Amplifier (LPA) DC fault.

- **LPA Loop Fault**—PRU/URU Linear Power Amplifier (LPA) Loop fault.

- **LPA Over Power**—PRU/URU Linear Power Amplifier (LPA) output power level above operating limit.

- **LPA Low Power Fault**—Internal Linear Power Amplifier (LPA) Low Power fault. Gain of one or more internal amplifiers outside of specification).

- **LPA Missing**—LPA module is missing.

- **LPA Over Temperature**—PRU/URU LPA above operating limit.

PD Status Table

The **PD Status** table presents status information for the Power Detector in a Remote Unit. There can be between 1 and 4 PDs installed in a Prism Remote Unit.

PD->	1	2	3	4
System VSWR Fault				
RF Power Low				
Module Missing Fault				
Duplexer Mismatch				

- **System VSWR Fault**—PRU/URU VSWR measurement above specification.
- **RF Power Low**—PRU/URU RF Output Power below minimum threshold.
- **Module Missing Fault**—Power Detector module is missing.
- **Duplexer Mismatch**—Configured frequency range not supported by Duplexer.

Optical Status Table

The **Optical Status** table provides status information for SFPs installed in a Remote Unit (PRU/URU).There can be between 1 and 8 SFPs installed in a Remote Unit. If a column has no background color, an SFP is not installed in that slot.

Optical Status

SFP->	1	2	3	4	5	6	7	8
Optical RX High BER								
Optical RX No Light								
Optical Transmitter Fault								
Optical Over Drive								
Optical Under Drive								
Module Missing Fault	M							

- **Optical RX High BER**—High bit error rate (BER) detected by fiber optic receiver. Threshold is 0.00001.
- **Optical RX No Light**—No signal detected by optical receiver.
- **Optical Transmitter Fault**—SFP optical transmitter failed.
- **Optical Over Drive**—SFP optical receive input power above specification. Thresholds are as follows:
  - **1 dBm** for IR
  - **-9 dBm** for LR.
- **Optical Under Drive**—SFP optical receive input power below specification. Thresholds are as follows:
  - **-18 dBm** for IR
  - **-27 dBm** for LR.
- **Module Missing Fault**—SFP module is missing.

Remote Status Table

The **Remote Status** table provides general status information for a Remote Unit (PRU/URU).

<table>
<tr><td colspan="2">Remote Status</td></tr>
<tr><td>Host Lost</td><td></td></tr>
<tr><td>AC Power Supply Fault</td><td></td></tr>
<tr><td>Temperature High</td><td></td></tr>
<tr><td>Temperature Low</td><td></td></tr>
<tr><td>Contact Alarm Input 1 Active</td><td></td></tr>
<tr><td>Fan Under Speed</td><td>M</td></tr>
<tr><td>Contact Alarm Input 2 Active</td><td></td></tr>
<tr><td>Fan Over Speed</td><td></td></tr>
<tr><td>Door Open</td><td></td></tr>
<tr><td>SeRF Fault</td><td></td></tr>
<tr><td>Software Version Mismatch Fault</td><td></td></tr>
</table>

- **Host Lost**—Host is not communicating with PRU/URU.
- **AC Power Supply Fault**—Power supply is in a failed state, or the AC power is below the minimum required voltage.
- **Temperature High**—Temperature above operating limit. Threshold is 95°C.
- **Temperature Low**—Temperature below operating limit. Threshold is Minus 40°C.
- **Contact Alarm Input 1 Active**—Host Contact Alarm Input #1 active.
- **Fan Under Speed**—Fans operating below expected RPM.
- **Contact Alarm Input 2 Active**—Host Contact Alarm Input #2 active.
- **Fan Over Speed**—Fans operating above expected RPM.
- **Door Open**—Door open on PRU.
- **SeRF Fault**—Summary of SeRF Synthesizer Unlocked alarm and SeRF FPGA status.
- **Software Version Mismatch Fault**—Software version on the Host and Remote Units do not match.

Remote Unit Capacity and Temperature

The **Unit Information > View Status** page for Remote Units also provides unit capacity and temperature information for the selected Remote Unit (PRU/URU).

Capacity	1
Temperature	68.0C

- **Capacity**—the number of RF groups available to the Remote Unit.
- **Temperature**—The internal Temperature of the selected unit.

CLEARING DART CONFIGURATIONS

This procedure does the following:

- resets the gain
- resets the DART name
- clears all links
- clears the passband
- clears all associated alarms

1 In the System Tree, click on an icon for a Host or Remote Unit.

2 In the Unit Menu bar, click **Unit Configuration** > **Clear DART Configuration**, to open the **Clear DART Configuration** page.

3 In the **Select** column, select the DART(s) for which you want to clear configuration.

4 Click **Clear Configuration**.

5 In the confirmation window, click **OK**.

If the DART has been removed from the Host or PRU/URU chassis, then the entire DART entry disappears. If the DART is still present in the Host or PRU/URU chassis, then the **DART Name** and **Passband** is reset to default.

Unit Information	Unit Configuration	Unit Upgrades

Unit Configuration > Clear DART Configuration [system3 1]

Information: DART # 2 configuration cleared.

Select ▾	DART Number	DART Name	Band Type	Passband	Alarm Status
☐	1	pcs__	1900 PCS DL SuperDART	PCS_1930-1995	Clear
☐	5	cell_	850 Classic	Cellular A2ABA1B1	Clear
☐	6	UNKNOWN_DARTNAME	700 UpperC SGL SuperDART	NA	Clear
☐	8	UNKNOWN_DARTNAME	700 LowerABC SGL SuperDART	NA	Clear

[Clear Configuration] [Refresh]

SET THE CAPACITY FOR A NEW REMOTE UNIT RSI BOARD

The **Capacity** setting in the **Edit Properties** page pertains to the PRU/URU Remote SeRF Interface (RSI) board and the number of RF groups available to the Remote Unit. This parameter is set during manufacturing and should be changed only when the RSI board has been replaced.

Using the EMS GUI to Change the Remote Unit Capacity

The **Capacity** setting can be changed by logging onto the EMS through the Remote Craft port.

1 Open the unit and connect your laptop to the Craft port on the SeRF.

2 Login to the EMS, using the following parameters:

- IP address is `192.168.0.1`
- User Name is `operator`
- Password is `operator`

3 In the System Tree, click the icon of the PRU/URU whose properties you want to change.

4 In the Unit Menu bar, click **Unit Configuration** > **Edit Properties**, to open the **Unit Configuration > Edit Properties** page for the selected PRU.

5 In the **Capacity** list, set the **Capacity** of the new RSI board:

- For all RSI boards installed in a URH, **Capacity** should always be set to **3**.

- For an RSI board installed in a PRU, **Capacity** can be **1**, **2**, **3**, or **4** and indicates the number of RF Modules installed in the PRU.

6 Click **Apply**.

Using Telnet or ssh to Change the Remote Unit Capacity

Alternately, the capacity can be changed using Telnet or ssh.

1 Access the Edit Unit Properties page to determine the IP address for the Host and Remote Unit(s). In the System Menu bar, click **System Configuration > Edit Unit Properties**. Each row in the **Edit Unit Properties** table correspond to the unit identified in the **Unit Id** column. Use the **IP Address** column to determine the IP address for each unit.

2 Login to the Host using **telnet** or **ssh**.

3 From the Host, login to the Remote Unit using the following command,where **N** is the Remote Unit ID (**1** - **8**): **sshremote N**

4 Once logged into the Remote Unit, execute the following command, where **x** is the capacity (1-4): **/usr/local/fwu/bin/EEPROMWriteForCapacity.sh X**

REBOOTING A UNIT

CAUTION! The system configuration is stored on the Host. Rebooting the Host therefore results in a loss of RF for the Host and connected Remote Units until the Host comes back up. Depending on the system configuration, it can take 5 to 20 minutes before management communication is restored.

CAUTION! Host configuration persists across a Reboot. However, the current EMS session will close and you will need to log back in to the EMS after the Host reboot has completed.

CAUTION! Rebooting a Remote Unit causes Loss of Service and should not be used unless other troubleshooting processes have been followed and did not fix the issue being experienced at the PRU/URU.

1 In the System Tree, click on the icon of the unit that you want to reboot.

2 In the Unit Menu bar, click **Unit Configuration** > **Reboot**, to open the **Unit Configuration > Reboot** page.

> Unit Information   Unit Configuration   Unit Upgrades
>
> **Unit Configuration > Reboot [dvt2_host 1-1]**
>
> A Unit Reboot will cause a temporary loss of RF for up to 2 minutes. Do you want to Reboot this unit?
>
> Reboot
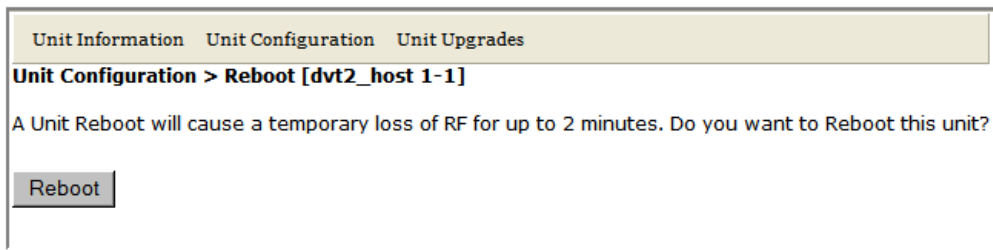
3 Click **Reboot**.

- Once the reboot starts, a process message displays.

> Unit Configuration   Unit Upgrades
>
> **Unit Configuration > Reboot [system3 1-1.1]**
>
> Unit is rebooting. Please wait one minute before trying to perform any actions on this unit.
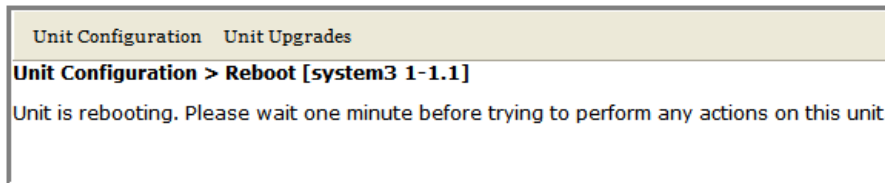
- After the reboot has completed, a **Unit has been rebooted** message displays.

> Unit Information   Unit Configuration   Unit Upgrades
>
> **Unit Configuration > Reboot [Building4 1-1]**
>
> Information: Unit has been rebooted.
> A Unit Reboot will cause a temporary loss of RF for up to 2 minutes. Do you want to Reboot this unit?
>
> Reboot
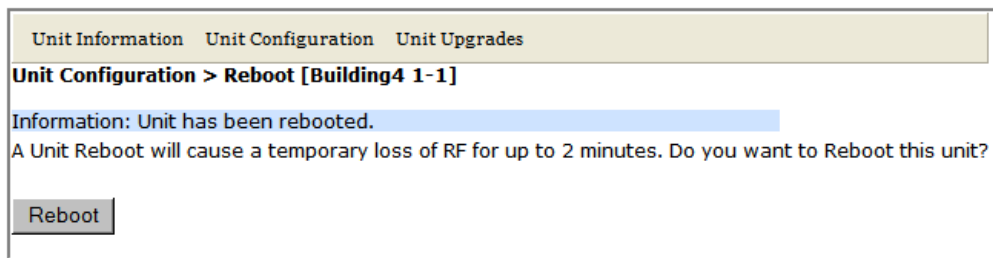
- After the Host reboots, the EMS login window opens.

RESETTING AN LPA

CAUTION!   Once an LPA Reset is started, Loss of Service occurs. It takes approximately 10 to 20 seconds before the LPA signal recovers. The GUI RF power reading will take longer depending on the number of Remotes equipped—for a fully loaded Prism system with 8 Remotes the power reading could take several minutes to update.

NOTE: Only a user logged in under the admin or a Network Manager account can change Prism system settings through the EMS.

You use the **LPA Reset** button to bring an LPA back into service (restart) that stopped because of a major LPA alarm. In a dual-LPA system, resetting the LPA applies to both LPAs at the same time.

1   To access the **Configure Remote Forward Gain** page, in the System Menu bar, click **System Configuration** > **Configure Remote Forward Gain**.

2   In the **Remote Id** list, select the Remote Unit whose LPA you need to reset.

3   In the **Remote DART** list, select the DART whose LPA you need to reset.

4   Click the **LPA Reset** button.

5   In the LPA Reset caution dialog, click **OK**.

Intentionally Blank Page

ALARMS

This section describes how to manage and understand the alarms that are reported by the EMS. This section also provides corresponding Trap names.

VIEW CURRENT ALARMS

To access the **View Current Alarms** page, in the System Menu bar, click **Alarms** > View **Current Alarms**. (For information on the alarm color codes, see "Alarm Color Codes" on page 44.)

Severity	Ack'd	Alarm Code	Alarm Name	▲ Timestamp	Unit Id	Unit Type	Unit Name	Module	Module Name	RF Band	Extended Info
Minor	☐	AC75	Door Open	2011/02/12 19:14:19	SciencesBldg1 1-1	PRU	LawrenceLab	SeRF	NA	NA	Click
Minor	☐	AC31	DART Under Drive	2011/02/12 14:17:41	SciencesBldg1 1	Host	SciencesBldg1	DART 2	ASTRNY1_Floor4	AWS ABC	Click
Major	☐	AC114	RF Power Low	2011/02/11 15:01:45	SciencesBldg1 1-1	PRU	UNKNOWN_REMOTENAME	Power Detector 2	NA	NA	Click
Major	☐	AC114	RF Power Low	2011/02/11 15:01:45	SciencesBldg1 1-1	PRU	UNKNOWN_REMOTENAME	Power Detector 4	NA	NA	Click
Major	☐	AC77	Fan Under Speed	2011/02/11 15:01:43	SciencesBldg1 1-1	PRU	UNKNOWN_REMOTENAME	SeRF	NA	NA	Click

Clear Alarms   Refresh

The **View Current Alarms** table provides the following information:

- **Severity**—whether the alarm is classified as Major or Minor.
- **Ack'd**—whether the alarm has been acknowledged, as indicated by a checkmark.
- **Alarm Code**—system-assigned alarm code.
- **Alarm Name**—descriptive name of alarm.
- **Timestamp**—date and time when the alarm occurred (**YYYY:MM:DD:HH:MM:SS**)
- **Unit Id**—identifies the unit within the system that raised the alarm; see "Unit Identification" on page 43.
- **Unit Type**—what the unit is, such as Host or Remote
- **Unit Name**—name assigned to the unit
- **Module**—type of module that is experiencing the alarm (SeRF, DART, LPA, LNA, Power Detector, SFP)
- **Module Name**—user-assigned name for the module.
- **RF Band**—type of passband provided by the DART.

- **Extended Info**—link that once clicked opens another web page, which provides further information on the alarm, including troubleshooting information, as shown in the following graphic.
  - **Description**—text description of alarm
  - **Remedy**—what you can do to correct the alarm state
  - **Threshold**—value that once surpassed generates an alarm
  - **Notes**—user-defined notes, if any, for the unit.

☑ Severity	Alarm Code	Alarm Name	Timestamp	Unit Id	Unit Type	Unit Name	Module	Module Name	RF Band
Major	AC114	RF Power Low	2011/02/11 15:01:45	SciencesBldg1 1-1	PRU	UNKNOWN_REMOTENAME	Power Detector 2	NA	NA

Description	PRU/URU RF Output Power below minimum threshold.
Remedy	Check for Host DART underdrive alarm or low RF input from BTS. Check the Host and Remote forward gains are set correctly.
Threshold Value	20 dBm
Notes	Centennial and Grizzly Peak

RF Module / Band D

RF Module/ Band C

RF Module/ Band B

RF Module/ Band A

SeRF & Power Supplies

Copyright © 2011 ADC Telecommunications, Inc. All Rights Reserved.

CLEAR CURRENT ALARMS

1   To access the **View Current Alarms** page, in the System Menu bar, click **Alarms** > **View Current Alarms**.

2   In the **View Current Alarms** page, click **Clear Alarms**.

Severity	Ack'd	Alarm Code	Alarm Name	⬆ Timestamp	Unit Id	Unit Type	Unit Name	Module	Module Name	RF Band	Extended Info
Minor	☐	AC75	Door Open	2011/02/12 19:14:19	SciencesBldg1 1-1	PRU	LawrenceLab	SeRF	NA	NA	Click
Minor	☐	AC31	DART Under Drive	2011/02/12 14:17:41	SciencesBldg1 1	Host	SciencesBldg1	DART 2	ASTRNY1_Floor4	AWS ABC	Click
Major	☐	AC114	RF Power Low	2011/02/11 15:01:45	SciencesBldg1 1-1	PRU	UNKNOWN_REMOTENAME	Power Detector 2	NA	NA	Click
Major	☐	AC114	RF Power Low	2011/02/11 15:01:45	SciencesBldg1 1-1	PRU	UNKNOWN_REMOTENAME	Power Detector 4	NA	NA	Click
Major	☐	AC77	Fan Under Speed	2011/02/11 15:01:43	SciencesBldg1 1-1	PRU	UNKNOWN_REMOTENAME	SeRF	NA	NA	Click

Alarms > View Current Alarms

Clear Alarms   Refresh

3   In the confirmation window, click **OK**.

Microsoft Internet Explorer

Do you want to clear the active alarms (all persistent alarms will be rediscovered)?

OK   Cancel

All current alarms, with the exception of persistent alarms, are cleared from the **View Current Alarms** table.

VIEW ALARM HISTORY

To access the **View Alarm History** page, in the System Menu bar, click **Alarms** > **View Alarm History**. (For information on the alarm color codes, see "Alarm Color Codes" on page 44.)

The **View Alarm History** table provides the following information:

- **Severity**—whether the alarm is classified as Major or Minor.

- **Ack'd**—whether the alarm has been acknowledged, as indicated by a checkmark.

- **Alarm Code**—system-assigned alarm code.

- **Alarm Name**—descriptive name of alarm.

- **Timestamp**—date and time when the alarm occurred (**YYYY:MM:DD:HH:MM:SS**)

- **Unit Id**—identifies the unit within the system that raised the alarm; see "Unit Identification" on page 43.

- **Unit Type**—what the unit is, such as Host or Remote

- **Unit Name**—name assigned to the unit

- **Module**—type of module that is experiencing the alarm (SeRF, DART, LPA, LNA, Power Detector, SFP)

- **Module Name**—user-assigned name for the module.

- **RF Band**—type of passband provided by the DART.

- **First**, **Previous**, **Last** buttons—if the **View Alarm History** table is longer than what can fit on a single web page, **First**, **Previous**, **Last** buttons are included:
    - **First**—jumps the display to the first page of alarms
    - **Previous**—jumps the display to the page of alarms that you viewed immediately prior to the current page
    - **Last**—jumps the display to the last page of alarms

- **Clear History** button—see "Clearing Alarm History" on page 172.

CLEARING ALARM HISTORY

1 To access the **View Alarm History** page, in the System Menu bar, click **Alarms** > **View Alarm History**.

2 Click **Clear History**.

3 In the confirmation window, click **OK**.
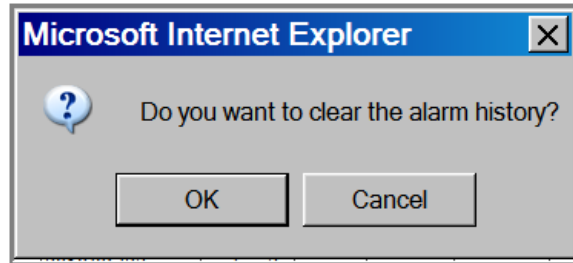
The **View Alarm History** page is cleared.

FILTERING THE ALARM HISTORY

The **View Alarm History** page allows you to filter, or select, which alarm histories you want to page.

1 To access the **View Alarm History** page, in the System Menu bar, click **Alarms** > **View Alarm History**.

2 Do the following in the **Filter** panel:

   a In the **View** list, select how you want to filter the alarms:

   • **None**—all alarms display

   • **Unit Name**—filter by the user-assigned name of a unit

   • **Host Number**—filter by the system-assigned number for the Host

   • **Remote Number**—filter by the system-assigned number for a Remote

   • **Event Name**—filter by an event (alarm or incident) name.

b In the **contains** box, enter the criteria by which you want to filter the alarm history list.

c Click **Filter**.

Alarms > View History Alarms

Filter

View [Event Name ▼] contains [DART] [Filter]

Download All   First|Previous|Next|Last

Severity	Ack'd	Alarm Code	Alarm Name ▲	Timestamp	Unit Id	Unit Type	Unit Name	Module	Module Name	RF Band	Extended Info
Information	☐	IC14	User login/logout	2010/06/23 20:07:23	dvt2_host 1	Host	dvt2_host	Undefined	--	--	Click
Information	☐	IC14	User login/logout	2010/06/23 18:41:06	dvt2_host 1	Host	dvt2_host	Undefined	--	--	Click
Information	☐	IC14	User login/logout	2010/06/23 18:38:51	dvt2_host 1	Host	dvt2_host	Undefined	--	--	Click
Information	☐	IC14	User login/logout	2010/06/23 17:00:26	dvt2_host 1	Host	dvt2_host	Undefined	--	--	Click
Clear	☐	AC31	DART Under Drive	2010/06/23 15:49:23	dvt2_host 1	Host	dvt2_host	DART 1	host1900_1	PCS_1930-1995	Click
Clear	☐	AC31	DART Under Drive	2010/06/23 15:31:31	dvt2_host 1	Host	dvt2_host	DART 5	host850_5	Cellular A2ABA1B1	Click
Minor	☐	AC31	DART Under Drive	2010/06/23 15:29:52	dvt2_host 1	Host	dvt2_host	DART 5	host850_5	Cellular A2ABA1B1	Click
Information	☐	IC6	Host DART fwd gain	2010/06/23 15:14:31	dvt2_host 1	Host	dvt2_host	DART 1	--	--	Click
Information	☐	IC6	Host DART fwd gain	2010/06/23 15:13:59	dvt2_host 1	Host	dvt2_host	DART 1	--	--	Click
Information	☐	IC6	Host DART fwd gain	2010/06/23 15:13:35	dvt2_host 1	Host	dvt2_host	DART 1	--	--	Click

[Clear History] [Refresh]

The **View Alarm History** page refreshes, and now lists only those alarms that meet the specified filter criteria. In this example, only those events with the word "DART" in them display.

Alarms > View History Alarms

Filter

View [Event Name ▼] contains [DART] [Filter]

Download All   First|Previous|Next|Last

Severity	Ack'd	Alarm Code	Alarm Name ▲	Timestamp	Unit Id	Unit Type	Unit Name	Module	Module Name	RF Band	Extended Info
Clear	☐	AC31	DART Under Drive	2010/06/23 15:49:23	dvt2_host 1	Host	dvt2_host	DART 1	host1900_1	PCS_1930-1995	Click
Clear	☐	AC31	DART Under Drive	2010/06/23 15:31:31	dvt2_host 1	Host	dvt2_host	DART 5	host850_5	Cellular A2ABA1B1	Click
Minor	☐	AC31	DART Under Drive	2010/06/23 15:29:52	dvt2_host 1	Host	dvt2_host	DART 5	host850_5	Cellular A2ABA1B1	Click
Information	☐	IC6	Host DART fwd gain	2010/06/23 15:29:47	dvt2_host 1	Host	dvt2_host	DART 5	--	--	Click
Information	☐	IC6	Host DART fwd gain	2010/06/23 15:27:35	dvt2_host 1	Host	dvt2_host	DART 5	--	--	Click
Information	☐	IC6	Host DART fwd gain	2010/06/23 15:27:09	dvt2_host 1	Host	dvt2_host	DART 5	--	--	Click
Clear	☐	AC31	DART Under Drive	2010/06/23 15:26:16	dvt2_host 1	Host	dvt2_host	DART 5	host850_5	Cellular A2ABA1B1	Click
Minor	☐	AC31	DART Under Drive	2010/06/23 15:26:06	dvt2_host 1	Host	dvt2_host	DART 1	host1900_1	PCS_1930-1995	Click
							dvt2_host	DART 1	--	--	Click

3 To remove the filter:

   a In the **View** list, select **None**.

   b Delete any text from the **contains** box.

   c Click **Filter**.

MANAGE ALARMS

To access the **Manage Alarms** page, in the System Menu bar, click **Alarms** > **Manage Alarms**.

- For an example of a **Manage Alarms** page for a Host Unit, see Figure 23 on page 175 and Figure 24 on page 176.

- For an example of a **Manage Alarms** page for a Remote Unit, see Figure 25 on page 177 and Figure 26 on page 178.

The **Manage Alarms** page has the following elements:

- **Select** menu—has the following implementations:
  - **Global**—displays alarms for the Host and all connected Remote Units. Please note, however, that this view does not reflect the current status of alarm enable/disable conditions—it is designed to show you at a glance those alarms that can be managed. To effect a change in the management of an alarm and to see the current state of an alarm, select a specific unit.
  - **Unit name**—each unit in the system is listed by name, which allows you to select for which unit you want to manage alarms.

- **Antenna Disconnect Severity** menu—see "Antenna Disconnect Alarm" on page 181.

- **Unit** field—what type of unit the alarm pertains to:
  - **Host**
  - **Remote**

- **Module** field—which module the alarm pertains to:
  - **DART**—can be up to eight DARTs listed
  - **LNA**—can be up to two LNAs listed
  - **Power Detector**
  - **SFP**—can be up to eight SFPs listed
  - **SeRF**

- **Alarm Name** field—identifies the alarm by name; see Table 23 on page 178.

NOTE: **For definitions of the alarms listed above, see** "Troubleshooting Alarms" on page 185**.**

- **Enabled** selection box—select to enable alarm reporting for the corresponding alarm.

- **Threshold Value** field—value that once surpassed generates the specified alarm; see Table 23 on page 178.

☐ Unit	Module	Alarm Name	Enabled	Threshold Value
Host	SeRF	Temperature High	☑	62 Deg C
Host	SeRF	Temperature Low	☑	0 Deg C
Host	SFP 1	Optical RX High BER	☑	0.00001
Host	SFP 1	Optical RX No Light	☑	--
Host	SFP 1	Optical Over Drive	☑	1 dBm(IR)/-9dBm(LR)
Host	SFP 1	Optical Under Drive	☑	-18 (IR) dBm/-27 dBm (LR)
Host	DART 1	DART DC Supply Fault	☑	--
Host	DART 2	DART DC Supply Fault	☑	--
Host	DART 4	DART DC Supply Fault	☑	--
Host	DART 5	DART DC Supply Fault	☑	--
Host	DART 6	DART DC Supply Fault	☑	--
Host	DART 1	DART Over Drive	☑	+19 dBm
Host	DART 2	DART Over Drive	☑	+19 dBm
Host	DART 4	DART Over Drive	☑	+19 dBm
Host	DART 5	DART Over Drive	☑	+19 dBm
Host	DART 6	DART Over Drive	☑	+19 dBm
Host	DART 1	DART Under Drive	☑	-18 dBm
Host	DART 2	DART Under Drive	☑	-21 dBm
Host	DART 4	DART Under Drive	☑	-18 dBm
Host	DART 5	DART Under Drive	☑	-49 dBm
Host	DART 6	DART Under Drive	☑	-18 dBm
Host	DART 1	DART ALC Limiting	☑	19 dBm
Host	DART 2	DART ALC Limiting	☑	16 dBm
Host	DART 4	DART ALC Limiting	☑	19 dBm
Host	DART 5	DART ALC Limiting	☑	-12 dBm
Host	DART 6	DART ALC Limiting	☑	19 dBm

Figure 23. Example of Manage Alarms Page—Host Unit Part 1

Alarms > Manage Alarms

Select SciencesBldg1 1

Unit	Module	Alarm Name	Enabled	Threshold Value
Host	SeRF	Temperature High	☑	62 Deg C
Host	SeRF	Temperature Low	☑	0 Deg C
Host	SFP 1	Optical RX High BER	☑	0.00001
Host	SFP 1	Optical RX No Light	☑	--
Host	SFP 1	Optical Over Drive	☑	1 dBm(IR)/-9dBm(LR)
Host	SFP 1	Optical Under Drive	☑	-18 (IR) dBm/-27 dBm (LR)
Host	DART 1	DART DC Supply Fault	☑	--
Host	DART 2	DART DC Supply Fault	☑	--
Host	DART 4	DART DC Supply Fault	☑	--
Host	DART 5	DART DC Supply Fault	☑	--
Host	DART 6	DART DC Supply Fault	☑	--
Host	DART 1	DART Over Drive	☑	+19 dBm
Host	DART 2	DART Over Drive	☑	+19 dBm
Host	DART 4	DART Over Drive	☑	+19 dBm
Host	DART 5	DART Over Drive	☑	+19 dBm
Host	DART 6	DART Over Drive	☑	+19 dBm
Host	DART 1	DART Under Drive	☑	-18 dBm
Host	DART 2	DART Under Drive	☑	-21 dBm
Host	DART 4	DART Under Drive	☑	-18 dBm
Host	DART 5	DART Under Drive	☑	-49 dBm
Host	DART 6	DART Under Drive	☑	-18 dBm
Host	DART 1	DART ALC Limiting	☑	19 dBm
Host	DART 2	DART ALC Limiting	☑	16 dBm
Host	DART 4	DART ALC Limiting	☑	19 dBm
Host	DART 5	DART ALC Limiting	☑	-12 dBm
Host	DART 6	DART ALC Limiting	☑	19 dBm

Figure 24. Example of Manage Alarms Page—Host Unit Part 2

Alarms > Manage Alarms

Select 1-SciencesBldg1 1-1 ▼

Unit	Module	Alarm Name	Enabled	Threshold Value
PRU	SeRF	Temperature High	☑	95 Deg C
PRU	SeRF	Temperature Low	☑	Minus 40 Deg C
PRU	SeRF	Door Open	☑	--
PRU	SFP 1	Optical RX High BER	☑	0.00001
PRU	SFP 1	Optical RX No Light	☑	--
PRU	SFP 1	Optical Over Drive	☑	1 dBm(IR)/-9dBm(LR)
PRU	SFP 1	Optical Under Drive	☑	-18 dBm (IR)/ -27 dBm (LR)
PRU	DART 1	DART DC Supply Fault	☑	--
PRU	DART 3	DART DC Supply Fault	☑	--
PRU	DART 7	DART DC Supply Fault	☑	--
PRU	DART 1	DART Temperature High	☑	85 Deg C
PRU	DART 3	DART Temperature High	☑	85 Deg C
PRU	DART 7	DART Temperature High	☑	85 Deg C
PRU	DART 1	DART Temperature Low	☑	minus 40 deg C
PRU	DART 3	DART Temperature Low	☑	minus 40 deg C
PRU	DART 7	DART Temperature Low	☑	minus 40 deg C
PRU	DART 1	Uplink Inactivity Fault	☐	-85.0 dBm
PRU	DART 3	Uplink Inactivity Fault	☐	NA
PRU	DART 7	Uplink Inactivity Fault	☐	-85.0 dBm
PRU	Power Detector 1	System VSWR Fault	☑	3:1
PRU	Power Detector 2	System VSWR Fault	☑	3:1
PRU	Power Detector 4	System VSWR Fault	☑	3:1
PRU	Power Detector 1	RF Power Low	☑	20 dBm
PRU	Power Detector 2	RF Power Low	☑	20 dBm
PRU	Power Detector 4	RF Power Low	☑	20 dBm

Figure 25. Example of Manage Alarms Page—Remote Unit Part 1

Figure 26. Example of Manage Alarms Page—Remote Unit Part 2

Enable and Disable Host and Remote Unit Alarms

The **Manage Alarms** page allows you to enable and disable alarm reporting for the alarms listed in Table 23 on page 178.

Table 23. *Alarms That Can Be Enabled/Disabled*

Unit	Module	Alarm	Alarm Threshold
Remote	RDI	AC Power Supply 1 Fault	
Remote	RDI	AC Power Supply 2 Fault	
Remote	RDI	AC Power Supply 3 Fault	
Remote	RDI	AC Power Supply 4 Fault	
Remote	PRU/URU	AC Power Supply Fault	

Table 23. *Alarms That Can Be Enabled/Disabled (Cont.)*

Unit	Module	Alarm	Alarm Threshold
Host	DART	DART ALC Limiting	+19 - Fwd Gain dBm
Host	DART	DART DC Supply Fault	
Remote	DART	DART DC Supply Fault	
Host	DART	DART Over Drive	+19 dBm
Remote	DART	DART Temperature High	85 Deg C
Remote	DART	DART Temperature Low	minus 40 deg C
Host	DART	DART Under Drive	+5 - Fwd Gain - 20 dBm
Remote	SeRF	Door Open	
Remote	DART	Downconvert Fault	
Remote	DART	DART DC Supply Fault	
Remote	SFP	Excess Connections	
Host	DART	FLM Downconvert Fault	
Remote	DART	FWD Cal Tone Fault	
Remote	SFP	Invalid Device Connection	
Remote	LNA	LNA Power Fault	
Host	SFP	Optical Over Drive	1 dBm(IR)/-9dBm(LR)
Remote	SFP	Optical Over Drive	1 dBm(IR)/-9dBm(LR)
Host	SFP	Optical RX High BER	0.00001
Remote	SFP	Optical RX High BER	0.00001
Host	SFP	Optical RX No Light	
Remote	SFP	Optical RX No Light	
Host	SFP	Optical Under Drive	-18 (IR) dBm/-27 dBm (LR)
Remote	SFP	Optical Under Drive	-18 dBm (IR)/ -27 dBm (LR)
Remote	DART	REV Test Tone Low	
Remote	PD	RF Power Low	0 dBm*
Host	DART	RLM Upconvert Fault	
Host	DART	RLM Upconvert Indeterminate	
Remote	SeRF	Software Version Mismatch Fault	
Remote	PD	System VSWR Fault	3:1
Host	SeRF	Temperature High	62 Deg C
Remote	SeRF	Temperature High	95 Deg C
PRU/URU	SeRF	Temperature High	62 Deg C
Host	SeRF	Temperature Low	0 Deg C
Remote	SeRF	Temperature Low	Minus 40 Deg C
PRU/URU	SeRF	Temperature Low	0 Deg C
Remote	LPA	Under Power	
Remote	DART	Upconvert Fault	
Remote	DART	Upconvert Indeterminate	
Remote	DART	Uplink Inactivity Fault	10 dB above the noise floor.
* You can manually set the threshold for RF Power Low; see "Set RF Power Low Threshold" on page 180			

Do the following to enable/disable alarm reporting:

1 To access the **Manage Alarms** page, in the System Menu bar, click **Alarms** > **Manage Alarms**.

2 In the **Select** list, select the Remote Unit for which you want to change the threshold of the **RF Power Low** alarm.

3 In the **Threshold Value** box for the **RF Power Low** alarm, enter the new threshold, which must be between **0 dB** - **40 dB**.

4 Click **Apply**.

Set RF Power Low Threshold

The following rules apply to setting alarm thresholds:

- Only the threshold for the **RF Power Low** alarm can be changed.

- Only users with Network Manager or Admin privileges can perform this procedure.

- Alarm thresholds cannot be set through SNMP MIBs.

- If you perform a **Reset to Factory Defaults**, the alarm threshold values are reset; you will need to be reconfigure the alarm threshold values, as necessary.

- Alarm threshold values are configured by unit—they cannot be set globally for all units in the system.

Do the following to set the **RF Power Low** alarm threshold:

1 To access the **Manage Alarms** page, in the System Menu bar, click **Alarms** > **Manage Alarms**.

2 In the **Select** list, select the Remote Unit for which you want to change the threshold of the **RF Power Low** alarm.

3 In the **Threshold Value** box for the **RF Power Low** alarm, enter the new threshold, which must be between **0 dB** - **40 dB**.

4 Click **Apply**.

Antenna Disconnect Alarm

In the **Manage Alarms** page, there is an **Antenna Disconnect Severity** menu, which pertains only to Remote Access Units (RAUs) in an InterReach Spectrum system. This feature is therefore not applicable to a FlexWave Prism system and should not be changed from its default setting.

MANAGE CONTACT ALARMS

1 To access the **Manage Contact Alarms** page, in the System Menu bar, click **Alarms** > **Manage Contact Alarms**.

Alarms > Manage Contact Alarms

Select 1-SciencesBldg1 1-1 ▾

▾	Unit Name	Contact Alarm	Severity	Mode	Name	Enabled
	1-SciencesBldg1 1-1	SENSE1	Minor ▾	Normally Open ▾		☑
	1-SciencesBldg1 1-1	SENSE2	Minor ▾	Normally Open ▾		☑

Apply   Refresh

2 In the **Select** menu, select for which unit contact alarms are to be configured.

The **Manage Contact Alarms** page has the following Read-Only elements:

- **Unit Name**—name assigned to the unit
- **Contact Alarm**—name assigned to the contact alarm

3 In the **Severity** list, set the severity level of the contact alarm:

- **Minor** (default)
- **Major**

4 In the **Mode** list, set the mode for the contact alarm:

- **Normally Open** (default)
- **Normally Closed**

5 In the **Name** box, enter a name for this alarm.

- Enter between 1 and 255 alphanumeric characters. Spaces and Underscores are allowed, except they cannot be used as the first character.
- If you do not want to name the alarm, leave the **Name** box empty.

6 In the **Enabled** selection box for the alarm that you want to manage, do one of the following:

- Select the **Enabled** checkbox to enable alarm reporting for this alarm type.
- Remove (deselect) the checkmark from the **Enabled** checkbox to disable alarm reporting for this alarm type.

7 Click **Apply**.

ACKNOWLEDGE ALL ALARMS

1 To access the **Acknowledge All Alarms** page, in the System Menu bar, click **Alarms** > **Acknowledge All Alarms**.

> **Alarms > Acknowledge All Alarms**
>
> Do you want to acknowledge all alarms?
>
> [Acknowledge All]
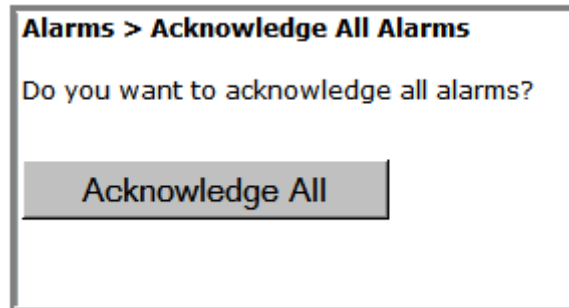
2 Click **Acknowledge All**.

3 In the confirmation window, click **OK**.

> **Microsoft Internet Explorer** ✕
>
> ❓ Do you want to acknowledge all alarms?
>
> [OK] [Cancel]
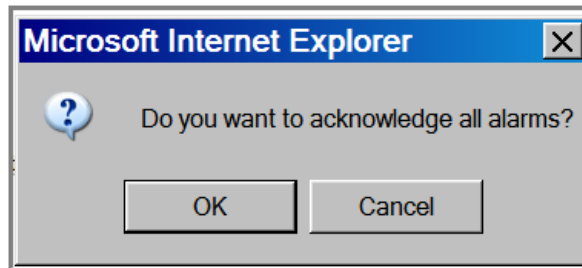
An **All alarms have been acknowledged** message displays.

> **Alarms > Acknowledge All Alarms**
>
> Information: All alarms have been acknowledged.
> Do you want to acknowledge all alarms?
>
> [Acknowledge All]
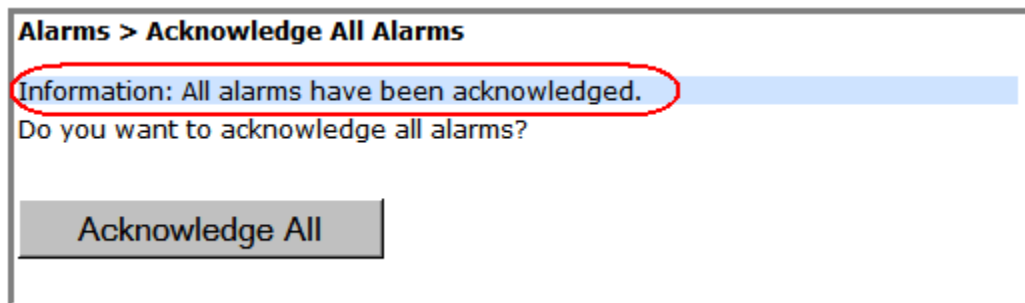
CLEAR ALL DISCONNECT ALARMS

NOTE: Clear All Disconnects is not applicable to the Host—it is applicable only to PRUs.

CAUTION! This procedure removes all information related to the disconnected units from the configuration database.

1 To access the **Clear All Disconnects** page, in the System Menu bar, click **Alarms** > **Clear All Disconnects**.

> **Alarms > Clear All Disconnects**
>
> Do you want to clear all Disconnect alarms?
>
> [Clear All Disconnects]
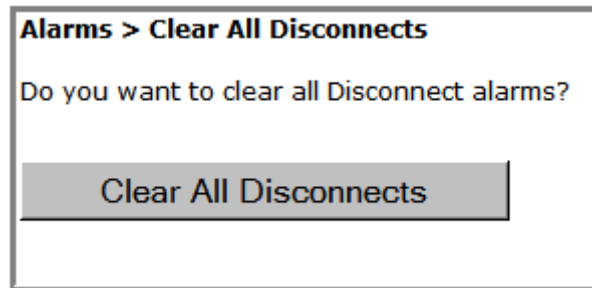
2 Click **Clear All Disconnects**.

After approximately one minute, the System Tree updates by removing the disconnect overlay from the unit icon(s). (For an example of the disconnect overlay, see Table 11 on page 42.)

> **Alarms > Clear All Disconnects**
>
> Information: All disconnect alarms have been cleared.
> Do you want to clear all Disconnect alarms?
>
> [Clear All Disconnects]
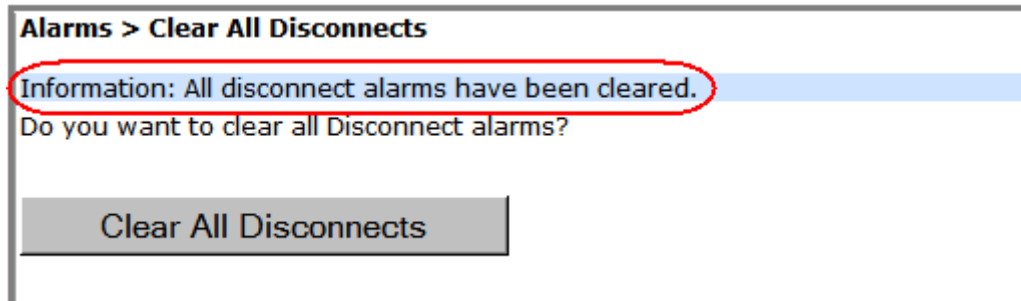
TROUBLESHOOTING ALARMS

This section lists and defines alarms that the FlexWave Prism EMS reports, and provides remedies for those alarms. The MIB Trap name for each alarm is also listed.

Major Alarms—Host Unit

Alarm:	**Remote Lost**
Trap:	`fwuHstSERFRmtLostFault`
Alarm Code:	AC1
Definition:	Remote Unit (PRU/URU) not communicating with Host.
Remedy:	Check that the PRU/URU has power and that the power switch is on. Check that at least one Host SFP is connected to this PRU/URU and has acceptable RX power.

Major Alarms—Host Unit DARTs

Alarm:	**DART DC Supply Fault**
Trap:	`fwuHstDARTDCSupplyFault`
Alarm Code:	AC28
Definition:	DART card DC supply voltages outside specification.
Remedy:	Check whether the Host supply voltage is in the range of 21-60 VDC. If the voltage is correct and the alarm persists for 5 minutes (may be transient on startup), replace the DART.

Alarm:	**DART Downconverter 1 Synthesizer Unlocked**
Trap:	`fwuHstDARTDwnCon1SynLockFault`
Alarm Code:	AC25
Definition:	DART downconverter 1 synthesizer unlocked.
Remedy:	The Downconverter 1 Synthesizer Unlocked alarm can occur during Host reboots and DART hotswaps. If the alarm persists after 5 minutes, replace the DART.

Alarm:	**DART Downconverter 2 Synthesizer Unlocked**
Trap:	`fwuHstDARTDwnCon2SynLockFault`
Alarm Code:	AC26
Definition:	DART downconverter 2 synthesizer unlocked.
Remedy:	The Downconverter 2 Synthesizer Unlocked alarm can occur during Host reboots and DART hotswaps. If the alarm persists after 5 minutes, replace the DART.

Alarm: **DART Fault**

Trap: `fwuHstDARTFault`

Alarm Code: AC29

Definition: Summary of DART Downconverter 1 Synthesizer Unlocked, Downconverter 2 Synthesizer Unlocked, Upconverter Synthesizer Unlocked, DC Supply Fault alarms, and DART FPGA status.

Remedy: Inspect alarms (**Alarms > View Current Alarms**) for upconverter/downconverter/DC supply alarms on the same Host DART and follow the remedies for those alarms. If none of these alarms are found, unplug and replug the DART in the Host. If the alarm persists, replace the DART.

Alarm: **DART Hardware Mismatch**

Trap: `fwuHstDARTHardwareMismatchFault`

Alarm Code: AC32

Definition: Host DART does not support the selected passband. Fault occurs when a Host DART is replaced with another DART of the incorrect type.

Remedy: Install a DART that supports the selected passband. If the Host DART position is to be changed to a different frequency band, remove and clear the DART configuration (**Unit Configuration > Clear DART Configuration**), install the new DART, set the passband, and establish the new link (**System Configuration > Configure DART Links**).

Alarm: **DART Over Drive**

Trap: `fwuHstDARTOverDriveFault`

Alarm Code: AC30

Definition: DART forward RF input too high.

Threshold: +19 dBm

Remedy: Reduce the Host DART forward RF input level.

Alarm: **DART Upconverter Synthesizer Unlocked**

Trap: `fwuHstDARTUpConSynLockFault`

Alarm Code: AC27

Definition: DART upconverter synthesizer unlocked.

Remedy: The DART Upconverter Synthesizer Unlocked alarm can occur during Host reboots and DART hotswaps. If the alarm persists after 5 minutes, replace the DART.

Alarm: **FLM Downconverter Fault**

Trap: `fwuHstBTSFLMFailFault`

Alarm Code: AC47

Definition: Forward Link Monitor (FLM) fault active.

Remedy: If alarm persists, then replace the DART.

Alarm: **Module Missing Fault**

Trap: `fwuHstModuleMissingFault`

Alarm Code: AC2

Definition: One of the Host pluggable modules is missing (DART/SFP).

Remedy: Either replace Host module or clear DART configuration (**Unit Configuration > Clear DART Configuration**).

Alarm: **RLM Upconvert Fault**

Trap: `fwuHstRLMUpconvertFailureFault`

Alarm Code: AC48

Definition: Reverse Link Monitor (RLM) fault active.

Remedy: Running System Test (**System Configuration > Perform System Test**) with un-terminated Host DARTs may cause a false **RLM Upconvert Fault**. Ensure that all Host DARTs are terminated before running System Test. If alarm persists, then replace the DART.

Major Alarms—Host SeRF Modules

Alarm: **Fan Fault**

Trap: `fwuHstSysCardFanFault`

Alarm Code: AC6

Definition: Fan not functioning.

Remedy: Verify intake and exhaust vents are clear of obstructions and/or debris. If alarm persists, replace Fan Module.

Alarm: **SeRF Fault**

Trap: `fwuHstSERFFault`

Alarm Code: AC10

Definition: Summary of SeRF Synthesizer Unlocked alarm and SeRF FPGA status.

Remedy: Check for related Host SeRF alarms (**Alarms > View Current Alarms**). If no SeRF alarms exist, FPGA is faulty; replace Host SeRF Module.

Alarm: **SeRF Synthesizer Unlocked**

Trap: `fwuHstSERFSynthAlarmFault`

Alarm Code: AC9

Definition: SeRF synthesizer unlocked.

Remedy: Check Host reference clock settings (**Unit Configuration > Edit Properties**). Reseat the System Module. If reference clock source is external, verify 10 MHz clock source and connection. If reference clock source is internal and the alarms persists, replace the Host System Module.

Alarm: **Temperature High**

Trap: `fwuHstOverTempFault`

Alarm Code: AC4

Definition: Temperature above operating limit.

Threshold: 62°C

Remedy: Check for Host Fan Fault alarm (**Alarms > View Current Alarms**). Verify that ambient temperature is less than 50°C. Verify Host air intake and exhaust vents are clear of debris.

Major Alarms—Host Unit SFPs

Alarm: **Optical Over Drive**

Trap: `fwuHstSERFOptOverDriveFault`

Alarm Code: AC16

Definition: SFP optical receive input power above specification.

Threshold: Threshold for IR is 1 dBm, and for LR is -9 dBm

Remedy: Reduce the optical receive level by adding optical attenuation. Replace optical attenuator if faulty.

Alarm: **Optical RX No Light**

Trap: `fwuHstSERFOptRxNoLightFault`

Alarm Code: AC14

Definition: No signal detected by optical receiver.

Remedy: Check for broken fiber optic cable; replace if found. Check for disconnected fiber optic cable; reconnect cable if necessary. Check that the PRU/URU has power.

Alarm: **Optical Transmitter Fault**

Trap: `fwuHstSERFOptLaserFault`

Alarm Code: AC15

Definition: SFP optical transmitter failed.

Remedy: Replace Host SFP.

Major Alarms—Remote Units

The following alarms apply to both the Prism Remote Unit (PRU) and the URH Remote Unit (URU).

Alarm:	**Module Missing Fault**
Trap:	`fwuRmtModuleMissingFault`
Alarm Code:	AC68
Definition:	A pluggable module is missing from a Remote Unit, and can be any of the following: DART, SFP, LNA, LPA, or PD.
Remedy:	Either replace the PRU/URU module or clear DART configuration (**Unit Configuration > Clear DART Configuration**).

Major Alarms—PRU/URU DARTs

The following alarms apply to DARTs installed in a Prism Remote Unit (PRU) or a URH Remote Unit (URU).

Alarm:	**DART DC Supply Fault**
Trap:	`fwuRmtDARTDCSupplyFault`
Alarm Code:	AC97
Definition:	DART card DC supply voltages outside specification.
Remedy:	If the alarm persists for 5 minutes (may be transient on startup), replace the DART.

Alarm:	**DART Fault**
Trap:	`fwuRmtDARTFault`
Alarm Code:	AC101
Definition:	Summary of DART Downconverter 1 Synthesizer Unlocked, Downconverter 2 Synthesizer Unlocked, Upconverter Synthesizer Unlocked, DC Supply Fault alarms, and DART FPGA status.
Remedy:	Inspect alarms (**Alarms > View Current Alarms**) for upconverter/downconverter/DC supply alarms on the PRU/URU DART and follow the remedies for those alarms. For PRU DART only—if none of these alarms are present, power cycle the RF Module. If the alarm persists, replace the RF Module.

Alarm:	**DART Hardware Mismatch**
Trap:	**fwuRmtDARTHardwareMismatchFault**
Alarm Code:	AC98
Definition:	Host DART does not support the selected passband. Fault occurs when a Host DART is replaced with another DART of the incorrect type.
Remedy:	Install a DART that supports the selected passband. If the position of the PRU/URU DART is to be changed to a different frequency band, remove and clear the DART configuration (**Unit Configuration > Clear DART Configuration**), install the new DART, set the passband, and establish the new link (**System Configuration > Configure DART Links**).

Alarm:	**Downconvert Fault**
Trap:	**fwuRmtDownconvertfailureFault**
Alarm Code:	AC128
Definition:	Band specific alarm raised during Reverse Link Monitoring on PRU/URU.
Remedy:	Retry System Test (**System Configuration > Perform System Test**). If alarm persists, replace the DART.

Alarm:	**Downconverter 1 Synthesizer Unlocked**
Trap:	**fwuRmtDARTDwnCon1SynLockFault**
Alarm Code:	AC93
Definition:	DART downconverter 1 synthesizer unlocked.
Remedy:	The Downconverter 1 Synthesizer Unlocked alarm can occur during Host reboots and DART hotswaps. If the alarm persists after 5 minutes, replace the DART.

Alarm:	**Downconverter 2 Synthesizer Unlocked**
Trap:	**fwuRmtDARTDwnCon2SynLockFault**
Alarm Code:	AC94
Definition:	DART downconverter 2 synthesizer unlocked.
Remedy:	The Downconverter 2 Synthesizer Unlocked alarm can occur during Host reboots and DART hotswaps. If the alarm persists after 5 minutes, replace the DART.

Alarm:	**FWD Cal Tone Fault**
Trap:	**fwuRmtDownlinkCalToneFailureFault**
Alarm Code:	AC124
Definition:	Forward calibration tone not at expected level.
Remedy:	Retry System Test (**System Configuration > Perform System Test**). If alarm persists, replace the DART.

Alarm:	**REV Test Tone Low**
Trap:	`fwuRmtUplinkFailureDetectLowFault`

Alarm Code:	AC125
Definition:	Reverse test tone not at expected level.
Remedy:	Retry System Test (**System Configuration > Perform System Test**). If alarm persists, replace the DART.

Alarm:	**Upconvert Fault**
Trap:	`fwuRmtUpconvertfailureFault`

Alarm Code:	AC126
Definition:	Band specific alarm raised during Forward Link Monitoring on PRU/URU.
Remedy:	Retry System Test (**System Configuration > Perform System Test**). If alarm persists, replace the DART.

Alarm:	**Upconvert Indeterminate**
Trap:	`fwuRmtUpconIndetFault`

Alarm Code:	AC129
Definition:	Band specific alarm raised during Forward Link Monitoring on PRU/URU.
Remedy:	Retry System Test (**System Configuration > Perform System Test**). If alarm persists, replace the DART.

Alarm:	**Upconverter Synthesizer Unlocked**
Trap:	`fwuRmtDARTUpConSynLockFault`

Alarm Code:	AC95
Definition:	DART upconverter synthesizer unlocked.
Remedy:	The DART Upconverter Synthesizer Unlocked alarm can occur during Host reboots and DART hotswaps. If the alarm persists after 5 minutes, replace the DART.

Major Alarms—PRU/URU SeRF Modules

The following alarms apply to a SeRF module installed in a Prism Remote Unit (PRU) or in a URH Remote Unit (URU).

Alarm:	**Fan Under Speed**
Trap:	`fwuRmtFanUnderSpeedFault`

Alarm Code:	AC77
Definition:	Fans operating below expected RPM.
Remedy:	Verify intake and exhaust vents are clear of obstructions and/or debris. If alarm persists, replace Fan Module.

Alarm: **Host Lost**

Trap: `fwuRmtSeRFHstLostFault`

Alarm Code: AC88

Definition: Host not communicating with PRU/URU.

Remedy: Check that the Host has power and that the power switch is on. Check that at least one of the PRU/URU SFPs is connected to this Host and has acceptable RX power.

Alarm: **SeRF Fault**

Trap: `fwuRmtSERFFault`

Alarm Code: AC87

Definition: Summary of SeRF Synthesizer Unlocked alarm and SeRF FPGA status.

Remedy: Check for related Host SeRF alarms (**Alarms > View Current Alarms**). If no SeRF alarms exist, FPGA is faulty; replace PRU SeRF Module.

Alarm: **SeRF Synthesizer Unlocked**

Trap: `fwuRmtSERFSynthAlarmFault`

Alarm Code: AC86

Definition: SeRF synthesizer unlocked.

Remedy: Ensure that the PRU/URU has an optical input signal. Check that the Host reference clock is properly configured and is not in alarm; otherwise replace the PRU/URU SeRF module.

Alarm: **Temperature High**

Trap: `fwuRmtOverTempFault`

Alarm Code: AC73

Definition: Temperature above operating limit.

Threshold: 95°C

Remedy: Check for PRU/URU Fan Fault alarm (**Alarms > View Current Alarms**). Verify that ambient temperature is less than 50°C. Verify that the air intake and exhaust vents for the PRU/URU are clear of debris.

Major Alarms—PRU/URU SFPs

The following alarms apply to SFPs installed in a Prism Remote Unit (PRU) or in a URH Remote Unit (URU).

NOTE: Cascading Remote Units is not supported in this release. Alarms that pertain to cascaded Remote Units are included as reference only.

Alarm: **Excess Connections**

Trap: `fwuRmtExcessConnFault`

Alarm Code: AC134

Definition: Two or more PRU/URU connected to a single cascaded PRU/URU, or a ninth PRU/URU connected in cascade, or there are more outgoing fibers than incoming fibers on a PRU/URU in a cascade.

Remedy: Connect fiber optic cables per cascade connection rules. Refer to appropriate installation guide for details.

Alarm: **Fiber Connection Mismatch**

Trap: `fwuRmtFiberConnMismatchFault`

Alarm Code: AC133

Definition: Fiber optic cable connections between cascaded PRU/URUs not following SFP connection rules.

Remedy: Connect fiber optic cables per cascade connection rules. Refer to appropriate installation guide for details.

Alarm: **Invalid Device Connection**

Trap: `fwuRmtInvalidDevConnFault`

Alarm Code: AC135

Definition: PRU/URU is connected to a DRU or vice versa.

Remedy: Ensure that cascaded Remotes are all the same type (that is, a PRU to a PRU and a DRU to a DRU). Refer to appropriate installation guide for details.

Alarm: **Optical Over Drive**

Trap: `fwuRmtSERFOptOverDriveFault`

Alarm Code: AC84

Definition: SFP optical receive input power above specification.

Threshold: Threshold for IR is 1 dBm, and for LR is -9 dBm

Remedy: Reduce the optical receive level by adding optical attenuation. Replace optical attenuator if faulty.

Alarm: **Optical RX No Light**

Trap: `fwuRmtSERFOptRxNoLightFault`

Alarm Code: AC82

Definition: No signal detected by optical receiver.

Remedy: Check/repair optical overdrive conditions (**Unit Information > View Optical Ports**). Ensure that fiber optic connections are clean. Check for kinks or sharp bends in the fiber optic cable; replace fiber optic cable if unable to correct any problems found.

Alarm: **Optical Transmitter Fault**

Trap: `fwuRmtSERFOptLaserFault`

Alarm Code: AC83

Definition: SFP optical transmitter failed.

Remedy: Replace Host SFP.

Major Alarms—PRU or URU Duplexer

The following alarms apply to Duplexers, which are installed in the Prism Remote Unit (PRU) or the URH Remote Unit (URU).

Alarm: **Duplexer Mismatch**

Trap: `fwuRmtDuplexerFreqMismatchFault`

Alarm Code: AC116

Definition: Configured frequency range not supported by Duplexer.

Remedy: Change DART passband to fit within duplexer frequency range (**System Configuration** > **Configure DART Links)**. If alarm persists, contact ADC.

Major Alarms—PRU or URU LNA

The following alarms apply to LNAs installed in a Prism Remote Unit (PRU) or URH Remote Unit (URU).

Alarm: **LNA Power Fault**

Trap: `fwuRmtLNAPowerFault`

Alarm Code: AC115

Definition: PRU/URU Low Noise Amplifier (LNA) Power fault.

Remedy: The low noise amplifier has an internal error. If alarm persists, replace the RF Module.

Major Alarms—PRU or URU LPA

The following alarms apply to LPAs installed in a Prism Remote Unit (PRU) or URH Remote Unit (URU).

Alarm:	**LPA DC Fault**
Trap:	`fwuRmtLPADcFault`
Alarm Code:	AC109
Definition:	PRU/URU Linear Power Amplifier (LPA) DC fault.
Remedy:	Caused by internally detected problem with the LPA. Impact is loss of RF service. Reset LPA. If alarm persists, replace the RF Module.

Alarm:	**LPA Disabled**
Trap:	`fwuRmtLPADisableFault`
Alarm Code:	AC105
Definition:	PRU/URU Linear Power Amplifier (LPA) disabled due to an internally detected problem. (VSWR, DC, Loop Fault, Low Power, or Temperature High alarm).
Remedy:	The LPA is disabled because of an internally detected problem. Perform an LPA Reset. If the fault persists replace the RF Module.

Alarm:	**LPA Loop Fault**
Trap:	`fwuRmtLPALoopFault`
Alarm Code:	AC110
Definition:	PRU/URU Linear Power Amplifier (LPA) Loop fault.
Remedy:	Caused by internally detected problem with the LPA. Impact is loss of RF service. Lower DART(s) gain by 10 dB, reset the LPA, and return gain to previous value. If alarm persists, replace RF Module.

Alarm:	**LPA Low Power Fault**
Trap:	`fwuRmtLPALowPowerFault`
Alarm Code:	AC111
Definition:	Internal Linear Power Amplifier (LPA) Low Power fault. Gain of one or more internal amplifiers outside of specification).
Remedy:	Caused by internally detected problem with the LPA. Impact is loss of RF service. Reset LPA. If alarm persists, replace the RF Module.

Alarm:	**LPA Missing**
Trap:	`fwuRmtLPADetectFault`
Alarm Code:	AC112
Definition:	Linear Power Amplifier (LPA) detection fault. LPA missing from PRU.
Remedy:	Cause is faulty RF Module. Impact is loss of RF service. If alarm persists, replace the RF Module.

Alarm: **LPA Over Power**

Trap: `fwuRmtLPAOverPowerFault`

Alarm Code: AC107

Definition: PRU/URU Linear Power Amplifier (LPA) output power level above operating limit.

Threshold: Variable by LPA band.

Remedy: Causes include, forward path gains are set too high or Host RF input levels are too high. Impact is loss of RF service. Reduce PRU forward gain ("System Configuration -> Configure Remote Forward Gain"). Reset the LPA, and then monitor RF output power levels. Adjust gain to acceptable values. If the alarm persists, replace the RF Module.

Alarm: **LPA VSWR Fault**

Trap: `fwuRmtLPAVswrFault`

Alarm Code: AC108

Definition: PRU/URU Linear Power Amplifier (LPA) VSWR fault.

Threshold: 3:1

Remedy: Causes include, faulty RF Module, faulty/loose RF Module to bulkhead cable, faulty/loose external lightning arrestor, cable or antenna. Impact is loss of RF service. Reset LPA. If alarm persists, replace the RF Module.

Major Alarms—PRU or URU Power Detector

Alarm: **RF Power Low**

Trap: `fwuRmtRFPowerFault`

Alarm Code: AC114

Definition: PRU/URU RF Output Power below minimum threshold.

Threshold: 0 dBm; can be configured by user, see "Set RF Power Low Threshold" on page 180.

Remedy: Check for Host DART underdrive alarm or low RF input from BTS. Check the Host and Remote forward gains are set correctly.

Alarm: **System VSWR Fault**

Trap: `fwuRmtSystemVswrFault`

Alarm Code: AC113

Definition: PRU/URU VSWR measurement above specification.

Threshold: 3:1

Remedy: Perform cable sweeps on external antenna cable system. Put a load on the PRU/URU by disconnecting the external antenna cable to determine if the source of the VSWR condition is internal or external. If internal, replace the RF Module. If external, troubleshoot and determine source of high VSWR reading.

Minor Alarms—Host Unit DARTs

Alarm:	**DART ALC Limiting**
Trap:	`fwuHstDARTALCLimitingFault`
Alarm Code:	AC33
Definition:	Host DART forward path Automatic Level Control active.
Threshold:	+19 - Fwd Gain
Remedy:	Decrease the Host DART forward path gain (**System Configuration > Configure Host Forward Gain**), or reduce the RF signal level from the BTS/BDA.

Alarm:	**DART Under Drive**
Trap:	`fwuHstDARTUnderDriveFault`
Alarm Code:	AC31
Definition:	DART forward RF input signal below the normal operating limit.
Threshold:	+5 - Fwd Gain - 20
Remedy:	Check that an RF signal is present at the Host DART forward input. If an RF signal is present, then increase the forward gain of the Host DART. If the alarm does not clear when gain is at maximum, increase the power of the BTS/BDA RF signal.

Alarm:	**RLM Upconvert Indeterminate**
Trap:	`fwuHstRLMUpConIndetFault`
Alarm Code:	AC49
Definition:	Unable to run RLM due to Host Reverse Gain being set too low.
Remedy:	Increase Host Reverse Gain (**System Configuration** > **Configure Host Forward Gain)**.

Minor Alarms—Host Unit SeRF Module

Alarm:	**Temperature Low**
Trap:	`fwuHstUnderTempFault`
Alarm Code:	AC5
Definition:	Temperature below operating limit.
Threshold:	0°C
Remedy:	Verify that ambient temperature is greater than 0°C; fix low temperature condition in the Host's location.

Minor Alarms—Host Unit SFPs

Alarm:	**Optical RX High BER**
Trap:	`fwuHstSERFOptRxBERFault`
Alarm Code:	AC13
Definition:	High bit error rate (BER) detected by fiber optic receiver.
Threshold:	0.00001
Remedy:	Check/repair optical overdrive conditions (**Unit Information > View Optical Ports**). Ensure that fiber optic connections are clean. Check for kinks or sharp bends in the fiber optic cable; replace fiber optic cable if unable to correct any problems found.

Alarm:	**Optical Under Drive**
Trap:	`fwuHstSERFOptUnderDriveFault`
Alarm Code:	AC17
Definition:	SFP optical receive input power below specification.
Threshold:	Threshold for IR is -1 dBm, and for LR is -27 dBm
Remedy:	Check fiber optic cable for too much attenuation and/or dirty connections. Check SFP type (wavelength or IR/LR) being used; replace the SFP if it is the wrong type.

Minor Alarms—PRU/URU DARTs

The following alarms apply to DARTs installed in a Prism Remote Unit (PRU) or in a URH Remote Unit (URU).

Alarm:	**DART Temperature High**
Trap:	`fwuRmtDARTOverTempFault`
Alarm Code:	AC99
Definition:	DART temperature above operating limit.
Threshold:	85°C
Remedy:	Check the PRU/URU fans. Check the air flow around the PRU/URU. Ensure that the PRU/URU door is closed and that the ambient temperature is less than 50°C. Check that the heatsink material on the PRU/URU DARTs has not been damaged. If the alarm persists, replace RF Module.

Alarm:	**DART Temperature Low**
Trap:	`fwuRmtDARTLowTempFault`

Alarm Code:	AC100
Definition:	DART temperature below operating limit.
Threshold:	-40°C
Remedy:	Check ambient conditions; fix low temperature conditions in the DART's location.

Alarm:	**Delay Out Of Range**
Trap:	`fwuRmtRangingFault`

Alarm Code:	AC96
Definition:	PRU/URU delay settings outside the valid range.
Remedy:	Enter forward and reverse delay values (**System Configuration > Configure Delay**) within the displayed range.

Minor Alarms—PRU/URU SeRF Modules

The following alarms apply to SeRF modules installed in a Prism Remote Unit (PRU) or in a URH Remote Unit (URU).

Alarm:	**Fan Over Speed**
Trap:	`fwuRmtFanOverSpeedFault`

Alarm Code:	AC76
Definition:	Fans operating above expected RPM.
Remedy:	If alarm persists, then replace the Fan Module.

Alarm:	**Temperature Low**
Trap:	`fwuRmtUnderTempFault`

Alarm Code:	AC74
Definition:	Temperature below operating limit.
Threshold:	Minus 40°C
Remedy:	Verify that ambient temperature is greater than -40°C; fix low temperature condition at the location of the PRU/URU.

Minor Alarms—PRU/URU SFPs

The following alarms apply to SFPs installed in a Prism Remote Unit (PRU) or in a URH Remote Unit (URU).

Alarm:	**Optical RX High BER**
Trap:	`fwuRmtSERFOptRxBERFault`
Alarm Code:	AC81
Definition:	High bit error rate (BER) detected by fiber optic receiver.
Threshold:	0.00001
Remedy:	Check/repair optical overdrive conditions (**Unit Information > View Optical Ports**). Ensure that fiber optic connections are clean. Check for kinks or sharp bends in the fiber optic cable; replace fiber optic cable if unable to correct any problems found.

Alarm:	**Optical Under Drive**
Trap:	`fwuRmtSERFOptUnderDriveFault`
Alarm Code:	AC85
Definition:	SFP optical receive input power below specification.
Threshold:	Threshold for IR is -1 dBm, and for LR is -27 dBm
Remedy:	Check fiber optic cable for too much attenuation and/or dirty connections. Check SFP type (wavelength or IR/LR) being used; replace the SFP if it is the wrong type.
Remedy:	Check for any major alarms (**Alarms > View Current Alarms**). Follow the remedies for those alarms.

Minor Alarms—PRU or URU LPAs

The following alarms apply to LPAs installed in a Prism Remote Unit (PRU) or URH Remote Unit (URU).

Alarm:	**LPA Over Temperature**
Trap:	`fwuRmtLPAHighTempFault`
Alarm Code:	AC106
Definition:	PRU/URU LPA above operating limit.
Threshold:	89°C
Remedy:	Check ambient temperature. Fix any temperature problems in the area of the PRU/URU. Check the PRU/URU temperature. Replace fan if it is faulty and correct any air flow problems around the PRU/URU. Reset LPA. If the alarm persists, replace the RF Module.

Contact Alarms—Host System Card

Alarm:	**Host Major Contact Alarm Output Active**
Trap:	`fwuHstContactAlarmOutput1`
Alarm Code:	AC41
Definition:	User configurable Major Contact Alarm Output active.
Remedy:	Check for any major alarms (**Alarms > View Current Alarms**). Follow the remedies for those alarms.

Alarm:	**Host Minor Contact Alarm Output Active**
Trap:	`fwuHstContactAlarmOutput2`
Alarm Code:	AC42
Definition:	User configurable Minor Contact Alarm Output active.
Remedy:	Check for any minor alarms (**Alarms > View Current Alarms**). Follow the remedies for those alarms.

Alarm:	**Host Contact Alarm Input 1**
Trap:	`fwuHstContactAlarmInput1`
Alarm Code:	AC43
Definition:	Host Contact Alarm Input #1 active. Alarm level is user configurable.
Remedy:	Check equipment connected to Host Contact Alarm Input 1, or check contact polarity (that is, Normally Open or Normally Closed).

Alarm:	**Host Contact Alarm Input 2**
Trap:	`fwuHstContactAlarmInput2`
Alarm Code:	AC44
Definition:	Host Contact Alarm Input #2 active. Alarm level is user configurable.
Remedy:	Check equipment connected to Host Contact Alarm Input 2, or check contact polarity (that is, Normally Open or Normally Closed).

Contact Alarms—Remote Unit

The following alarms can apply to the Prism Remote Unit (PRU) or the URH Remote Unit (URU).

Alarm:	**Contact Alarm Input 1 Active**
Trap:	`fwuRemoteContactAlarmInput1`
Alarm Code:	AC65
Definition:	Remote Unit (PRU/URU) Contact Alarm Input #1 active.
Remedy:	Check equipment connected to Remote Unit (PRU/URU) Contact Alarm Input 1, or check contact polarity (i.e., Normally Open or Normally Closed).

Alarm:	**Contact Alarm Input 2 Active**
Trap:	`fwuRemoteContactAlarmInput2`
Alarm Code:	AC66
Definition:	Remote Unit (PRU/URU) Contact Alarm Input #2 active.
Remedy:	Check equipment connected to Remote Unit (PRU/URU) Contact Alarm Input 2, or check contact polarity (i.e., Normally Open or Normally Closed).

USERS

This section tells you how to manage users, passwords, and user access to a Prism system.

UNDERSTANDING FLEXWAVE EMS USER ACCOUNTS

The EMS provides security, which can be broadly classified as:

- **User Authentication**, which defines the way a user is identified prior to being allowed to log on to the EMS. User Authentication ensures that only known users have access by providing a method of identifying each user through a user ID and password.

- **User Authorization**, which involves managing the user's privileges in the Prism network management infrastructure. Authorization is based on the concept of user access system configuration restrictions.

There are three user-access accounts that can be assigned by the admin:

- admin—the default user account that has unrestricted access to all EMS user accounts and management capabilities. To protect against unauthorized access to the Prism network, the user assigned the admin role should follow the process described in "Change Your Personal Password" on page 210 to change the password for the admin user account.

- Network Manager—has read and write access to all system functions except user account management.

- Network User—has read only permissions into the system.

There are also two default user-access accounts for the Remote that cannot be deleted or changed:

- operator—is only supported on the Craft interface of a Remote, and provides Read Only access to most of the Prism Remote functions. However, the **operator** login can be only to change the Remote Capacity setting (see "Set the Capacity for a New Remote Unit RSI Board" on page 162).

- viewer—has Read Only rights for Prism and URH Remotes.

FlexWave EMS prevents a login in which the user enters an invalid User ID or password. Table 24 lists the default user accounts and passwords.

Table 24. *Default User Account Device Access*

User Name	Default Password	Port Access	
		Host	Remote
admin	adc123	Network and Craft ports	N/A
viewer	viewer	N/A	Craft port
operator	operator	N/A	Craft port

MANAGE USERS PAGE

The Manage Users page allows you to:

-
-
-

Add a New User

CAUTION! If Auto Complete (that is, remember username/password) is turned on in your web browser, when you add a new user, the browser automatically fills in Prism user names and passwords with the saved information. To avoid this, disable Auto Complete in your browser.

1 To access the **Manage Users** page, in the System Menu bar, click **Users** > **Manage Users**.

2 In the **Manage Users** page, click **Add New User**.
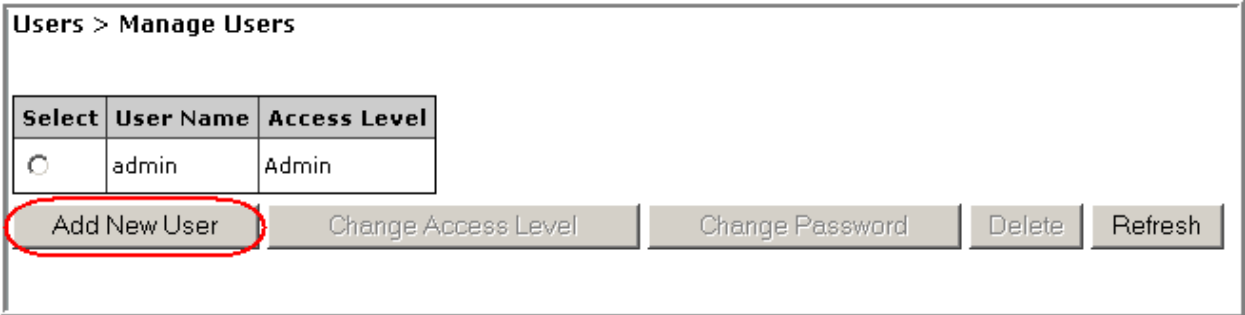
3 Do the following in the **Add New User** page:

a In the **Name** box, enter a user name, which must start with an alphabetical character, contain at least 5 characters (alphanumeric or underscore only), and contain no spaces.

b In the **Password** box, enter a password specific to this user. The Password must contain at least 6 alphanumeric or special characters, and cannot be empty or contain spaces.
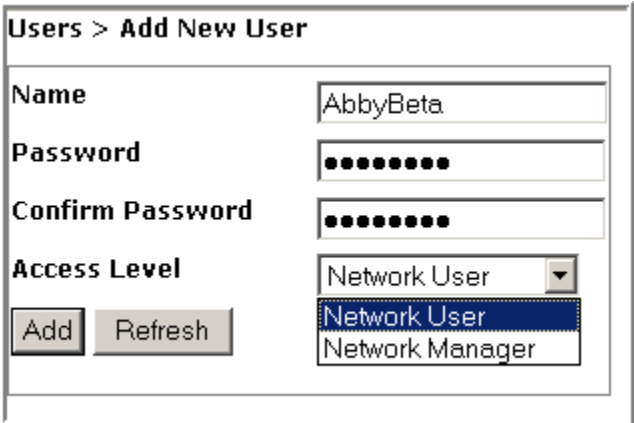
c In the **Confirm Password** box, enter the exact same password as you entered in the **Password** box.

d In the **Access Level** menu, select the access level for this user. See

4 Click **Add**.

The following message displays, listing the new user by **Name**. Additionally, the **Add New User** fields are cleared so you can add other users as needed.

5 In the System Menu bar, click **Users** > **Manage Users** to see an updated list of users.

Change a User's Access Level

1 In the System Menu bar, click **Users** > **Manage Users** to see a list of users.

2 To change a user's access, select the user in the **Select** column, which activates the operational buttons.

3 Click **Change Access**.

4 Verify that the name listed for **Selected User** is the user whose access level you want to change.

5 In the **Change Access Level** page, use the **Access Level** menu to change the access level for this user. For further information on access levels, see "Understanding FlexWave EMS User Accounts" on page 204.

6 Click **Change Access**.

The **Access Level for <*username*> is changed successfully** message displays.

7 In the System Menu bar, click **Users** > **Manage Users** to see an updated list of users.

Select	User Name	Access Level
○	AbbyBeta	Network User
○	BillCharles	Network Manager
○	CallieDelta	Network User
○	DavidEcho	Network User
○	admin	Admin

Users > Manage Users

[Add New User] [Change Access Level] [Change Password] [Delete] [Refresh]

At this time the operational buttons, with the exception of **Add New User** and **Refresh**, will be disabled, as no user is selected.

Change a User Password

NOTE: **Only the admin user or a user with the Network Manager access level can change the password of another user.**
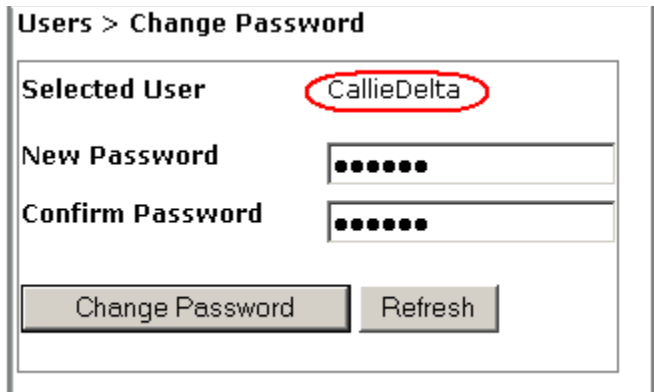
1 In the System Menu bar, click **Users** > **Manage Users** to see a list of users.

2 To change a user's password, select the user in the **Select** column, which activates the operational buttons.

Users > Manage Users

Select	User Name	Access Level
○	AbbyBeta	Network User
○	BillCharles	Network Manager
●	CallieDelta	Network User
○	DavidEcho	Network User
○	admin	Admin

[Add New User] [Change Access Level] [Change Password] [Delete] [Refresh]

3 Click **Change Password**.

4 In the **Change Password** page, do the following:

a Verify that the name listed for **Selected User** is for the user whose password you want to change.

b In the **New Password** box, enter a new password for this user. The Password must contain at least 6 alphanumeric or special characters, and cannot be empty or contain spaces.
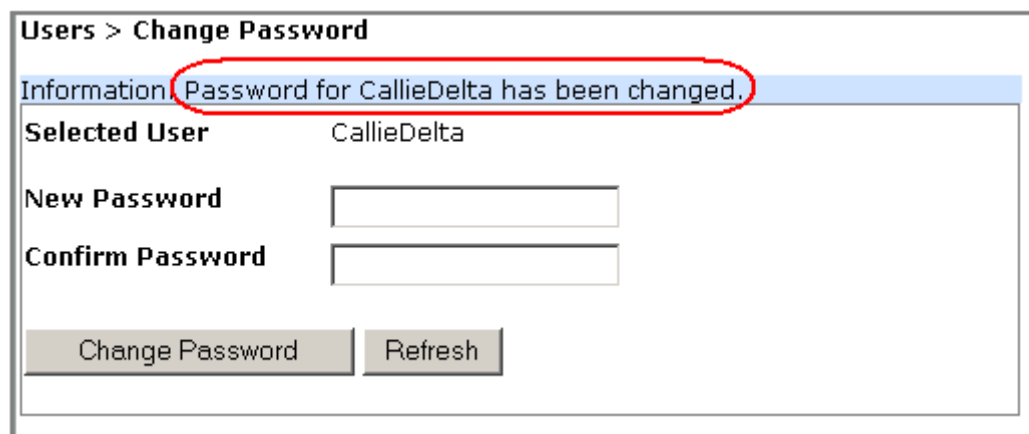
c In the **Confirm Password** box, enter the exact same password as you entered in the **New Password** box.

5 Click **Change Password**.

The **Password changed successfully** message displays.

CHANGE YOUR PERSONAL PASSWORD

1 In the System Menu bar, click **Users** > **Change Password**.

2 In the **Change Password** page, do the following:

    a In the **Old Password** box, enter your existing password.

    b In the **New Password** box, enter a new password for this user. The Password must contain at least 6 alphanumeric or special characters, and cannot be empty or contain spaces.

    c In the **Confirm Password** box, enter the exact same password as you entered in the **New Password** box.

3 Click **Change Password**.

Users > Change Password	
Old Password	
New Password	
Confirm Password	
Change Password	Refresh

The **Password for <*username*> has been changed** message displays.

Users > Change Password	
Information: Password for Carrie has been changed.	
Old Password	
New Password	
Confirm Password	
Change Password	Refresh

RECOVERING A PASSWORD

If a user changes his or her password and then forgets the new password, the admin user needs to recreate an account for the user.

If the password is changed and then forgotten for the admin user, the admin should contact ADC for assistance.

DELETE A USER

1 In the System Menu bar, click **Users** > **Manage Users** to see a list of users.

2 Select the user whose account is to be deleted in the **Select** column, which activates the operational buttons.

3 Click **Delete**.

4 In the confirmation dialog, which identifies the user being deleted, click **OK**.
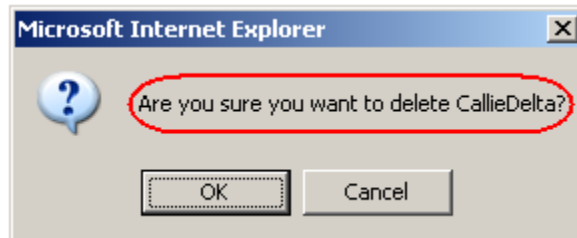
The **User deleted successfully** message displays and the **Users** table is updated in the **Manage Users** page.

UPGRADING THE SYSTEM AND UNITS

Upgrading a Prism system or a unit within a Prism system is a three-step process, in which you do the following:

1 Upload the upgrade file.

2 Use the upgrade file to update the system or unit.

3 Commit the update.

UPLOAD THE UPGRADE FILES

Use the **Upload** page to transfer the required upgrade files from a computer or laptop to your Prism system or unit.

Each software upgrade requires the following files to go from one version to the next:

- **upgrade.*x-y*.tar.gz.md5**

- **upgrade.*x-y*.tar.gz**
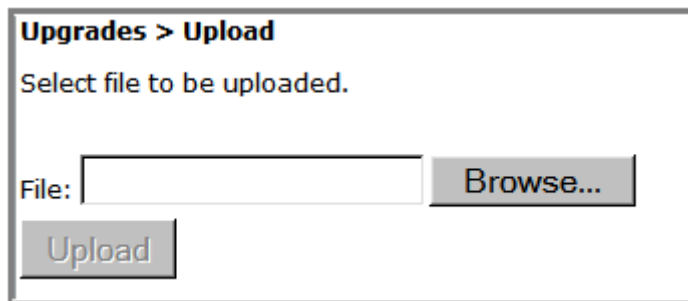
where

- **x** identifies the version from which the unit/system is being upgraded

- **y** identifies the version to which the unit/system is being upgraded.

NOTE: **Each upgrade file set is designed to upgrade a specific EMS release, which may be updating the EMS GUI or unit firmware, or both. If you try to apply upgrade files to a system/unit that is not running the EMS release for which the upgrade files are designed, the update will abort when it runs its version check.**

Do the following to upload the required upgrade files:

1   Contact ADC to obtain the appropriate upgrade files (see "Appendix C: Contacting ADC/TE Connectivity" on page 297).

2   Verify that there is sufficient space on the disk drive to accommodate the upgrade files that you need to upload.

3   Save the upgrade files to your computer.

4   To access the **Upload** page, in the System Menu bar, click **Upgrades** > **Upload**.

5   Click **Browse**.

6   In the **Choose File** dialog, navigate to where the upgrade ***.tar.gz** and ***.tar.gz.md5** files are stored.

7 Select the ***.tar.gz** file, and then click **Open**.
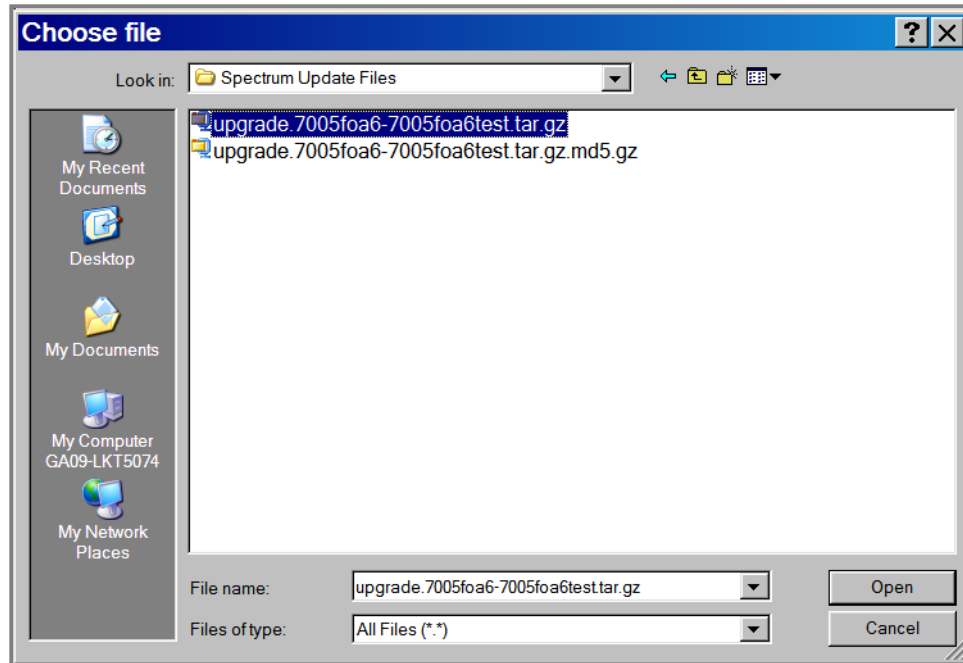
The **Choose File** dialog closes and the name of the selected file displays in the **Upgrades** > **Upload** page **File** box.
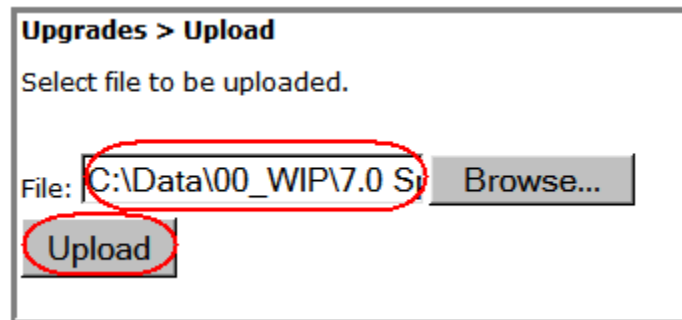
8 Click **Upload**.

Wait for the **File has been uploaded** message to display.
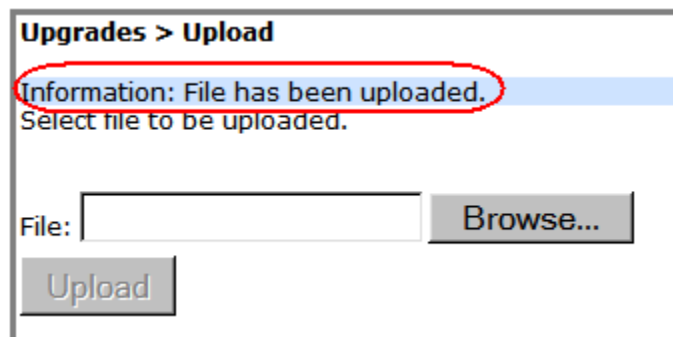
9   In the **Upload** page, Click **Browse**.

1O In the **Choose File** dialog, navigate to where the upgrade ***.tar.gz** and ***.tar.gz.md5** files are stored.

11 Select the ***.tar.gz.md5** upgrade file, and then click **Open**.

12 The **Choose File** dialog closes and the name of the selected file displays in the **Upgrades** > **Upload** page **File** box.

13 Click **Upload**.

Wait for the **File has been uploaded** message to display.

UPDATING A PRISM SYSTEM

Follow this procedure to update a FlexWave Prism system, or an individual unit within a FlexWave Prism system.

CAUTION!   **Do not make any configuration changes during an update.**

CAUTION!   **This procedure takes the system selected for update temporarily offline (see estimates in Table 25). Perform this procedure during normal maintenance window.**

Table 25.   *Estimated Time a System is Offline During an Upgrade*

System Configuration	Approximate Time Offline (Minutes)
1 Host + 1 Remote Unit	7 - 11
1 Host + 2 Remote Units	10 - 18
1 Host + 3 Remote Units	15 - 27
1 Host + 4 Remote Units	21 - 37
1 Host + 5 Remote Units	28 - 48
1 Host + 6 Remote Units	37 - 61
1 Host + 7 Remote Units	48 - 76
1 Host + 8 Remote Units	60 - 92

NOTE: **To update an individual unit, see** "Updating Individual Units" on page 221**.**

Do the following to update an FlexWave Prism system:

1   Access the Software/Firmware report to verify current system software.

a   In the System Menu bar, click **System Information > Get Information**.

The **System Information > Get Information** page opens.

b   In the **Type** list, select **Software/Firmware**. (This is the default setting.)

```
System Information > Get Information

┌─Reports──────────────────────────────────────────────────┐
│                                                          │
│  Type              ┌──────────────────┬─┐  ┌──────────┐  │
│                    │ Software/Firmware │▼│  │ Download │  │
│                    └──────────────────┴─┘  └──────────┘  │
│                                                          │
└──────────────────────────────────────────────────────────┘

┌─Software/Firmware────────────────────────────────────────┐
│ ┌───────────────┬───────────────┬───────────────┬─────────────┬─────────────────┐ │
│ │▼ Module Type  │     Name      │   Unit Id     │  Version    │ Upgrade Status  │ │
│ ├───────────────┼───────────────┼───────────────┼─────────────┼─────────────────┤ │
│ │Host           │SciencesBldg1  │SciencesBldg1 1│7.1.0.4dev5  │Normal operation │ │
│ ├───────────────┼───────────────┼───────────────┼─────────────┼─────────────────┤ │
│ │PRU            │LawrenceLab    │SciencesBldg1 1-1│7.1.0.4dev5│Normal operation │ │
│ └───────────────┴───────────────┴───────────────┴─────────────┴─────────────────┘ │
│ ┌──────────┐                                             │
│ │ Refresh  │                                             │
│ └──────────┘                                             │
│                                                          │
└──────────────────────────────────────────────────────────┘
```

The **Software/Firmware** table provides the following information:

- **Module Type**—type of unit (Host, PRU, or URU).

- **Name**—user-assigned name for the unit.

- **Unit Id**—identifies the unit within the system (see "Unit Identification" on page 43).

- **Version**—version of installed software/firmware.

- **Upgrade Status**—the following states can be seen. However, with the exception of **Normal operation** and **Upgraded**, the states occur very quickly during the corresponding action and are rarely viewed.

    – **Normal operation**

    – **Upgrading**

    – **Upgrading reboot**

    – **Committing**

    – **Aborting**

    – **Recovering**

    – **Upgraded**

    – **NA** (analog units only).

2 Follow the steps in "Upload the Upgrade Files" on page 214 to upload the required upgrade files.

3 Update the Host and the Remote Unit(s):

a In the System Menu bar, click **Upgrades** > **Update Units**.

In the **Update Units** page, you are notified that the file that you uploaded in "Upload the Upgrade Files" on page 214 is ready for use. If an upgrade file is not listed, repeat the steps in "Upload the Upgrade Files" on page 214.

Upgrades > Update Units

Information: upgrade.7005foa6-7005foa6test.tar.gz is available for upgrade.
This command will take the unit(s) temporarily offline.
Do not make any configuration changes during the update.
Do you want to update the unit(s) now?

Unit Type   Host+DRU+PRU+URU ▼
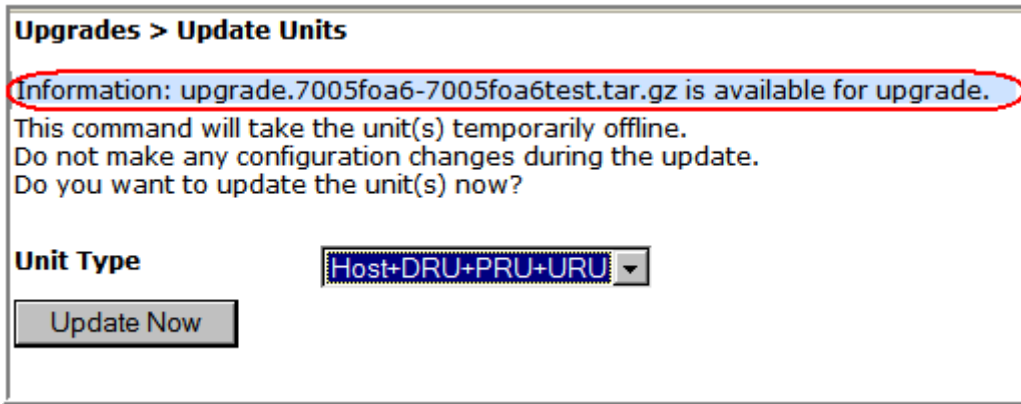
[Update Now]

b In the **Select Unit Type** list, select **Host+DRU+PRU+URU**.

Upgrades > Update Units

Information: nintyfiveMB.tar.gz is available for upgrade.
This command will take the unit(s) temporarily offline.
Do not make any configuration changes during the update.
Do you want to update the unit(s) now?

Unit Type   Host+DRU+PRU+URU ▼
                   Host+DRU+PRU+URU
[Update Now]   IFEU + RAU
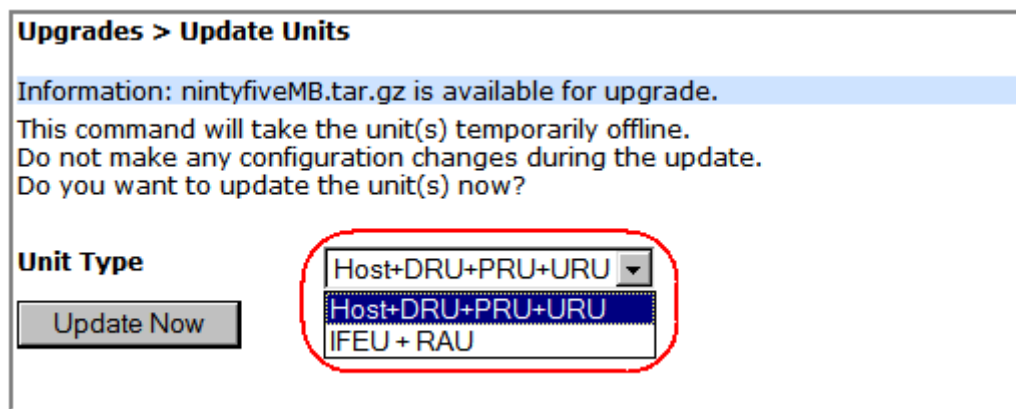
NOTE: **The IFEU + RAU option pertains to an InterReach Spectrum system only and is not applicable to a Prism system. As such, do not select the IFEU + RAU option.**

c Click **Update Now**. An information message that the update has started appears.
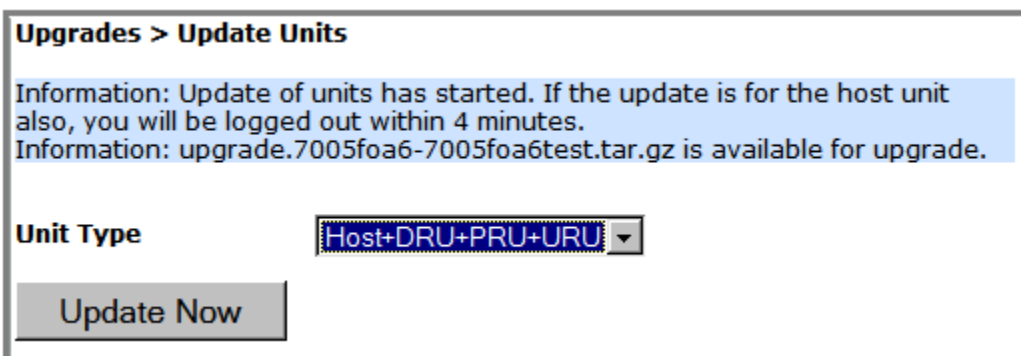
Upgrades > Update Units

Information: Update of units has started. If the update is for the host unit also, you will be logged out within 4 minutes.
Information: upgrade.7005foa6-7005foa6test.tar.gz is available for upgrade.

Unit Type   Host+DRU+PRU+URU ▼

[Update Now]

Within four minutes, the EMS logs you off and terminates the EMS session.

CAUTION! At this point, the system goes offline for the approximate time listed in Table 25 on page 216.

    d Wait approximately four minutes, and then log back in to the EMS to complete this procedure.

4 Complete Step 1 on page 216 to verify the status of the Host/Remote Unit(s) updates.

COMMIT THE UPGRADE

NOTE: If you need to abort an update, go to "Abort an Update" on page 220.

1 Complete the steps in "Updating a Prism System" on page 216.

2 In the System Menu bar, click **Upgrades** > **Commit**.

3 In the **Upgrades > Commit** page, click **Commit**.
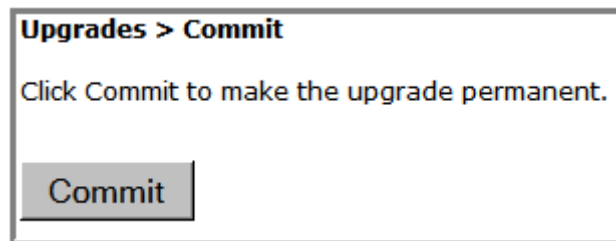
> **Upgrades > Commit**
>
> Click Commit to make the upgrade permanent.
>
> [Commit]

4 In the confirmation window, click **OK**.

> **Microsoft Internet Explorer** [×]
>
> ❓ Do you want to commit (make permanent) the upgrade?
>
> [OK]   [Cancel]

The system informs you when the commit operation has completed.

> **Upgrades > Commit**
>
> Information: Commit operation completed.
> Click Commit to make the upgrade permanent.
>
> [Commit]
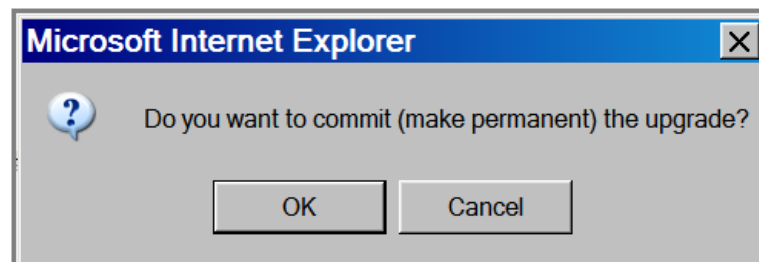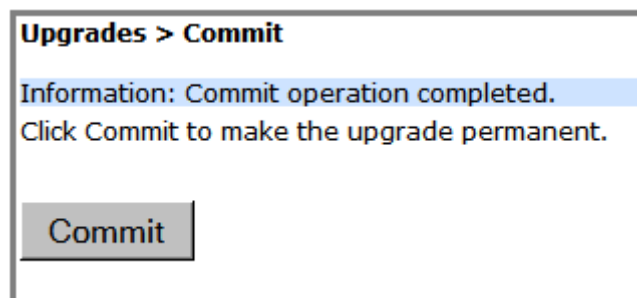
ABORT AN UPDATE

An upgrade can be aborted, if necessary.

NOTE: **If you want to commit an update, go to** "Commit the Upgrade" on page 219**.**

1   To access the **Upgrades Abort** page, in the System Menu bar, click **Upgrades** > **Abort**.

Upgrades > Abort

Click Abort to cancel the upgrade.
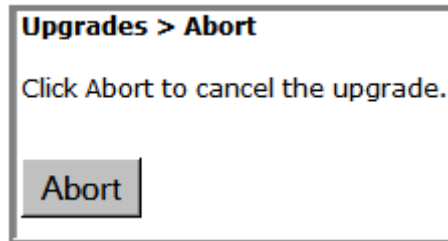
Abort

2   Click **Abort**.

3   In the confirmation window, click **OK**.

Microsoft Internet Explorer

Do you want to abort (undo) the upgrade?

OK   Cancel
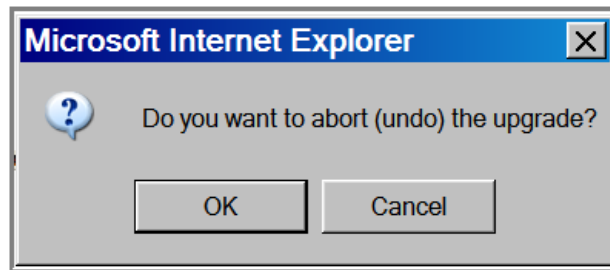
The system informs you when the abort operation has completed.

Upgrades > Abort

Information: Operation aborted.
Click Abort to cancel the upgrade.

Abort
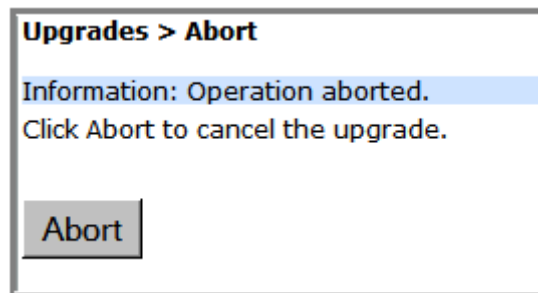
UPDATING INDIVIDUAL UNITS

Only perform a unit update on a unit when the unit is being added to the system as a new or replacement unit, and the new unit requires a firmware update to match the firmware version of the other units within the system.

CAUTION! **If this procedure is performed on a Host Unit, the Host is taken offline (see estimates in Table 25 on page 216). Perform this procedure during normal maintenance time.**

CAUTION! **Do not make any configuration changes during an update.**

NOTE: **To update a Prism system, follow the steps in** "Updating a Prism System" on page 216**.**

Complete the following steps to update an individual Host, PRU, or URU:

1 Access the Software/Firmware report to verify current system software.

   a In the System Menu bar, click **System Information > Get Information**.

      The **System Information > Get Information** page opens.

   b In the **Type** list, select **Software/Firmware**. (This is the default setting.)

System Information > Get Information

Reports

| Type | Software/Firmware ▼ | Download |

Software/Firmware

▼ Module Type	Name	Unit Id	Version	Upgrade Status
Host	SciencesBldg1	SciencesBldg1 1	7.1.0.1	Normal operation
PRU	LawrenceLab	SciencesBldg1 1-1	7.1.0.1	Normal operation

Refresh

   For information on the **Software/Firmware** table, see "Updating a Prism System".

2 Follow the steps in "Upload the Upgrade Files" on page 214 to upload the required update files.

3 In the System Tree, click on the icon of the unit that you want to update.

4 In the Unit Menu bar, click **Unit Upgrades**, **Upgrade**.

NOTE: If you have not uploaded the required update files, the following page opens, and the Update button is disabled. You cannot continue until the correct update files have been loaded.
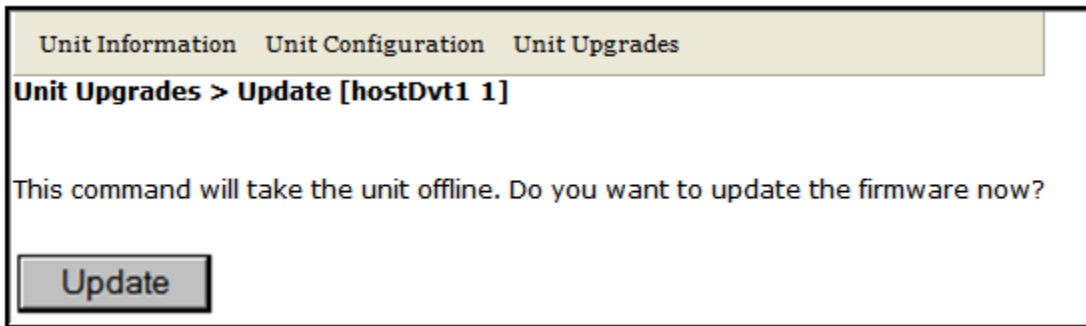
Unit Information   Unit Configuration   Unit Upgrades
Unit Upgrades > Update [host_ 1]

Information: Please upload the upgrade file (*.tar.gz).
Do you want to upgrade this unit?

Update

5 Click **Update**.

Unit Information   Unit Configuration   Unit Upgrades
Unit Upgrades > Update [hostDvt1 1]

This command will take the unit offline. Do you want to update the firmware now?

Update

Within four minutes, the EMS logs you off and terminates the EMS session.

CAUTION! At this point, the system goes offline for the approximate time listed in Table 25 on page 216.

6 Wait approximately four minutes, and then log back in to the EMS to complete this procedure.

7 Complete Step 1 on page 216 to verify the status of the update. Do not move forward to the next step until the **UpGrade Status** in the Software/Firmware table is listed as **Upgraded**.

8 Commit the update to the unit. (If you need to abort an update, go to "Abort an Update" on page 220.)

    a In the System Menu bar, click **Upgrades** > **Commit**.

    b In the **Upgrades > Commit** page, click **Commit**.
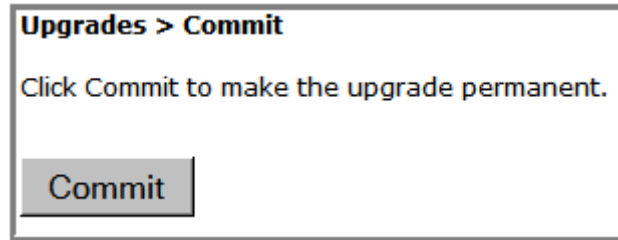
Upgrades > Commit

Click Commit to make the upgrade permanent.

[Commit]

    c In the confirmation window, click **OK**.

Microsoft Internet Explorer [X]

(?) Do you want to commit (make permanent) the upgrade?

[OK]   [Cancel]

The system informs you when the commit operation has completed.

Upgrades > Commit

Information: Commit operation completed.
Click Commit to make the upgrade permanent.
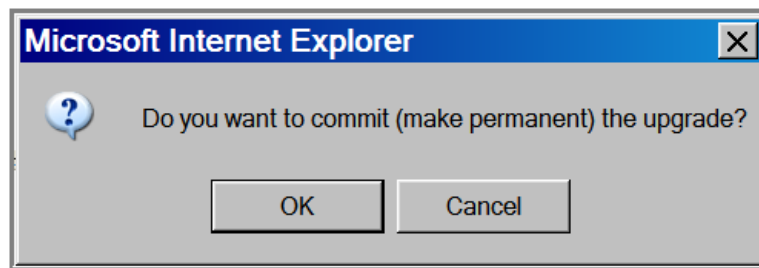
[Commit]
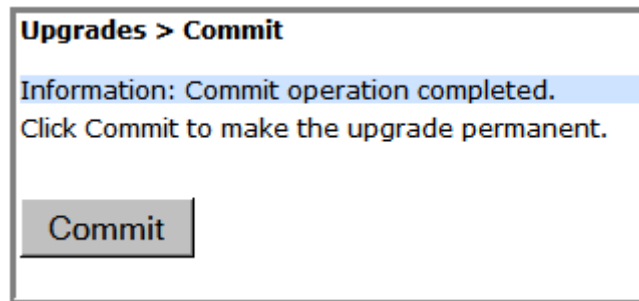
9 Complete Step 1 on page 216 to verify the status of the update.

Intentionally Blank Page

SPECIAL FEATURES

This section describes special features of the Prism EMS.

NOTE: Some of the features in this section are for use by ADC only.

RUN SCRIPT

The **Run Script** page, accessed via **Special Features > Run Script**, is not applicable to a Prism system and should not be used.

RUN COMMAND

The **Run Command** page, accessed via **Special Features > Run Command**, is not applicable to a Prism system and should not be used.

CONFIGURE FEATURE

CAUTION! **This procedure requires a system reboot. The system configuration is stored on the Host. Rebooting the Host therefore results in a loss of RF for the Host and connected Remote Units until the Host comes back up. Depending on the system configuration, it can take 5 to 20 minutes before management communication is restored.**

CAUTION! **Host configuration will not persist across a Configure Feature Reboot—all settings will revert to factory default. You will need to reconfigure the Prism system after the system reboots.**

CAUTION! **The current EMS session will close and you will need to log back in to the EMS after the Host reboot has completed.**

1 Document all configuration data, as settings will have to be re-entered. To record the current configuration:

    a Follow the procedures in "Viewing the All Report" on page 112 to access the system configuration reports.

    b Follow the procedures in "Downloading a Report" on page 113 to download the system configuration reports to a hard drive.

2 To access the **Configure Feature** page, in the System Menu bar, click **Special Features > Configure Feature**.

3 In the **Feature** box, enter the code for the feature.

4 In the **Password** box, enter the password that enables the feature.

5 Click **Apply**.

Special Features > Configure Feature

Passwords can not be more than eight characters.

Feature	feature
Password	●●●●●●

Apply

6 In the confirmation dialog, click **OK**.

Microsoft Internet Explorer

You will need to reboot the system for the changes to take effect.
Do you want to reboot the system? It can take up to 2 minutes and will take the system offline.

OK   Cancel
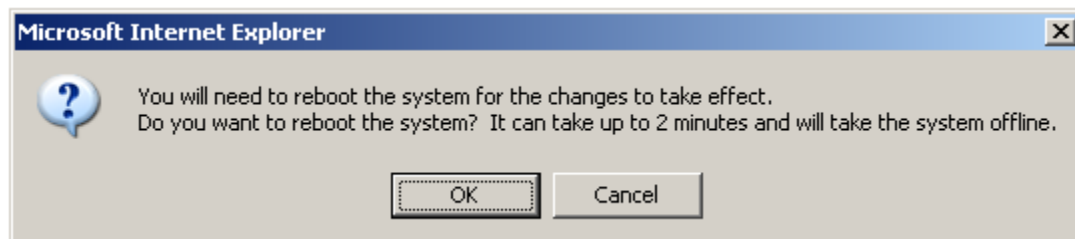
7 Log back in to the EMS once the login window displays.

8 Follow the steps in "Initial FlexWave Prism System Setup" on page 55 to reconfigure the Prism system, using the settings recorded in Step 1 on page 227.

Intentionally Blank Page

USING AN SNMP INTERFACE

SNMP OVERVIEW

SNMP (Simple Network Management Protocol) is an international standard for remote control of online devices. A typical scenario involves the devices being controlled, remote computers (called managers) that can control them, a network connection, and SNMP software. The SNMP software includes SNMP manager software on controlling computers, SNMP agent software on managed devices, and one or more MIBs used by the SNMP managers for each controlled device. In some cases, SNMP proxy agent software is run on an intermediate device to access a managed device that would not otherwise be directly accessible.

The Prism system SNMP interface, shown schematically in Figure 27 allows a remote user using an SNMP manager to access the same database as accessed by the standard EMS interface.
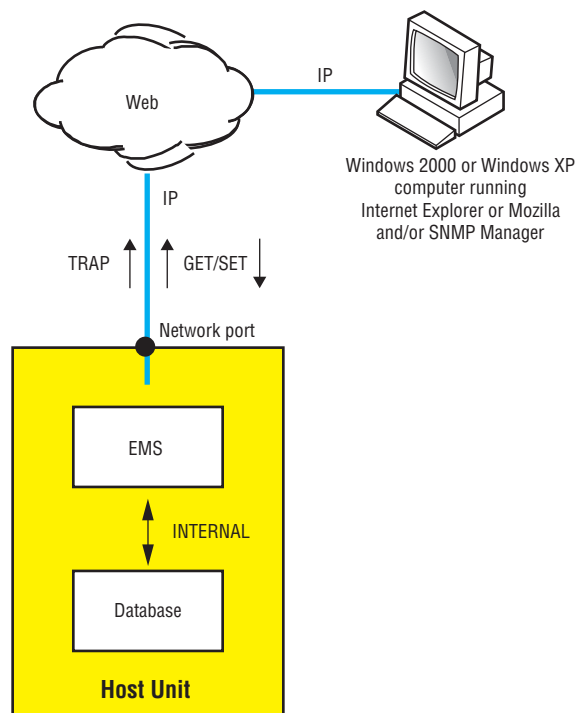
Figure 27. SNMP and a Prism System

WORKING WITH PRISM MIB FILES

NOTE: **Examples shown in this chapter use a browser from AdventNet or iReasoning. Procedural details may vary with another browser, but the basic steps are the same.**

NOTE: **In the Prism system, the database accessed through the SNMP interface is the same database as used by the EMS graphical user interface. There is therefore a similarity between MIB objects and the parameters displayed in the EMS Web pages.**

Figure 28 shows the features of a typical MIB browser.
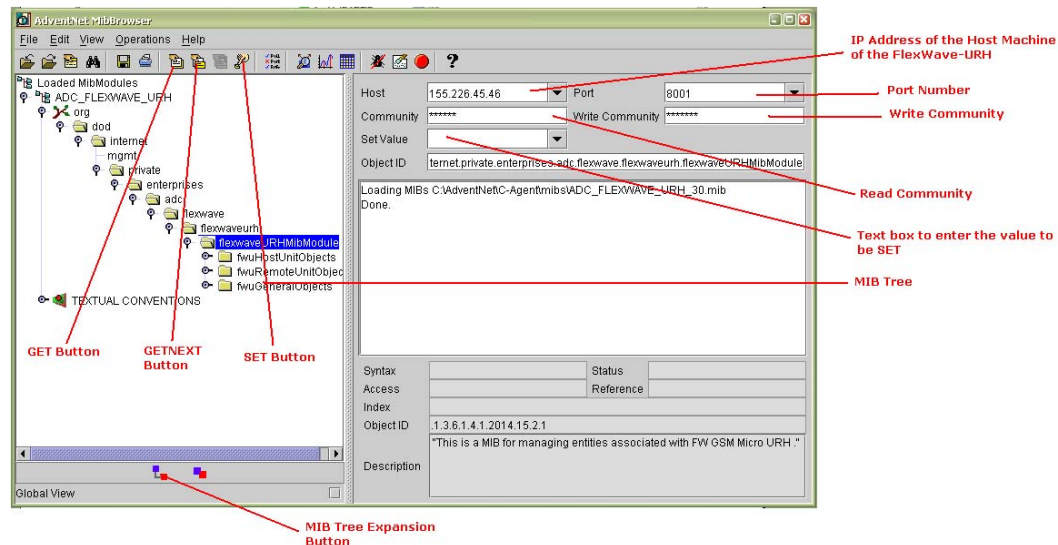
Figure 28. Typical MIB Browser

As mentioned earlier, a MIB is a database specification containing definitions and organization of information. The database consists of tables of objects used to exchange information between a manager and agent. Database information is exchanged using the following basic operations:

• **GET**—obtains an object value from the database.

• **SET**—sets the value of an object in the database.

• **GET-NEXT**—gets the next item in the database, be it the next type of object or the next object of the specified type. This is especially useful for discovering the presence of entries in dynamic tables.

• **GET-BULK**—requests multiple items in one message.

• **TRAP/NOTIFICATION**—sends an alarm in which a response can be sent by a manager to an agent confirming receipt of the alarm.

In a manager browser, a MIB looks like the EMS System Tree's hierarchy of folders and files, as shown in Figure 29.
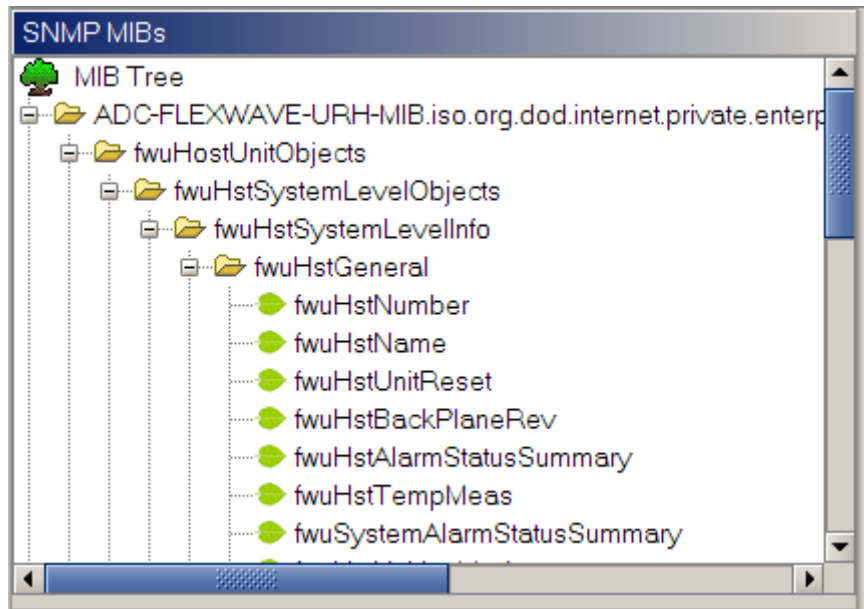
Figure 29. Prism MIB Tree

MIB items are arranged in a hierarchy of groups, like a hierarchy of folders. Known OIDs specify scalars (objects). MIB objects are arranged in groups and tables. To be specified completely, table entries require one or more row indices. Each set of objects (within a single folder) represents one such group or table. An object marked with a key symbol indicates that view is the key value for that table.

The Prism MIB is defined by three files:

- **ADC-FWU-URH-TC-MIB.mib**

- **ADC-FWU-IRS-TC-MIB.mib**

- **ADC-FLEXWAVE-URH.mib**

The MIB can be found on the SeRF II card in the Host in **/usr/local/fwu/mibs**.

"Prism MIB Objects" on page 236 lists objects that may be accessed for **GET/SET** operations and traps/notifications that are sent to SNMP managers registered to receive them whenever the respective fault condition occurs.

NOTE: **TRAPS/NOTIFICATIONS** are listed with the corresponding EMS alarm in "Troubleshooting Alarms" on page 185.

Accessing Prism MIBs

The Prism Agent MIB can be accessed using any SNMP manager with an active network connection. The IP address of the Host must be known and entered in the MIB browser.

1 On the manager computer, open the MIB Browser.

2 Load the MIB files in the following order:

    a `ADC-FWU-URH-TC-MIB.mib`

    b `ADC-FWU-IRS-TC-MIB.mib`

    c `ADC-FLEXWAVE-URH.mib`

3 Enter the IP address of the Host of the Prism system in the text box provided next to **Host**.

4 Enter the **Port number** as `161`.

NOTE: If you are upgrading from a previous release, note the change in the SNMP Port number. In previous releases, the SNMP Port number was 8001. It is now 161.

5 Enter the **Read Community** as `public` and **Write Community** as `private`.

6 Set **Timeout** to **15 seconds**.

7 For SNMP version v2c and v3, set **Maximum Repetitions** to **10** or less.

8 To see an overview the MIB content, expand the MIB tree, as shown below.
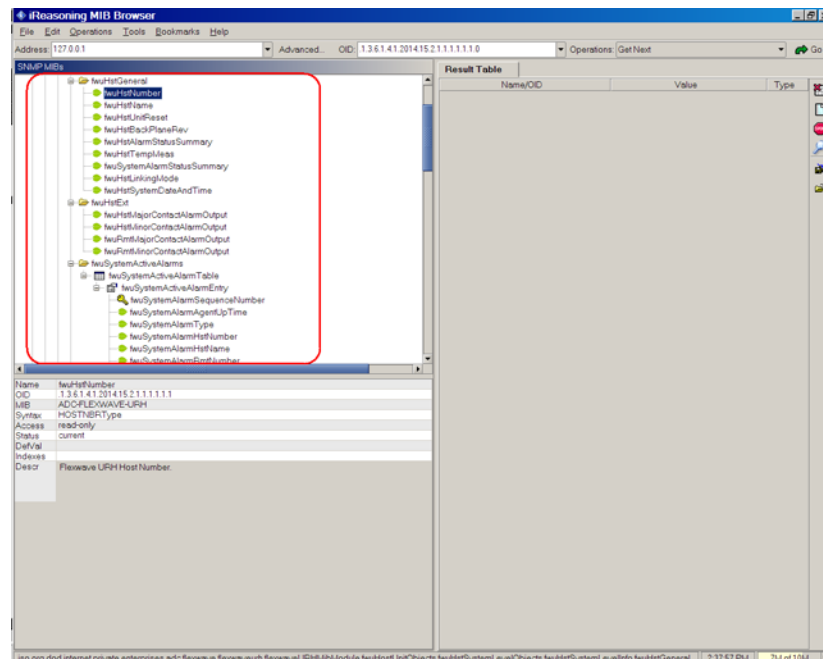
System Date and Time MIB Format

fwuHstSystemDateandTime allows you to set the system date and time, where the input is as follows:

`YYYY-MM-DD,HH:MM:SS.D (24-Hour Time Format)`

where fields are required (none are optional) and indicate the following in 24-Hour time format.

- `YYYY`—Year

- `MM`—Month

- `DD`—date

- `HH`—Hour

- `MM`—Min ute

- `SS`—Seconds

You can input the month, date, hour, minutes, seconds, and deci seconds as a single digit or as a double digit (that is, prefixed with 0).

The supported date and time range is from `1970-01-01,00:00:00` to `2037-12-31,23:59:59`.

The output for month, date, hour, minutes, and seconds will always be in double digit format (prefixed with 0). The output for deci seconds will always be single digit.

For example, the output of **2009-01-02,03:04:05** can be resultant from either of the following inputs:

- Input 1—**2009-01-02,03:04:05**

- Input 2—**2009-1-2,3:4:5**

Band Types

Table 26 lists the band types for Host RF DARTs, and Table 27 on page 236 lists the band types for Remote IF DARTs.

Table 26. *MIB Band Types—Host RF DARTS*

MID Value	Band Type
-1	undefined
1	Classic850
2	Classic1900
3	ClassicSMR800
4	ClassicSMR900
5	ClassicAws2100
6	Classic1800
200	SingleSuperPcs1900
201	SingleSuper1800
202	SingleSuperUmts2100
203	SingleSuperAws2100
8	SuperPcs1900
10	SuperUmts2100
11	SuperAws2100
12	SuperEgsm900
13	SuperLowerAbc700
14	SuperUpperC700
205	SingleSuperLowerAbc700
206	SingleSuperUpperC700

Table 27. *MIB Band Types—Remote IF DARTS*

MID Value	Band Type
15	SuperIf850
16	SuperIfPcs1900
17	SuperIfSmr800
18	SuperIfSmr900
19	SuperIf1800
21	SuperIfAws2100
23	SuperIfPath1LowerAbc700
24	SuperIfPath1UpperC700
25	SuperIfPath2LowerAbc700
26	SuperIfPath2UpperC700
207	SingleSuperIf850
208	SingleSuperIfPcs1900
209	SingleSuperIfSmr800
210	SingleSuperIfSmr900
211	SingleSuperIf1800
213	SingleSuperIfAws2100
215	SingleSuperIfPath1LowerAbc700
216	SingleSuperIfPath1UpperC700
217	SingleSuperIfPath2LowerAbc700
218	SingleSuperIfPath2UpperC700

PRISM MIB OBJECTS

Objects in the Prism Agent MIB divide into two types: **GET/SET** objects and Trap/Notification objects.

For each **GET** and **SET** object, there is an SNMP syntax, which is a range of values defined in the MIB file. These values are what can be entered in a **SET** command and returned in a **GET** command.

The following sections list all MIB objects within the Prism Agent MIB. Objects that are available for **SET** commands are also available for **GET** commands.

Parameters in ADC-FLEXWAVE-URH-MIB

System-Level Parameters

System Date and Time

SNMP MIB: `fwuHstSystemDateAndTime`

Description: The date and time settings on the system

Values: 1970-01-01,00:00:00 to 2037-12-31,23:59:59; see "System Date and Time MIB Format" on page 234

Default: System time

Syntax: DateAndTime

Access Level: Octet String

System Alarm Acknowledge

SNMP MIB: `fwuSystemAlarmAck`

Description: Acknowledges all or individual alarms

Values: 0 = Acknowledge all alarms
Greater then 0, Id of the alarm to be acknowledged

Syntax: Integer32

Access Level: Read-Write

System Alarm Level

SNMP MIB: `fwuAlarmLevel`

Description: Alarm level of system

Syntax: AlarmType

Access Level: Read-Write

System Test On Power Up

SNMP MIB: `fwuPwrUpLinkTest`

Description: System/Link Test on Power Up (Link Test)

Values: 1 = Enable
0 = Disable

Default: 0

Syntax: Unsigned32

Access Level: Read-Write

DART Band Type for System Test User Commanded

SNMP MIB: `fwuUserCommLinkTestDartBandType`

Description: Band type (the RF DART type) of selected units

Values: See "Band Types" on page 235.

Default: 0

Syntax: BandType

Access Level: Read-Write

DART ID for System Test User Commanded

SNMP MIB: `fwuUserCommLinkTestDartId`

Description: Id of a particular DART

Values: 1 - 8

Syntax: Integer32

Access Level: Read-Write

System Alarm Status Summary

SNMP MIB: `fwuSystemAlarmStatusSummary`

Description: Alarm Status Summary for entire system

Syntax: AlarmType

Access Level: Read Only

Clear System Configuration

SNMP MIB: `fwuClearSysConfig`

Description: Changing the value from 0 to 1 clears the setting for the entire settings on the system

Values: 0 = Disable
1= Enable

Default: 0

Syntax: Integer32

Access Level: Read-Write

Last Run Time of System/Link Test

SNMP MIB: `fwuLinkTestLastRunTime`

Description: Time when the System/Link test was last run

Syntax: DateAndTime

Access Level: Read Only

Host Unit Parameters

Host Parameters

Host Number

SNMP MIB: `fwuHstNumber`

Description: Number enumerating a Host

Values: A number greater than 0

Default: 1

Syntax: Integer32

Access Level: Read Only

Host Name

SNMP MIB: `fwuHstName`

Description: User defined name of the Host

Values: Alphanumeric Characters. Except as first character, the underscore (_) character is allowed. Must be 5 to 40 characters in length, with no spaces.

Default: Unknown_HostName

Syntax: Display String

Access Level: Read-Write

Host Unit Reset

SNMP MIB: `fwuHstUnitReset`

Description: Resets the Host SeRF card when the value is changed from 0 to 1

Values: 0= normal
1 = reset

Default: 0

Syntax: Integer

Access Level: Read-Write

Host Back Plane Revision

SNMP MIB: `fwuHstBackPlaneRev`

Description: Provides the back plane revision of the Host (Three pin Version Number of the Chassis back plane)

Values: SIZE (1...40)

Syntax: Octal String

Access Level: Read Only

Host Alarm Status Summary

SNMP MIB: **`fwuHstAlarmStatusSummary`**

Description: Alarm Status Summary for Host

Syntax: ALARM-TYPE

Access Level: Read Only

Temperature Measurement

SNMP MIB: **`fwuHstTempMeas`**

Description: Host system temperature value in Celsius

Values: SIZE (1...8)

Syntax: Octal String

Access Level: Read Only

Linking Mode

SNMP MIB: **`fwuHstLinkingMode`**

Access Level: The DART Linking mode on the System

Values: 2 = Manual

Default: 2

Syntax: Integer

Access Level: Read-Write

Host SeRF Card Parameters

Linux Kernel Version

SNMP MIB: **`fwuHstSERFLinuxKernelVer`**

Description: Linux Kernel Version of the Host system

Syntax: Display String

Access Level: Read Only

Linux Boot Loader Version

SNMP MIB: **`fwuHstSERFLinuxBootLoaderVer`**

Description: Version Number of the second stage boot loader

Syntax: Display String

Access Level: Read Only

Compact Flash SW Version

SNMP MIB: **`fwuHstSERFCompactFlashSWVer`**

Description: Compact Flash Version of the Host system

Values: Format of: **`aa.bb.cc.dd`**
where each of **`aa`**, **`bb`**, **`cc`**, **`dd`** must be between 00 and 99

Syntax: Display String

Access Level: Read Only

PPC HW Monitor SW Version

SNMP MIB: `fwuHstSERFPPCHWMonSWVer`

Description: Software Version of the hardware Monitor process running on the Host

Syntax: Display String

Access Level: Read Only

PPC Application Monitor SW Version

SNMP MIB: `fwuHstSERFPPCAPPMonSWVer`

Description: Software Version of the Application Monitor process running on the Host

Syntax: Display String

Access Level: Read Only

SNMP Agent SW Version

SNMP MIB: `fwuHstSERFPPCSNMPAgentSWVer`

Description: Software Version of the HTTP/SNMP agent running on Host

Syntax: Display String

Access Level: Read Only

PPC Mate Monitor SW Version

SNMP MIB: `fwuHstSERFPPCMATEMonSWVer`

Description: Software Version of the Mate Monitor process running on the Host Unit

Syntax: Display String

Access Level: Read Only

PPC ENET Monitor SW Version

SNMP MIB: `fwuHstSERFPPCENETMonSWVer`

Description: Software Version of the Ethernet Monitor process running on the Host Unit

Syntax: Display String

Access Level: Read Only

PPC FPGA Monitor SW Version

SNMP MIB: `fwuHstSERFPPCFPGAMonSWVer`

Description: Version of FPGA Loaded on SeRF

Syntax: Display String

Access Level: Read Only

Linux First Stage Boot Loader Version

SNMP MIB: `fwuHstSERFLinuxBootLoaderVer`

Description: Boot Loader1 Version of the Host system

Syntax: Display String

Access Level: Read Only

SeRF FPGA Version

SNMP MIB: `fwuHstSERFFPGAVer`

Description: Version of FPGA Loaded on SeRF

Syntax: Display String

Access Level: Read Only

RI ADC Part Number

SNMP MIB: `fwuHstSERFRIADCPartNumber`

Description: Host SeRF Inventory - ADC Part Number

Syntax: Display String

Access Level: Read Only

RI Serial Number

SNMP MIB: `fwuHstSERFRISerialNumber`

Description: Host SeRF Inventory - Serial Number

Syntax: Display String

Access Level: Read Only

RI Date Code

SNMP MIB: `fwuHstSERFRIDateCode`

Description: Host SeRF Inventory - Date Code

Syntax: Display String

Access Level: Read Only

SeRF RI Hardware Version

SNMP MIB: `fwuHstSERFRIHWVer`

Description: Host SeRF Inventory - Hardware Version

Syntax: Octal String

Access Level: Read Only

SeRF RI Hardware Generation

SNMP MIB: `fwuHstSERFRIHWGen`

Description: Host SeRF Hardware Generation

Values: 0 = First Generation
                   1 = Second Generation

Syntax: Integer

Access Level: Read Only

pThread Software Version

SNMP MIB: `fwupThreadSoftwareVersion`

Description: The version number of pThread process

Syntax: DisplayString

Access Level: Read Only

Subagent Software Version

SNMP MIB: `fwuSubagentSwVersion`

Description: The version number of the subagent

Syntax: DisplayString

Access Level: Read Only

Web Server Software Version

SNMP MIB: `fwuWebServerSwVersion`

Description: The version number of web server

Syntax: DisplayString

Access Level: Read Only

Host SeRF Optics Parameters

SFP Number

SNMP MIB: `fwuHstSERFOptSFPNumber`

Description: SFP Numbers used as Index for Optical Ports

Values: 1 - 8

Syntax: Integer32

Access Level: Read Only

SFP Name

SNMP MIB: `fwuHstSERFOptSFPName`

Description: User defined SFP name - Optical Port Name

Values: Alphanumeric Characters. Except as first character, the underscore (_) character is allowed. Must be between 5 and 32 characters in length, with no spaces.

Default: UnknownSFPName

Syntax: Display String

Access Level: Read-Write

SFP Type

SNMP MIB: `fwuHstSERFOptSFPType`

Description: SFP Type - Optical Port Type

Syntax: OpticsType

Access Level: Read Only

SFP Transmission Color

SNMP MIB: `fwuHstSERFOptSFPTxColor`

Description: SFP wavelength in nanometer (nm)

Syntax: Integer32

Access Level: Read Only

FWD Launch Power

SNMP MIB: `fwuHstSERFOptFwdLaunchPowerMeas`

Description: Value of Host Transmit measured optical power in dBm

Syntax: DisplayString

Access Level: Read Only

REV Receive Power

SNMP MIB: `fwuHstSERFOptRevLaunchPowerMeas`

Description: Value of Host Receive measured optical power in dBm

Syntax: DisplayString

Access Level: Read Only

Mate Name

SNMP MIB: `fwuHstSERFOptMateName`

Description: Name of Host Mates

Values: Inherits the valid values from Host Name

Default: NA

Syntax: DisplayString

Access Level: Read Only

Mate ID

SNMP MIB: `fwuHstSERFOptMateId`

Description: ID (numerical) of companion Remote Unit

Values: See "Unit Identification" on page 43

Syntax: NodeAddr1

Access Level: Read Only

Mate SFP ID

SNMP MIB: `fwuHstSERFOptMateSfpId`

Description: Slot ID of the SFP used at remote end

Values: 1 - 8

Syntax: Integer32

Access Level: Read Only

Host SeRF ENET Switch Parameters

Ethernet Port Number

SNMP MIB: `fwuHstSERFEthPortNumber`

Description: An identifier for each Ethernet port

Values: 1...12

Syntax: Unsigned32

Access Level: Read Only

Ethernet Port Type

SNMP MIB: `fwuHstSERFEthPortType`

Description: An identifier for the type of Ethernet port

Syntax: EnetType

Access Level: Read Only

Host SFP ID

SNMP MIB: `fwuHstSERFEthPortSFPId`

Description: Identifier of SFP to which the Ethernet port connects

Values: 1...8

Syntax: Integer32

Access Level: Read Only

Rx-bytes

SNMP MIB: `fwuHstSERFEthPortRxBytes`

Description: Receive byte counter

Syntax: Counter64

Access Level: Read Only

Rx-packets

SNMP MIB: `fwuHstSERFEthPortRxPkts`

Description: Receive packet counter

Syntax: Counter64

Access Level: Read Only

Rx-fsc-errors

SNMP MIB: `fwuHstSERFEthPortRxFcsErrors`

Description: Receive FCS error counter

Syntax: Counter64

Access Level: Read Only

Receive-multicast-packets

SNMP MIB: **`fwuHstSERFEthPortRxMulticastPkts`**

Description: Receive multicast packet counter

Syntax: Counter64

Access Level: Read Only

Receive-broadcast-packets

SNMP MIB: **`fwuHstSERFEthPortRxBroadcastPkts`**

Description: Receive broadcast packet counter

Syntax: Counter64

Access Level: Read Only

Rx-fragmented-frames

SNMP MIB: **`fwuHstSERFEthPortRxFragmtdFrames`**

Description: Receive fragments counter

Syntax: Counter64

Access Level: Read Only

Rx-jabber-frames

SNMP MIB: **`fwuHstSERFEthPortRxJabbersFrames`**

Description: Receive jabber counter

Syntax: Counter64

Access Level: Read Only

Tx-byte-counter

SNMP MIB: **`fwuHstSERFEthPortTxByteCounter`**

Description: Transmit byte counter

Syntax: Counter64

Access Level: Read Only

Tx-packets

SNMP MIB: **`fwuHstSERFEthPortTxPkts`**

Description: Transmit packet counter

Syntax: Counter64

Access Level: Read Only

Tx-multicast-packets

SNMP MIB: **`fwuHstSERFEthPortTxMulticastPkts`**

Description: Transmit multicast packet counter

Syntax: Counter64

Access Level: Read Only

Tx-broadcast-packets

SNMP MIB: `fwuHstSERFEthPortTxBroadcastPkts`

Description: Transmit broadcast packet counter

Syntax: Counter64

Access Level: Read Only

Host SeRF FPGA Parameters

Status

SNMP MIB: `fwuHstSERFFPGAStatus`

Description: Gives the status if FPGA on SeRF Card

Values: 0 = PPC can talk to FPGA
1 = PPC cannot talk to FPGA

Default: 0

Syntax: Integer

Access Level: Read Only

Host List of Remotes Parameters

Monitor Index

SNMP MIB: `fwuHMmonIndex`

Description: Index of the Host mate monitor table

Syntax: Integer32

Access Level: Read Only

Remote ID

SNMP MIB: `fwuHMmonRmtID`

Description: ID (numerical) of companion Remote Unit

Values: See "Unit Identification" on page 43

Syntax: NodeAddr1

Access Level: Read Only

Remote IP Address

SNMP MIB: `fwuHMmonRmtIPAddress`

Description: List of IP addresses of connected Remote Unit(s)

Syntax: IpAddress

Access Level: Read Only

Host DART Module Parameters

Card Number

SNMP MIB:	`fwuHstDARTNumber`
Description:	A unique identifier for each DART Module Object
Values:	Range 1 - 8
Syntax:	Integer
Access Level:	Read Only

Card Name

SNMP MIB:	`fwuHstDARTName`
Description:	A user defined name for each DART Module
Values:	Alphanumeric Characters. Except as first character, the underscore (_) character is allowed. Must be between 5 and 32 characters in length, with no spaces.
Description:	Unknown_DART
Syntax:	Display String
Access Level:	Read-Write

Band Type

SNMP MIB:	`fwuHstDARTBandType`
Description:	Band type of Host DART Module
Values:	See "Band Types" on page 235.
Default:	-1
Syntax:	BAND-TYPE
Access Level:	Read Only

Passband

SNMP MIB:	`fwuHstDARTPassBand`
Description:	Passband for the selected DART
Values:	SIZE (0...40)
Default:	-1
Syntax:	OCTET STRING
Access Level:	Read-Write

Operating Mode

SNMP MIB:	`fwuHstDARTOperatingMode`
Description:	Operating mode of the DART Module
Syntax:	ModeType
Access Level:	Read-Write

Diversity Status

SNMP MIB: **fwuHstDARTDiversityStatus**

Description: Diversity Status of Host DART Module

Values: 0 = Non-diversity
                  1 = Diversity

Default: 0

Syntax: Integer

Access Level: Read Only

Forward Gain

SNMP MIB: **fwuHstDARTForwardGain**

Description: Primary Gain of Host DART Module

Default: 0

Syntax: GainType

Access Level: Read-Write

Reverse Gain

SNMP MIB: **fwuHstDARTReverseGain**

Description: Primary Gain of Host DART Module

Values: 5...36, Units = dB, increments 1dB

Default: 0

Syntax: GainType

Access Level: Read-Write

FPGA Status

SNMP MIB: **fwuHstDARTFPGAStatus**

Description: Host DART FPGA Status; indicates whether the SeRF FPGA can talk to the DART FPGA

Values: 0 = SeRF FPGA can talk to DART FPGA
                  1 = SeRF FPGA cannot talk to DART FPGA

Default: 0

Syntax: Integer

Access Level: Read Only

FPGA Program Version

SNMP MIB: **fwuHstDARTFPGAProgramVer**

Description: FPGA version on the DART Module

Syntax: Display String

Access Level: Read Only

RI ADC Part Number

SNMP MIB: `fwuHstDARTRIADCPartNumber`

Description: Host DART Inventory Data - ADC Part Number

Syntax: Display String

Access Level: Read Only

RI Serial Number

SNMP MIB: `fwuHstDARTRISerialNumber`

Description: Host DART Inventory Data - Serial Number

Syntax: Display String

Access Level: Read Only

RI Date Code

SNMP MIB: `fwuHstDARTRIDateCode`

Description: Host DART Inventory Data Code

Syntax: Display String

Access Level: Read Only

DART RI HW Version

SNMP MIB: `fwuHstDARTRIHWVer`

Description: Host DART Inventory Data - HW Version

Syntax: Display String

Access Level: Read Only

Row Status

SNMP MIB: `fwuHstDARTRowStatus`

Description: The status of this conceptual row

Syntax: RowStatus

Access Level: Read-Create

Peak Average Input Power Level 1

SNMP MIB: `fwuHstDARTPeakInputPwrLvl1`

Description: Peak Average input Power Level1. For Diversity systems, this will be NA.

Default: NA

Syntax: DisplayString

Access Level: Read Only

Peak Average Input Power Level 2

SNMP MIB: `fwuHstDARTPeakInputPwrLvl2`

Description: Peak Average input Power level2. For Diversity systems, this will be NA.

Default: NA

Syntax: DisplayString

Access Level: Read Only

Min Average Input Power Level 1

SNMP MIB: `fwuHstDARTPeakAvgInputPwrLvl1`

Description: Minimum Average Input Power Level1. For Diversity systems, this will be NA.

Default: NA

Syntax: DisplayString

Access Level: Read Only

Min Average Input Power Level 2

SNMP MIB: `fwuHstDARTPeakAvgInputPwrLvl2`

Description: Minimum Average Input Power Level2. For Diversity systems, this will be NA.

Default: NA

Syntax: DisplayString

Access Level: Read Only

Peak Input Power Level 1

SNMP MIB: `fwuHstDARTMinAvgInputPwrLvl1`

Description: Peak Input Power Level2. For Diversity systems, this will be NA.

Default: NA

Syntax: DisplayString

Access Level: Read Only

Peak Input Power Level 2

SNMP MIB: `fwuHstDARTMinAvgInputPwrLvl2`

Description: Peak Input Power Level2. For Diversity systems, this will be NA.

Default: NA

Syntax: DisplayString

Access Level: Read Only

Power Level Mode

SNMP MIB: `fwuHstDARTInputPowerMode`

Description: DART power level Mode

Values: 0 = snapshot
                   1 = maxHold

Default: 0

Syntax: Integer

Access Level: Read-Write

Power Level Max Hold Reset

SNMP MIB: `fwuHstDARTPwrLevelMaxHoldReset`

Description: Host DART Input Power Level Max Hold Reset

Values: -1 = Not Applicable
                   0 = Normal
                   1 = Reset

Default: -1

Syntax: Integer

Access Level: Read-Write

Last Max Hold Reset Time

SNMP MIB: `fwuHstDARTLastMaxHoldResetTime`

Description: Date and Time of the last maxHold reset time of the Host DART

Syntax: DateAndTime

Access Level: Read Only

Identify RF Source

SNMP MIB: `fwuHstDARTInputSrc`

Description: Identifies whether the connection is to BTS/BDA

Values: 1 = BTS
                   2 = BDA

Default: 1

Syntax: Integer

Access Level: Read-Write

Host System Card Parameters

RI ADC Part Number

SNMP MIB: `fwuHstSysCardRIADCPartNumber`

Description: Rmt Inventory Data - ADC Part Number

Syntax: Display String

Access Level: Read Only

RI Serial Number

SNMP MIB: **`fwuHstSysCardRISerialNumber`**

Description: Rmt Inventory Data - Serial Number

Syntax: Display String

Access Level: Read Only

RI Date Code

SNMP MIB: **`fwuHstSysCardRIDateCode`**

Description: Rmt Inventory Data - Date Code

Syntax: Display String

Access Level: Read Only

RI HW Version

SNMP MIB: **`fwuHstSysCardRIHWVer`**

Description: Rmt Inventory Data - Hardware Version

Syntax: Display String

Access Level: Read Only

10 MHz Reference Clock

SNMP MIB: **`fwuHstSysCard10MhzRefClock`**

Description: System Card Reference clock

Values: 0-Internal
1-external ref clock

Default: 0

Syntax: Integer

Access Level: Read-Write

Clock Priority Level

SNMP MIB: **`fwuHstSysCardCPLevel`**

Description: System card master clock priority level

Values: 1...14

Default: 14

Syntax: Integer32

Access Level: Read-Write

Output Reference Clock

SNMP MIB: **`fwuHstSysCardOutputRefClock`**

Description: System Card Reference clock. System Module supports only 10 MHz and System Board II supports both 10 MHz and 30 MHz Clock output.

Values: 0 = Off
1 = 10 MHz clock
2 = 30 MHz clock

Default: 1 for Host
2 for IF Remote

Syntax: Integer

Access Level: Read-Write

RI Hardware Generation

SNMP MIB: **`fwuHstSysCardRIHWGen`**

Description: Host System Card Hardware Generation

Values: 0 = First Generation
1 = Second Generation

Default: 1

Syntax: Integer

Access Level: Read Only

Remote Unit Parameters

Remote Parameters

Number

SNMP MIB: **`fwuRmtNumber`**

Description: Number of the connected Remote Unit.

Values: See "Unit Identification" on page 43

Syntax: UnitId2

Access Level: Read Only

Name

SNMP MIB: **`fwuRmtName`**

Description: User defined name of the Remote Unit.

Values: Alphanumeric Characters. Except as first character, the underscore (_) character is allowed. Must be between 5 and 40 characters in length, with no spaces.

Syntax: Display String

Access Level: Read-Write

Alarm Status Summary

SNMP MIB: `fwuRmtAlarmStatusSummary`

Description: Summary of alarm status of the (connected) Remote Unit.

Syntax: AlarmType

Access Level: Read Only

Type

SNMP MIB: `fwuRmtType`

Description: Type of Remote.

Syntax: unitType

Access Level: Read Only

Temperature Measurement

SNMP MIB: `fwuRmtTempMeasurement`

Description: Temperature of each Remote Unit in celsius.

Syntax: Octal String

Access Level: Read Only

Prism Unit Reset

SNMP MIB: `fwuPrismUnitReset`

Description: Boolean. Way to reset the Remote Unit remotely. Only applicable to URH Remote Units (URUs).

Values: 0 = Normal
1 = Reset

Default: Default: 0

Syntax: Integer

Access Level: Read-Write

Catalog State

SNMP MIB: `fwuRmtCatalogState`

Description: Catalog state of Remote Unit.

Values: This is used in the Recovery of the Remote Unit

Syntax: CatalogType

Access Level: Read Only

Table Row Status

SNMP MIB: `fwuRmtGeneralTableRowStatus`

Description: The status of this conceptual row.

Syntax: RowStatus

Access Level: Read-Create

DART Id

SNMP MIB: **`fwuUsrCommLinkTestDartId`**

Description: To identify the DART

Values: 1 - 8

Syntax: Unsigned32

Access Level: Read-Write

Prism Remote System Card

RI ADC Part Number

SNMP MIB: **`fwuRmtSysCardRIADCPartNumber`**

Description: Remote Unit Inventory Data: ADC Part Number.

Syntax: Display String

Access Level: Read Only

RI Serial Number

SNMP MIB: **`fwuRmtSysCardRISerialNumber`**

Description: Remote Unit Inventory Data: Serial Number

Syntax: Display String

Access Level: Read Only

RI Date Code

SNMP MIB: **`fwuRmtSysCardRIDateCode`**

Description: Remote Unit Inventory Data: DateCode Number

Syntax: Display String

Access Level: Read Only

RI Hardware Version

SNMP MIB: **`fwuRmtSysCardRIHWVersion`**

Description: Rmt Inventory Data - Hardware Number

Syntax: Display String

Access Level: Read Only

10 Mhz Reference Clock

SNMP MIB: **`fwuRmtSysCard10MhzRefClock`**

Description: Remote System Card Reference clock. It can be internal or external.

Values: 0-Internal
1-external ref clock

Description: 0

Syntax: Integer

Access Level: Read Only

Output Reference Clock

SNMP MIB: `fwuRmtSysCardOutputRefClock`

Description: Remote System Card Reference clock. System Board supports only 10 MHz and System Board II supports both 10 MHz and 30 MHz Clock output

Values: 0 - off
1 - clock10mhz
2 - clock30mhz

Default: 2

Syntax: Integer

Access Level: Read-Write

RI Hardware Gen

SNMP MIB: `fwuRmtSysCardRIHWGen`

Description: Remote System Card Hardware Generation

Values: First Generation = 0
Second Generation = 1

Syntax: Integer

Access Level: Read Only

Prism Remote SeRF General

Linux Kernel Version

SNMP MIB: `fwuRmtSERFLinuxKernelVer`

Description: Linux Kernel Version of the remote system.

Syntax: Display String

Access Level: Read Only

Linux BootLoader Version

SNMP MIB: `fwuRmtSERFLinuxBootLoaderVer`

Description: Linux Boot loader Version of the remote system.

Syntax: Display String

Access Level: Read Only

Linux First Stage Boot Loader Version

SNMP MIB: `fwuRmtSERFLinuxBootLoaderVer`

Description: Boot Loader1 Version of the host system.

Syntax: Display String

Access Level: Read Only

Compact Flash SW Version

SNMP MIB: **`fwuRmtSERFCompactFlashSWVer`**

Description: Compact Flash Software Version of the remote system.

Values: Format of: **`aa.bb.cc.dd`**
where each of **`aa`**, **`bb`**, **`cc`**, **`dd`** must be between 00 and 99

Syntax: Display String

Access Level: Read Only

PPC HW Monitor SW Version

SNMP MIB: **`fwuRmtSERFPPCHWMonSWVer`**

Description: Hardware monitor process Software Version of the remote system.

Syntax: Display String

Access Level: Read Only

PPC Application Monitor SW Version

SNMP MIB: **`fwuRmtSERFPPCAPPMonSWVer`**

Description: Application monitor process Software Version of the remote system.

Syntax: Display String

Access Level: Read Only

PPC Agent SW Version

SNMP MIB: **`fwuRmtSERFPPCSNMPAgentSWVer`**

Description: SNMP agent Software Version of the remote system.

Syntax: Display String

Access Level: Read Only

PPC Mate Monitor SW Version

SNMP MIB: **`fwuRmtSERFPPCMATEMonSWVer`**

Description: Mate monitor process Software Version of the remote system.

Syntax: Display String

Access Level: Read Only

PPC ENET Monitor SW Version

SNMP MIB: **`fwuRmtSERFPPCENETMonSWVer`**

Description: ENET monitor process Software Version of the remote system.

Syntax: Display String

Access Level: Read Only

PPC FPGA Monitor SW Version

SNMP MIB: **`fwuRmtSERFPPCFPGAMonSWVer`**

Description: FPGA monitor process Software Version of the remote system.

Syntax: Display String

Access Level: Read Only

SeRF FPGA Version

SNMP MIB: `fwuRmtSERFFPGAVer`

Syntax: Display String

Access Level: Read Only

RI ADC Part Number

SNMP MIB: `fwuRmtSERFRIADCPartNumber`

Description: Remote SeRF Inventory - ADC Part Number.

Syntax: Display String

Access Level: Read Only

pThread Software Version

SNMP MIB: `fwuRmtpThreadSoftwareVer`

Description: The version number of pThread process.

Syntax: DisplayString

Access Level: Read Only

Web Server Software Version

SNMP MIB: `fwuRmtWebServerSwVer`

Description: The version number of web server.

Syntax: DisplayString

Access Level: Read Only

RI Hardware Version

SNMP MIB: `fwuRmtSERFPPCHWMonSWVer`

Description: Hardware monitor process Software Version of the remote system.

Syntax: DisplayString

Access Level: Read Only

RI Hardware

SNMP MIB: `fwuRmtSERFRIHWGen`

Description: Remote SeRF Hardware Generation.

Values: First Generation = 0
Second Generation = 1

Syntax: Integer

Access Level: Read Only

Prism Remote SeRF Optics

Optics Number

SNMP MIB: `fwuRmtSERFOptSFPNumber`
Description: A unique identifier of each SFP
Values: 1 - 8
Syntax: Integer
Access Level: Read Only

Optics Name

SNMP MIB: `fwuRmtSERFOptSFPName`
Description: User defined name of each Remote SFP.
Values: Alphanumeric Characters. Except as first character, the underscore (_) character is allowed. Must be between 5 and 32 characters with no spaces.
Syntax: Display String
Access Level: Read- Write

Optics Type

SNMP MIB: `fwuRmtSERFOptSFPType`
Description: SFP Type - Optical Port Type.
Syntax: OpticsType
Access Level: Read Only

Optics Color

SNMP MIB: `fwuRmtSERFOptSFPColor`
Description: SFP wavelength in nanometer.
Values: Integer32
Syntax: Read Only

REV Launch Power

SNMP MIB: `fwuRmtSERFOptRevLaunchPowerMeas`
Description: Value of Remote Receive measured optical power in dbm .
Syntax: Display String
Access Level: Read Only

Forward Receive Power

SNMP MIB: `fwuRmtSERFOptFwdLaunchPowerMeas`
Description: Value of Remote Transmit measured optical power in dbm.
Syntax: Display String
Access Level: Read Only

Mate Name

SNMP MIB: `fwuRmtSERFOptMateName`

Description: Name of Remote mate.

Values: Inherits valid values from Remote name

Syntax: DisplayString

Access Level: Read Only

Mate Unit ID

SNMP MIB: `fwuRmtSERFOptMateId`

Description: Numerical ID of companion Remote Unit.

Values: See "Unit Identification" on page 43

Syntax: NodeAddr1

Access Level: Read Only

Mate Unit SFP ID

SNMP MIB: `fwuRmtSERFOptMateSfpId`

Description: Identifier of SFP to which the mate connects .

Values: 1 - 8

Syntax: Integer32

Access Level: Read Only

Mode

SNMP MIB: `fwuRmtSERFIPEnable`

Description: Mode of IP enable RF carrier.

Values: 1= IPEnable
2 = IP Disable

Default: 2

Syntax: Integer

Access Level: Read- Write

SFP Direction

SNMP MIB: `fwuRmtSERFOptMateSfpDir`

Description: Indicates whether the fiber is incoming or outgoing on this SFP port.

Values: -1 = Unknown
0 = In
1 = Out

Syntax: Integer

Access Level: Read Only

Prism Remote SeRF ENET Switch

Ethernet Port Number

SNMP MIB: `fwuRmtSERFEthPortNumber`

Description: A unique identifier for each Ethernet port.

Values: Port number, which can be between 1 and 12

Syntax: Unsigned32

Access Level: Read Only

Ethernet Port Type

SNMP MIB: `fwuRmtSERFEthPortType`

Description: An identifier for the type of Ethernet port.

Values: Port type:
Network port
Craft port
Management port
Switch port

Syntax: ENET-TYPE

Access Level: Read Only

Ethernet SFP Id

SNMP MIB: `fwuRmtSERFEthSFPID`

Description: Identifier of SFP to which this ethernet port connects to.

Syntax: Integer32

Access Level: Read Only

Rx-bytes

SNMP MIB: `fwuRmtSERFEthPortRxBytes`

Description: Receive byte counter.

Syntax: Counter64

Access Level: Read Only

Rx-packets

SNMP MIB: `fwuRmtSERFEthPortRxPkts`

Description: Receive packet counter.

Syntax: Counter64

Access Level: Read Only

Rx-fsc-errors

SNMP MIB: `fwuRmtSERFEthPortRxFscErrors`

Description: Receive FCS error counter.

Syntax: Counter64

Access Level: Read Only

Receive-multicast-packets

SNMP MIB: `fwuRmtSERFEthPortRxMulticastPkts`

Description: Receive multicast packet counter.

Syntax: Counter64

Access Level: Read Only

Receive-broadcast-packets

SNMP MIB: `fwuRmtSERFEthPortRxBroadcastPkts`

Description: Receive broadcast packet counter.

Syntax: Counter64

Access Level: Read Only

Rx-fragmented-frames

SNMP MIB: `fwuRmtSERFEthPortRxFragmtdFrames`

Description: Receive fragments counter.

Syntax: Counter64

Access Level: Read Only

Rx-jabber-frames

SNMP MIB: `fwuRmtSERFEthPortRxJabbersFrames`

Description: Receive jabber counter.

Syntax: Counter64

Access Level: Read Only

Tx-byte-counter

SNMP MIB: `fwuRmtSERFEthPortTxByteCounter`

Description: Transmit byte counter

Syntax: Counter64

Access Level: Read Only

Tx-packets

SNMP MIB: `fwuRmtSERFEthPortTxPkts`

Description: Transmit packet counter

Syntax: Counter64

Access Level: Read Only

Tx-multicast-packets

SNMP MIB: `fwuRmtSERFEthPortTxMulticastPkt`

Description: Transmit multicast packet counter

Syntax: Counter64

Access Level: Read Only

Tx-broadcast-packets

SNMP MIB: `fwuRmtSERFEthPortTxBroadcastPkts`

Description: Transmit broadcast packet counter

Syntax: Counter64

Access Level: Read Only

Prism Remote SeRF FPGA

FPGA Status

SNMP MIB: `fwuRmtSERFFPGAStatus`

Description: Remote SeRF Card FPGA status.

Values: 0 = PPC can talk to FPGA
1= PPC cannot talk to FPGA

Default: 0

Syntax: Integer

Access Level: Read Only

Prism Remote DART

Card Number

SNMP MIB: `fwuRmtDARTNumber`

Description: A unique identifier for each DART Module Object.

Values: 1 - 8

Syntax: Unsigned32

Access Level: Read Only

Name

SNMP MIB: `fwuRmtDARTName`

Description: A user defined name for each DART Module.

Values: Alphanumeric Characters. Except as first character, the underscore (_) character is allowed. Must be between 5 and 32 characters in length, with no spaces.

Default: Unknown_DART

Syntax: DisplayString

Access Level: Read-Write

Band Type

SNMP MIB: `fwuRmtDARTBandType`

Description: Band type of the Host DART

Values: See "Band Types" on page 235.

Default: -1

Syntax: BandType

Access Level: Read Only

Passband

SNMP MIB:	`fwuRmtDARTPassBand`
Description:	Passband for the selected DART
Values:	Size of the passband, which can be between 0 and 40
Default:	-1
Syntax:	Octet String
Access Level:	Read-Write

Operating Mode

SNMP MIB:	`fwuRmtDARTOperatingMode`
Description:	Operating mode of the DART Module.
Default:	1
Syntax:	ModeType
Access Level:	Read-Write

Diversity Status

SNMP MIB:	`fwuRmtDARTDiversityStatus`
Description:	Diversity Status of Host DART Module.
Values:	1 = Diversity 0 = Non-diversity
Default:	0
Syntax:	Integer
Access Level:	Read-Write

Forward Gain

SNMP MIB:	`fwuRmtDARTForwardGain`
Description:	Primary Gain in forward path of Remote Unit DART Module.
Default:	0
Syntax:	GainType
Access Level:	Read-Write

Reverse Gain

SNMP MIB:	`fwuRmtDARTReverseGain`
Description:	Primary Gain in reverse path of Remote Unit DART Module.
Default:	0
Syntax:	GainType
Access Level:	Read Only

Forward Delay

SNMP MIB:	`fwuRmtDARTForwardDelay`
Description:	Remote DART Module forward delay in Micro Seconds.
Syntax:	DelayType
Access Level:	Read-Write

Reverse Delay

SNMP MIB: `fwuRmtDARTReverseDelay`

Description: Remote DART Module reverse delay in Micro Seconds

Syntax: DelayType

Access Level: Read-Write

FPGA Program Version

SNMP MIB: `fwuRmtDARTFPGAProgramVer`

Description: FPGA Version on the Remote Unit DART Module.

Syntax: DisplayString

Access Level: Read Only

FPGA Status

SNMP MIB: `fwuRmtDARTFPGAStatus`

Description: Remote DART FPGA Status. It indicates if the SeRF FPGA can talk to DART FPGA or not.

Values: 0 = SeRF FPGA can talk to DART FPGA
1 = SeRF FPGA cannot talk to DART FPGA

Default: 0

Syntax: Integer

Access Level: Read Only

Temperature Measurement

SNMP MIB: `fwuRmtDARTTempMeas`

Description: Temperature of Remote DART Module.

Syntax: DisplayString

Access Level: Read Only

ADC Part Number

SNMP MIB: `fwuRmtDARTRIADCPartNumber`

Description: Remote DART Inventory Data - ADC Part Number.

Syntax: Display String

Access Level: Read Only

Serial Number

SNMP MIB: `fwuRmtDARTRISerialNumber`

Description: Remote DART Inventory Data - Serial Number.

Syntax: Display String

Access Level: Read Only

Date Code

SNMP MIB: `fwuRmtDARTRIDateCode`
Description: Remote DART Inventory Data - DateCode.
Syntax: Display String
Access Level: Read Only

RI Hardware Version

SNMP MIB: `fwuRmtDARTRIHWVer`
Description: Remote DART Inventory Data - HW Version.
Syntax: Display String
Access Level: Read Only

Table Row Status

SNMP MIB: `fwuRmtDARTGeneralTableRowStatus`
Description: The status of this conceptual row.
Syntax: RowStatus
Access Level: Read-Create

Actual Forward Delay

SNMP MIB: `fwuRmtDARTActualForwardDelay`
Description: Actual value of Forward delay for Remote DART.
Syntax: Integer32
Access Level: Read Only

Forward Delay - Lower Bound

SNMP MIB: `fwuRmtDARTForwardLowerboundDelay`
Description: Lower bound of Forward delay for Remote DART
Syntax: Integer32
Access Level: Read Only

Forward Delay - Upper Bound

SNMP MIB: `fwuRmtDARTForwardUpperboundDelay`
Description: Upper bound of Forward delay for Remote DART.
Syntax: Integer32
Access Level: Read Only

Remote DART Actual Reverse Delay

SNMP MIB: `fwuRmtDARTActualReverseDelay`
Description: Reverse delay for Remote DART.
Syntax: Integer32
Access Level: Read Only

Reverse Delay - Lower Bound

SNMP MIB: **fwuRmtDARTReverseLowerboundDelay**

Description: Lower bound of Reverse delay for Remote DART

Syntax: Integer32

Access Level: Read Only

Reverse Delay - Upper Bound

SNMP MIB: **fwuRmtDARTReverseUpperboundDelay**

Description: Upper bound of Reverse delay for Remote DART

Syntax: Integer32

Access Level: Read Only

Peak Input Power Level1

SNMP MIB: **fwuRmtDARTPeakInputPwrLvl1**

Description: Peak Input Power Level1 to a Remote DART.

Default: NA

Syntax: DisplayString

Access Level: Read Only

Peak Input Power Level2

SNMP MIB: **fwuRmtDARTPeakInputPwrLvl2**

Description: Peak Input Power Level2 to a Remote DART.

Default: NA

Syntax: DisplayString

Access Level: Read Only

Peak Average Input Power Level 1

SNMP MIB: **fwuRmtDARTPeakAvgInputPwrLvl1**

Description: Peak Average Input Power Level1 to a Remote DART.

Default: NA

Syntax: DisplayString

Access Level: Read Only

Peak Average Input Power Level 2

SNMP MIB: **fwuRmtDARTPeakAvgInputPwrLvl2**

Description: Peak Average Input Power Level2 to a Remote DART.

Default: NA

Syntax: DisplayString

Access Level: Read Only

Minimum Average Input Power Level 1

SNMP MIB: `fwuRmtDARTMinAvgInputPwrLvl1`

Description: Minimum Average Input Power Level1 to a Remote DART.

Default: NA

Syntax: DisplayString

Access Level: Read Only

Minimum Average Input Power Level 2

SNMP MIB: `fwuRmtDARTMinAvgInputPwrLvl2`

Description: Minimum Average Input Power Level2 to a Remote DART.

Default: NA

Syntax: DisplayString

Access Level: Read Only

Power Level Mode

SNMP MIB: `fwuRmtDARTInputPowerMode`

Description: Remote DART Input Power Level Mode.

Values: 0 = Snap Shot
                 1 = Max Hold

Default: 0

Syntax: Integer

Access Level: Read-Write

Power Level Max Hold Reset

SNMP MIB: `fwuRmtDARTPwrLevelMaxHoldReset`

Description: Resets the Power Level Max Hold

Values: -1 = Not Applicable
                 0 = normal
                 1 = reset

Default: -1

Syntax: Integer

Access Level: Read-Write

Last Max Hold Reset Time

SNMP MIB: `fwuRmtDARTLastMaxHoldResetTime`

Description: Date and Time of the last maxHold reset time of Remote.

Syntax: DisplayString

Access Level: Read Only

Reverse Path Gain Mode

SNMP MIB: `fwuRmtDARTReverseGainMode`

Description: To control gain mode on the Reverse Path. Applicable to both Classic and Super DARTs.

Values: 0 - Normal
1 - High

Default: 0

Syntax: Integer

Access Level: Read-Write

Prism Remote LPA

LPA Number

SNMP MIB: `fwuRmtLPANumber`

Description: A unique identifier for an LPA.

Values: 1 - 4

Syntax: Unsigned32

Access Level: Read Only

LPA Reset

SNMP MIB: `fwuRmtLPAReset`

Description: Set this object to a value of 1 to cause LPA to reset itself.

Values: 0 = normal
1 = reset

Default: 0

Syntax: Integer

Access Level: Read-Write

Operating Mode

SNMP MIB: `fwuRmtLPAOpState`

Description: The operating modes of Remote Unit LPA

Values: 0 = Operating
1 = Offline

Default: 1

Syntax: Integer

Access Level: Read Only

LPA Control

SNMP MIB: `fwuRmtLPAControl`

Description: To control the operating mode of Remote Unit LPA.

Values: 0 = Normal
1 = Standby

Default: 1

Syntax: Integer

Access Level: Read-Write

Model Number

SNMP MIB: `fwuRmtLPAPartNum`

Description: Remote LPA Part Number.

Syntax: DisplayString

Access Level: Read Only

Serial Number

SNMP MIB: `fwuRmtLPASerialNum`

Description: Remote LPA Serial Number.

Syntax: DisplayString

Access Level: Read Only

Hardware Version

SNMP MIB: `fwuRmtLPAHWVer`

Description: Remote LPA Hardware Version.

Syntax: DisplayString

Access Level: Read Only

Software Version

SNMP MIB: `fwuRmtLPASWVer`

Description: Remote LPA Software Version.

Syntax: DisplayString

Access Level: Read Only

Description

SNMP MIB: `fwuRmtLPADescr`

Description: Band type of Remote LPA

Syntax: DisplayString

Access Level: Read Only

Prism Remote Power Detector

Power Detector Number

SNMP MIB: `fwuRmtPowerDetectorNumber`

Description: Index and a unique identifier for each power detector.

Values: 1 - 4

Syntax: Integer32

Access Level: Read Only

RF Power Output Measurement

SNMP MIB: `fwuRmtRFPowerOutputMeas`

Description: The value of Remote RF Power Output in dBm

Values: Up to 5 characters

Syntax: Octet String

Access Level: Read Only

Duplexer RI Serial Number

SNMP MIB: `fwuRmtPwrDetectorBoardRISerialNum`

Description: Power Detector Inventory - Serial Number.

Syntax: DisplayString

Access Level: Read Only

Duplexer RI Date Code

SNMP MIB: `fwuRmtPwrDetectorBoardRIDateCode`

Description: Power Detector Inventory - Date Code.

Syntax: DisplayString

Access Level: Read Only

Duplexer RI Hardware Version

SNMP MIB: `fwuRmtPwrDetectorBoardRIHWVer`

Description: Power Detector Inventory - HW Version.

Values: Up to 8 Characters

Syntax: Octet String

Access Level: Read Only

Duplexer RI ADC Part Number

SNMP MIB: `fwuRmtPwrDetectorBoardRIADCPartNum`

Description: Power Detector Inventory - ADC Part Number.

Syntax: DisplayString

Access Level: Read Only

System VSWR Measurement

SNMP MIB: `fwuRmtSystemVswrMeas`

Description: Measured VSWR value

Values: Up to 8 Characters

Syntax: Octet String

Access Level: Read Only

Prism Remote LNA/Duplexer

LNA Number

SNMP MIB: `fwuRmtLNANumber`

Description: Index and an unique identifier for LNA Objects.

Values: Number that identifies an LNA and that can be from 1 to 8

Syntax: Integer32

Access Level: Read Only

LNA Type

SNMP MIB: `fwuRmtLNAType`

Description: Remote LNA card type.

Syntax: LnaType

Access Level: Read Only

RI ADC Part Number

SNMP MIB: `fwuRmtLNARIADCPartNumber`

Description: LNA Inventory Data - ADC Part Number.

Syntax: Display String

Access Level: Read Only

RI Serial Number

SNMP MIB: `fwuRmtLNARISerialNumber`

Description: LNA Inventory Data - Serial Number.

Syntax: Display String

Access Level: Read Only

RI Date Code

SNMP MIB: `fwuRmtLNARIDateCode`

Description: LNA Inventory Data - Date Code.

Syntax: Display String

Access Level: Read Only

RI Hardware Version

SNMP MIB: `fwuRmtLNARIHWVer`

Description: LNA Inventory Data - HW Version.

Syntax: DisplayString

Access Level: Read Only

Duplexer type

SNMP MIB: `fwuRmtDuplexerType`

Description: Duplexer hardware type.

Syntax: DuplexerType

Access Level: Read Only

Prism Remote RDI Card

RDI Number

SNMP MIB: `fwuRmtRDINumber`

Description: Index and an identifier for each RDI.

Values: Number that identifies an RDI and that can be from 1 to 4

Syntax: Unsigned32

Access Level: Read Only

RI ADC Part Number

SNMP MIB: `fwuRmtRDIRIADCPartNumber`

Description: RDI Inventory Data - ADC Part Number.

Syntax: Display String

Access Level: Read Only

RI Serial Number

SNMP MIB: `fwuRmtRDIRISerialNumber`

Description: RDI Inventory Data - Serial Number.

Syntax: Display String

Access Level: Read Only

RI DateCode

SNMP MIB: `fwuRmtRDIRIDateCode`

Description: RDI Inventory Data - Date Code.

Syntax: DisplayString

Access Level: Read Only

RI Hardware Version

SNMP MIB: `fwuRmtRDIRIHWVer`

Description: RDI Inventory Data - HW Version.

Syntax: Display String

Access Level: Read Only

Prism Remote RSI Card

RI ADC Part Number

SNMP MIB: `fwuRmtRSIRIADCPartNumber`

Description: Remote Inventory Data - ADC Part Number.

Syntax: Display String

Access Level: Read Only

Serial Number

SNMP MIB: `fwuRmtRSIRISerialNumber`

Description: Remote Inventory Data - Serial Number.

Syntax: Display String

Access Level: Read Only

Date Code

SNMP MIB: `fwuRmtRSIRIDateCode`

Description: Remote Inventory Data - Date Code.

Syntax: DisplayString

Access Level: Read Only

RI Hardware Version

SNMP MIB: `fwuRmtRSIRIHWVer`

Description: Remote Inventory Data - Hardware Version.

Syntax: Display String

Access Level: Read Only

Remote Capacity

SNMP MIB: `fwuRmtCapacity`

Description: The number of RF modules that may be installed in the Remote Unit.

Values: Number between 1 and 4

Default: 1

Syntax: Unsigned32

Access Level: Read Only

Common Managed Objects

Prism DART Mapping

Index

SNMP MIB: `fwuDARTMappingIndex`

Description: Index of DART Mapping Table.

Values: Number between 0 and 100

Syntax: Unsigned32

Access Level: Not Accessible

Unit Id

SNMP MIB: `fwuUnitID`

Description: Identifier for the unit

Syntax: HOSTNBR-TYPE

Access Level: Read Only

Unit DART Id

SNMP MIB: `fwuUnitDARTID`

Description: Identifier of DART on the unit

Values: Numerical value that can be from 1 to 8

Syntax: Integer32

Access Level: Read Only

Unit SFP Id

SNMP MIB: `fwuUnitSFPID`

Description: Identifier of unit SFP connected toward the mate DART (outgoing).

Values: Numerical value that can be from 1 to 8

Syntax: Integer32

Access Level: Read Only

Unit DART Passband

SNMP MIB: `fwuUnitDartPassBand`

Description: Band-Passband information of the linked DART on the Host side.

Values: Numerical value that indicates size, and that can be from 0 to 40

Syntax: OCTET STRING

Access Level: Read Only

Mate Id

SNMP MIB: `fwuMateID`

Description: Identifier of (companion) mate unit

Values: See "Unit Identification" on page 43

Syntax: REMOTENBR-TYPE

Access Level: Read Only

Mate DART Id

SNMP MIB: `fwuMateDARTId`

Description: Identifier of (companion) DART on mate unit.

Syntax: Integer32

Access Level: Read Only

Mate SFP Id

SNMP MIB: `fwuMateSFPId`

Description: Identifier of remote side SFP connected toward the unit DART (incoming)

Syntax: Integer32

Access Level: Read Only

Mate DART Passband

SNMP MIB: `fwuMateDartPassbnd`

Description: Band-Passband information of the linked DART on the Mate side.

Syntax: OCTET STRING

Access Level: Read Only

Start Time Slot on SFP

SNMP MIB: `fwuSfpStartTimeSlot`

Description: Starting time slot on the fiber that is carrying the RF traffic from unit to mate DART Module.

Values: 1-12

Syntax: Integer32

Access Level: Read Only

End Time Slot on SFP

SNMP MIB: `fwuSfpEndTimeSlot`

Description: Ending timeslot on the fiber that is carrying the RF traffic from unit to mate DART Module.

Values: 1-12

Syntax: Integer32

Access Level: Read Only

Mapping Status

SNMP MIB: `fwuMappingStatus`

Description: Status of DART mapping table

Syntax: RowStatus

Access Level: Set

Schedule System Link Test

System Link Test Mode

SNMP MIB: `sysLinkTestMode`

Description: RLM Test for System.

Values: 0 = Disable
1 = Enable

Syntax: INTEGER

Access Level: Read-Write

Start Date and Time

SNMP MIB: `sysLinkStartTime`

Description: The Start date and time of linking test execution.

Syntax: DateAndTime

Access Level: Read-Write

Recurrence Time

SNMP MIB: `sysLinkRecurrenceTime`

Description: Recurrence of system link test, in terms of days.

Values: 1 - 365
0 = don't recur

Syntax: Unsigned32

Access Level: Read-Write

DART Band Type

SNMP MIB: `sysLinkDARTBandType`

Description: Band type (the RF DART type) of selected units

Values: See "Band Types" on page 235.
Enter **0** to select all units.

Syntax: BandType

Access Level: Read-Write

DART Id

SNMP MIB: `fwuSchLinkTestDartId`

Description: In which slot the DART resides.

Values: 1 - 8

Syntax: Integer

Access Level: Read-Write

SNMP Settings

V1 Trap Agent Address Override Mode

SNMP MIB: `fwuV1TrapAgentAddrOverrideMode`

Description: V1 trap agent address override mode.

Values: 0 = Disable
1 = Enable

Default: 0

Syntax: INTEGER

Access Level: Read-Write

V1 Trap Agent Address Override IP Address

SNMP MIB: `fwuV1TrapAgentAddrOverrideIPAddr`

Description: V1 trap agent address overriding address

Syntax: DisplayString

Access Level: Read-Write

SNMP Trap Resend Interval

SNMP MIB: `fwuSnmpTrapResendInterval`

Description: Interval in minutes that must pass before the trap is resent

Values: 0 to 1440, where 0 = Disable

Syntax: Integer32

Access Level: Read-Write

Maximum for SNMP Trap Resend

SNMP MIB: `fwuSnmpTrapResendMaximum`

Description: Maximum number of times trap will be resent with   Disable = 0

Values: 0 to 360

Syntax: Integer32

Access Level: Read-Write

Ethernet Modem Wake Up

SNMP MIB: `fwuEthernetModemWakeUp`

Description: If an external modem is used, sends a "wake up" message

Values: 0 = False
1 = True

Syntax: Integer32

Access Level: Read-Write

Register SNMP Trap Manager

Row Index

SNMP MIB: `fwuTrapMgrRowId`

Description: Index for this table

Syntax: Integer

Access Level: Read-Write

Trap Manger IP Address

SNMP MIB: `fwuTrapMgrIpAddress`

Description: IP Address of the registered Trap manager

Values: Default = 127.0.0.1

Syntax: IpAddress

Access Level: Read-Write

Listening Port

SNMP MIB: `fwuTrapMgrListeningPort`

Description: Port at which the manager listens for the trap. This value must be set by the user before the row status is made active. Otherwise, an error will be indicated.

Values: 162, or any other unreserved port

Default: 162

Syntax: Integer

Access Level: Read-Write

Community

SNMP MIB: `fwuTrapCommunity`

Description: Trap Community for the manager

Values: Public
Private

Default: Public

Syntax: DisplayString

Access Level: Read-Write

Trap Version

SNMP MIB: `fwuTrapVersion`

Description: Version of SNMP used for this trap destination.

Values: 0 = V1
                          1 = V2c
                          2 = Inform

Default: 1

Syntax: Integer

Access Level: Read-Write

Row Status

SNMP MIB: `fwuTrapMgrRowStatus`

Description: The status of this conceptual row.

Syntax: RowStatus

Access Level: Read-Create

Geographic Locations

GEO Objects

Geo Heartbeat Timer

SNMP MIB: `fwuGeoHeartbeatTimer`

Description: Heartbeat can be sent at the timer specified here in minutes

Values: Number that represents minutes, that can be from 1 to 30

Default: 20

Syntax: Integer32

Access Level: Read Only

GEO Table Objects

Index

SNMP MIB: `fwuGeoIndex`

Description: Index of Geo table.

Values: Number that can be from 0 to 64

Syntax: Display String

Access Level: Read-Write

Geo Latitude

SNMP MIB: `fwuGeoLatitude`

Description: Identifies the Latitude of a Remote Unit.

Syntax: LatAndLong

Access Level: Read-Write

Geo Longitude

SNMP MIB: `fwuGeoLongitude`

Description: Identifies the Longitude of a Remote Unit.

Syntax: LatAndLong

Access Level: Read-Write

Geo Remote Name

SNMP MIB: `fwuGeoRmtName`

Description: Derived from `fwuRmtName`.

Syntax: Display String

Access Level: Read Only

Geo Status

SNMP MIB: `fwuGeoStatus`

Description: Standard SNMP row status for this table.

Values: 0 = not Present
1 = active
2 = inactive

Syntax: Integer

Access Level: Read Only

Managed Objects for Traps

Prism Input Contact Alarm Management Table

Unit Index

SNMP MIB: `fwuUnitIndex`

Description: The number of unit connected.

Values: See "Unit Identification" on page 43

Syntax: NodeAddr1

Access Level: Read Only

Alarm Code

SNMP MIB: `fwuSYstemAlarmCode`

Description: An alphanumeric code that uniquely identifies an alarm/fault.

Values: Each alarm/fault has a unique alphanumeric code. See "Troubleshooting Alarms" on page 185 or use the "Index of Alarms" on page 313 to find the page number for a specific alarm description, which includes the alarm code.

Syntax: Unsigned32

Access Level: Read Only

Contact Alarm

SNMP MIB: `fwuContactAlarm`

Description: Hardware Assigned Name

Syntax: Display String

Access Level: Read Only

Severity

SNMP MIB: `fwuContactAlarmSeverity`

Description: Severity of the alarm

Values: 2= Minor
3 = Major

Default: Minor

Syntax: Unsigned Integer

Access Level: Read-Write

Mode

SNMP MIB: `fwuContactAlarmMode`

Description: Mode of the Alarm

Values: 1=Normally Closed
2 = Normally Open

Default: 2

Syntax: Unsigned Integer

Access Level: Read-Write

Alarm Name

SNMP MIB: `fwuContactAlarmName`

Description: User Assigned Name

Values: Alphanumeric Characters. Except as first character, the underscore (_) character and spaces are allowed. Must be 5 to 40 characters in length.

Default: Blank (empty string)

Syntax: Display String

Access Level: Read-Write

Contact Alarm Enable

SNMP MIB: `fwuContactAlarmEnable`

Description: Enable/Disable the contact alarm

Values: 1 = Enabled
0 = Disabled

Default: Enabled

Syntax: Unsigned Integer

Access Level: Unsigned Integer

System Active Alarm Table

Alarm Sequence number

SNMP MIB: **fwuSystemAlarmSequenceNumber**

Description: Index and unique ID for each trap in AlarmTable.

Values: Index of the AlarmTable

Syntax: Unsigned32

Access Level: Not Accessible

Unit Node Address

SNMP MIB: **fwuSystemAlarmTrapNodeAddress**

Syntax: UnitId2

Access Level: Read-Write

System Label

SNMP MIB: **fwuSystemlabel**

Description: System Name or Host name

Syntax: DisplayString

Access Level: Read Only

Remote Name for Alarm

SNMP MIB: **fwuSystemAlarmRmtName**

Description: Remote name, where the alarm originated.

Syntax: DisplayString

Access Level: Read Only

Remote Type for Alarm

SNMP MIB: **fwuSystemAlarmRmtType**

Description: Identifies the type of the Remote (PRU or URU)

Syntax: UnitType

Access Level: Read Only

Module Type for Alarm

SNMP MIB: **fwuSystemAlarmModuleType**

Description: Hardware module type, where the alarm has originated like . SeRF, DART, SFP, LPA, LNA.

Syntax: ModuleType

Access Level: Read Only

Module Number for Alarm

SNMP MIB: `fwuSystemAlarmModuleNumber`

Description: Hardware module number, where the alarm has originated.

Values: Between 1 and 8

Syntax: Unsigned32

Access Level: Read Only

Module Name for Alarm

SNMP MIB: `fwuSystemAlarmModuleName`

Description: Name of hardware module where trap originated.

Syntax: DisplayString

Access Level: Read Only

Alarm Severity

SNMP MIB: `fwuSystemAlarmSeverity`

Description: Severity of the alarm

Syntax: AlarmType

Access Level: Read Only

Alarm Pass Band

SNMP MIB: `fwuSystemAlarmRFBand`

Description: Describes the Band that may be affected due the raised alarm PCS, GSM, AWS.

Syntax: DisplayString

Access Level: Read Only

Alarm Time

SNMP MIB: `fwuSystemAlarmTimeStamp`

Description: Time at trap in raised.

Syntax: SystemDateand Time

Access Level: Read Only

Alarm Code

SNMP MIB: `fwuSystemAlarmCode`

Description: An alphanumeric code that uniquely identifies an alarm/fault.

Values: Each alarm/fault has a unique alphanumeric code. See "Troubleshooting Alarms" on page 185 or use the "Index of Alarms" on page 313 to find the page number for a specific alarm description, which includes the alarm code.

Syntax: Unsigned32

Access Level: Read Only

Alarm Host Number

SNMP MIB: `SystemAlarmHstNbr`

Description: Number identifying the host in the system

Syntax: Unsigned32

Access Level: Read Only

Analog Node Address

SNMP MIB: `fwuSystemAlarmAnalogAddress`

Description: Analog Portion of the node address

Syntax: UnitID3

Access Level: Read Write

Alarm Management Table

Alarm Code

SNMP MIB: `fwuSystemAlarmCode`

Description: An alphanumeric code that uniquely identifies an alarm/fault.

Values: See "Troubleshooting Alarms" on page 185 or use the "Index of Alarms" on page 313 to find the page number for a specific alarm description, which includes the alarm code.

Syntax: Unsigned32

Access Level: Read Only

Alarm Control

SNMP MIB: `fwuSystemAlarmManageable`

Description: Indicates the ability to Enable or Disable alarm

Values: Enable = 1
                  Disable =0

Syntax: Updated

Access Level: Read Only

Alarm Threshold

SNMP MIB: `fwuSystemAlarmThreshold`

Description: The threshold at which the alarm is raised (Whenever applicable)

Values: See "Troubleshooting Alarms" on page 185 or use the "Index of Alarms" on page 313 to find the page number for a specific alarm description, which includes the alarm threshold, if any.

Syntax: DisplayString

Access Level: Read Only

Alarmed Module

SNMP MIB: `fwuSystemAlarmModType`

Description: Identifies the module type that raised the alarm.

Values: SeRF
DART
LPA
LNA
Power Detector
SFP

Syntax: Integer32

Access Level: Read Only

Alarm Enable Table

Alarm Code

SNMP MIB: `fwuSystemModuleAlarmcode`

Description: An alphanumeric code that uniquely identifies an alarm/fault.

Values: See "Troubleshooting Alarms" on page 185 or use the "Index of Alarms" on page 313 to find the page number for a specific alarm description, which includes the alarm code.

Syntax: Unsigned32

Access Level: Read Only

Node Address

SNMP MIB: `fwuSystemTrapNodeAddress`

Syntax: UnitId2

Access Level: Read Only

Alarmed Module Number

SNMP MIB: `fwuSystemAlarmModuleNo`

Description: Identifies the specific module type that raised the alarm.

Values: SeRF
DART
LPA
LNA
Power Detector
SFP

Syntax: Unsigned32

Access Level: Read Only