

## Full Configuration Setup

The Full Configuration menu allows you to fully configure the FibeAir 1500/1528 system without connecting the CeraView application. The menu includes all the options covered in the Quick Setup section plus some additional configuration options that are normally accessed from the CeraView application.

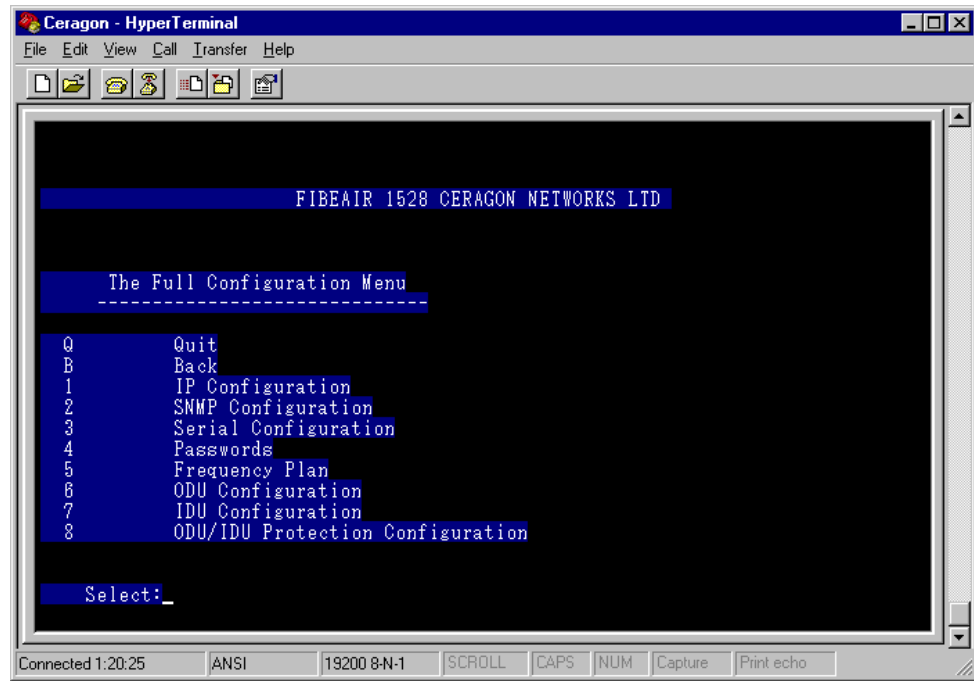


Figure 4-4 FibeAir 1500/1528 Terminal - Full Configuration Menu

Selecting the relevant options from the Full Configuration menu will guide you to the desired menu. The relevant operations are listed in each menu.

## Setting the Frequency Channel

To set the frequency channel, perform the following operations:

1. Connect to the Terminal.
2. From the Main Configuration menu, select **Full Configuration**.
3. From the Full Configuration menu, select **(5) Frequency Plan**. The Frequency Plan menu appears.

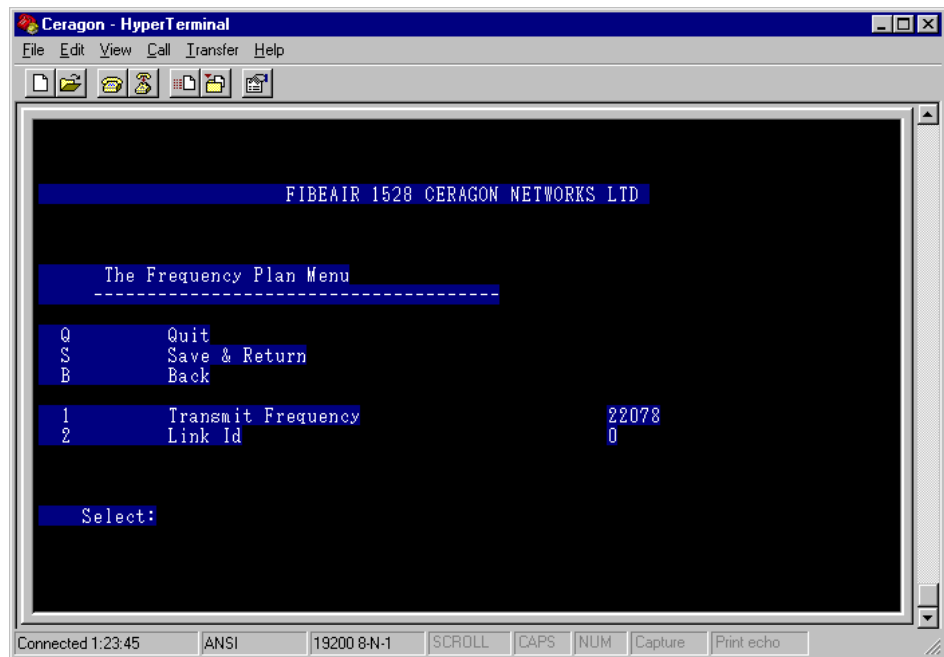


Figure 4-5 FibeAir 1500/1528 Terminal - Frequency Plan Menu

4. From the Frequency Plan menu, select **(1) Transmit Frequency**.
5. Enter the desired channel frequency.
6. Select **(S) Save & Return** to save the settings and return to the Full Configuration menu.

## Setting the Transmit Power Level

To set the transmitter power, perform the following operations:

1. Connect to the Terminal.
2. From the Main Configuration menu, select **Full Configuration**.
3. From the Full Configuration menu, select **(6) ODU Configuration**. The ODU Configuration menu appears.

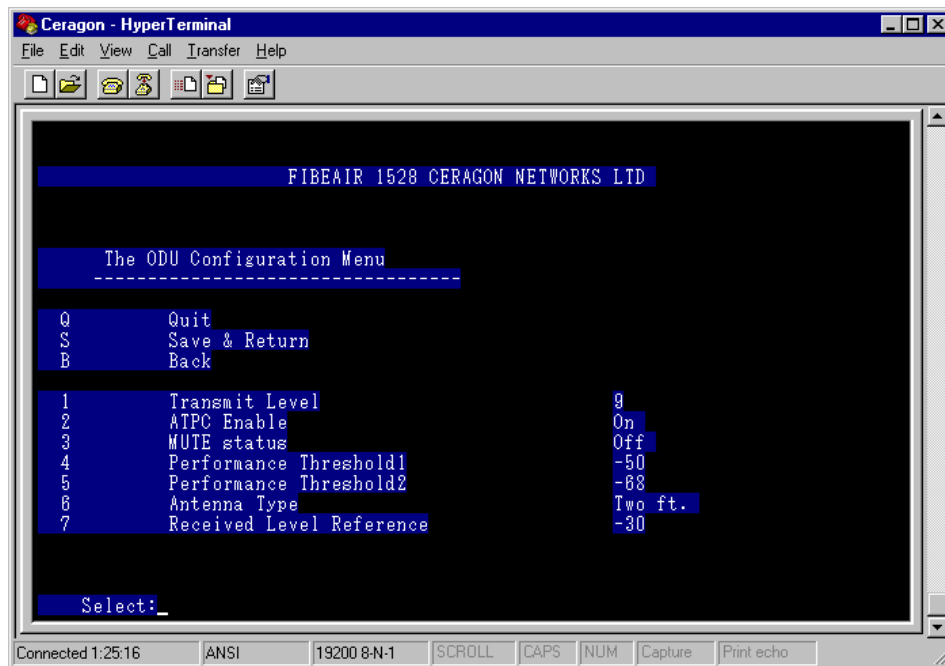


Figure 4-6 FibeAir 1500/1528 Terminal - ODU Configuration Menu

4. Select **(1) Transmit level**.
5. Enter the desired transmit level. The acceptable values are between  $-10$  dBm to  $+15$  dBm. Take into account the received level you expect (the default received level is  $+15$  dBm).
6. Select **(S) Save & Return** to save the settings and return to the Full Configuration menu.

For frequencies other than 38 GHz, the transmit level can be higher than 15 dBm. Refer to Appendix E for more details.

## Setting the IP Addresses

To set the IP Addresses, perform the following operations:

1. Connect to the Terminal.
2. From the Main Configuration menu, select **Full Configuration**.
3. From the Full Configuration menu, select **(1) IP Configuration**. The IP Configuration menu appears.

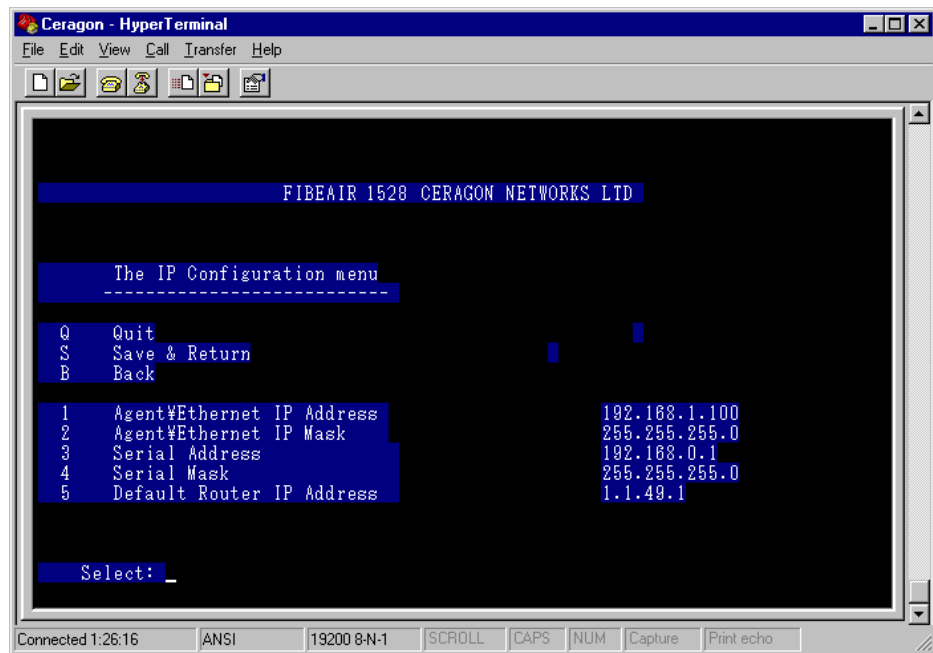


Figure 4-7 FibeAir 1500/1528 Terminal - IP Configuration Menu

#### For Ethernet Configuration:

6. Select **(1) Agent\Ethernet IP Address**, and enter the IP address.
7. Select **(2) Agent\Ethernet IP Mask**, and enter the IP mask.

#### For Serial Communication (Slip, PPP, or Dial-up Modem):

8. Select **(3) Serial Address**, and enter the serial address.
9. Select **(4) Serial Mask**, and enter the serial mask.
10. Select **(5) Default Gateway Router**, and enter the router's address.
11. Select **(S) Save & Return** to save the settings and return to the Full Configuration menu.
12. Restart the IDU.

## Configuring Serial Communication Settings (direct or dial-up)

This configuration is required when a dial up modem or a computer is connected to the IDU's serial port. To configure the serial communication settings, perform the following operations:

1. Connect to the Terminal.
2. From the Main Configuration menu, select **Full Configuration**.
3. From the Full Configuration menu, select **(3) Serial Configuration**.

- From the Serial Configuration menu, select **(1) Interface Communication**. The Interface Configuration menu appears.

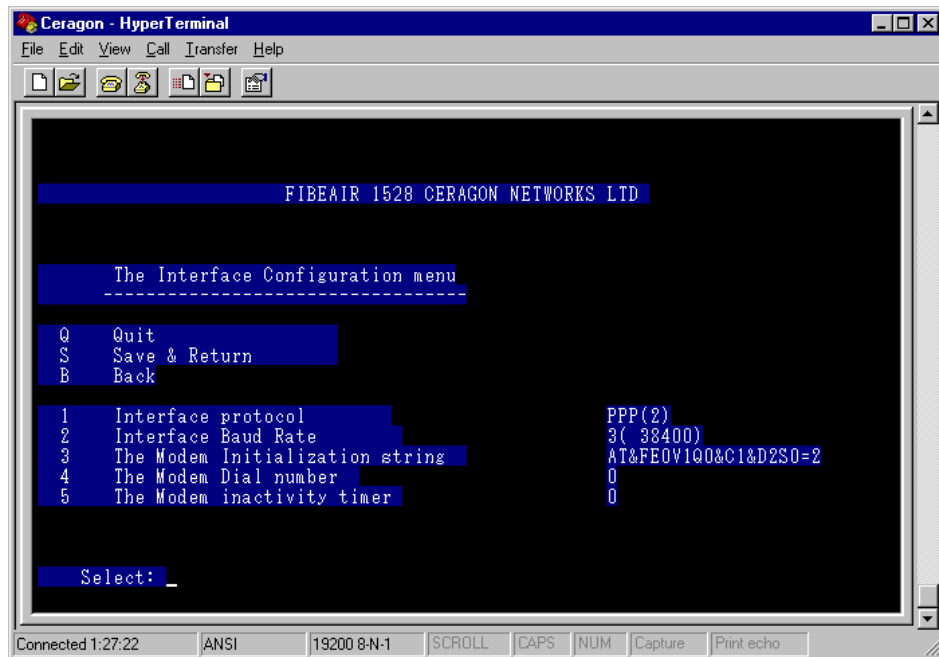


Figure 4-8 FibeAir 1500/1528 Terminal - Interface Configuration Menu

- Select **(1) Interface Protocol**, and then select **(2) PPP** or **(3) SLIP**.
- Select **(2) Interface Baud rate**, and then select the desired baud rate.

**Note:** For a modem connection, choose no more than 19,200. For a direct connection to a nearby computer, choose 38,400. Make sure that the same rate is defined in your network manager's dial up connection.

- In **(3) The Modem Initialization String**, leave the default string.

**Note:** Normally, the default should be used, unless the modem is connected through a PABX or in any other special case. In these cases, consult Ceragon Technical Service department.

- Select **(4) The Modem Dial Number** and enter a number if necessary.

**Note:** This is the telephone number to which the network manager's modem is connected.

- Select **(5) The Modem Inactivity Timer** and enter the value "0".

**Note:** This parameter states how long should the phone call will remain active when no data is transferred on the line. A value of 0 (zero), disables this inactivity timer.

- Select **(S) Save & Return** to save the settings and return to the Full Configuration menu.

## Configuring PPP Security Settings

The PPP protocol adds security to the communication, and therefore, additional parameters need to be configured in the system. This screen is not relevant for a SLIP connection.

To configure the PPP Security settings, perform the following operations:

1. Connect to the Terminal.
2. From the Main Configuration menu, select **Full Configuration**.
5. From the Full Configuration menu, select **(3) Serial Configuration**.
3. From the Serial Configuration menu, select **(2) PPP Security**. The PPP Security menu appears.

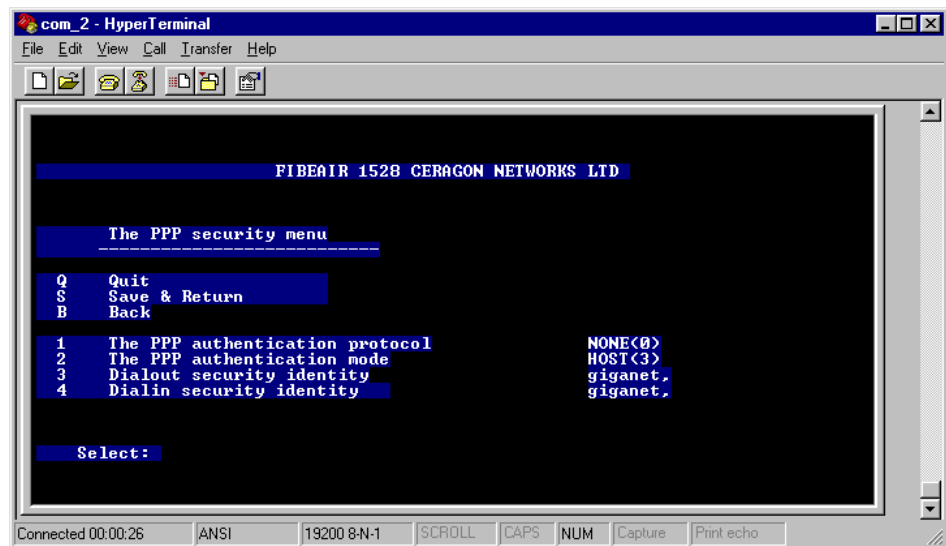


Figure 4-9 FibeAir 1500/1528 Terminal - PPP Security Menu

4. Select **(1) PPP Authentication Protocol**. Define the protocol:
  - 0 = None
  - 1 = PAP (without encryption)
  - 2 = CHAP (with encryption)
5. Select **(2) PPP Authentication Mode**.
  - 2 = GUEST: The IDU gives the “user name” and the “password” to the network manager.
  - 3 = HOST: The IDU receives the “use name” and the “password” from the network manager and validates them.
  - 4 = DYNAMIC: When the IDU receives a phone call, then it acts as HOST. If it initiates a call to the network manager (SNMP trap), it will act like a GUEST. In case of a direct connection (without a dialup modem), it acts as HOST.
6. Select **(3) Access Device Security Identity**. Enter user name (password). This will be sent by the IDU when configured for authentication and acts like a GUEST.

7. Select **(4) External Device Security Identity**. Enter user name (password). This will be received and validated by the IDU when configured for authentication and acts like a HOST.
8. Select **(S) Save & Return** to save the settings and return to the Full Configuration menu.

## SNMP Configuration

To connect to the IDU with SNMP-based management, you need to define the SNMP communities. These are passwords that define access rights of different users. If these are not identical to the definitions in the network management software (CeraView or any other SNMP based software), the authentication process will fail and access to the radio link is denied.

To configure the SNMP communities, perform the following operations:

1. Connect to the Terminal.
2. From the Main Configuration menu, select **Full Configuration**.
3. From the Full Configuration menu, select **(2) SNMP Configuration**. The SNMP Configuration menu appears.

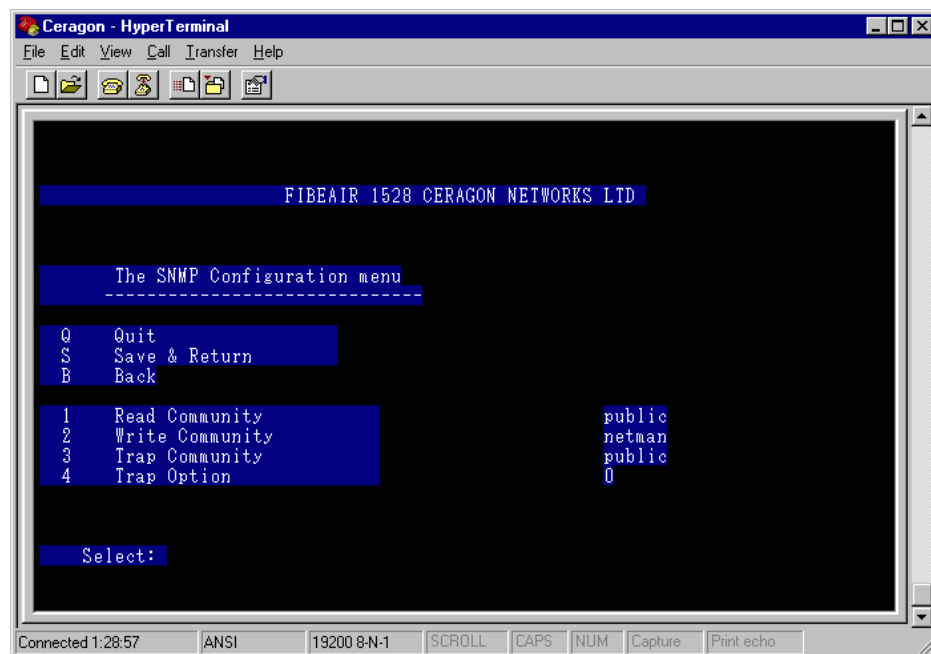


Figure 4-10 FibeAir 1500/1528 Terminal – SNMP Configuration Menu

4. Select **(1) Read Community** and set it to **public**. Users with this community will be allowed to read the link information, but will not be allowed to change anything.
5. Select **(2) Write Community** and set it to **netman**. Users with this community will be allowed to read and modify link information.

6. Select **(3) Trap Community** and set it to **public**. This password will be used by the IDU when it reports to a SNMP based manager. The same password needs to be included in the manager itself.
7. Select **(4) Trap Option** and set it to **Standard Trap (0)**. In the “Standard Trap” option, serial numbers will be added only to the private MIB traps. Otherwise, serial numbers will be added to all SNMP traps.
8. Select **(S) Save & Return** to save the settings and return to the Full Configuration menu.
9. Restart the IDU.

## Additional FibeAir 1500A/1528A Configuration

In addition to the setup procedures described above, the following terminal setup screens relate specifically to FibeAir 1500A/1528A.

### SSM (Synchronization Signal Message ) Configuration

Configuration (1) → Full Configuration (2) → IDU Configuration (7) → Access Configuration (4) → SSM Configuration (4)

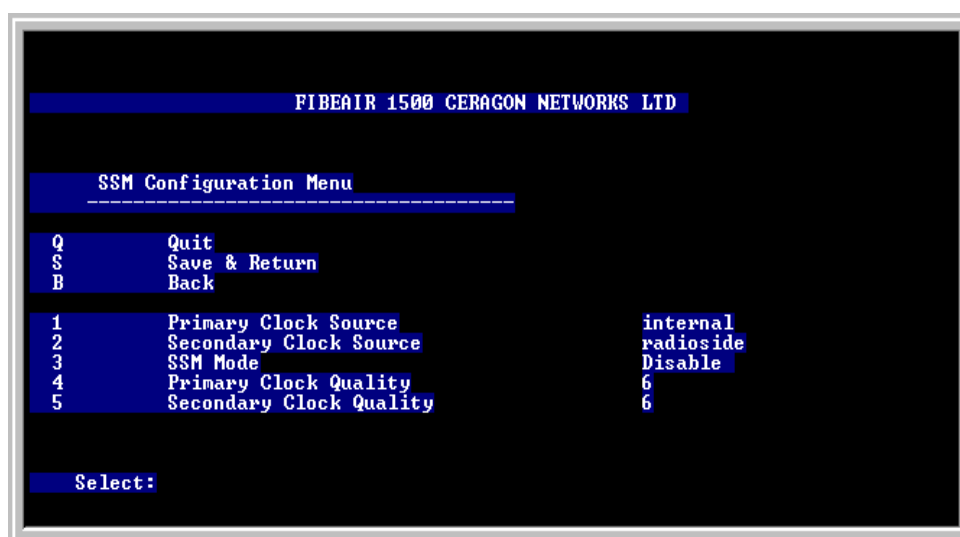


Figure 4-11 FibeAir 1500/1528 Terminal - SSM Configuration Menu

Note that changing the value of Standard Protocol (IDU Configuration → Radio Configuration → Standard Protocol) may cause an update of the Clock Quality (Primary and Secondary) values.

The update will be performed in the following cases:

Case	Previous Value	New Value
SDH → SONET/SONET_c	DNU (6)	DUS (7)
SONET/SONET_c → SDH	DUS (7)	DNU (6)



## ADM Configuration

Configuration (1) → Full Configuration (2) → IDU Configuration (7) → ADM Configuration (4)

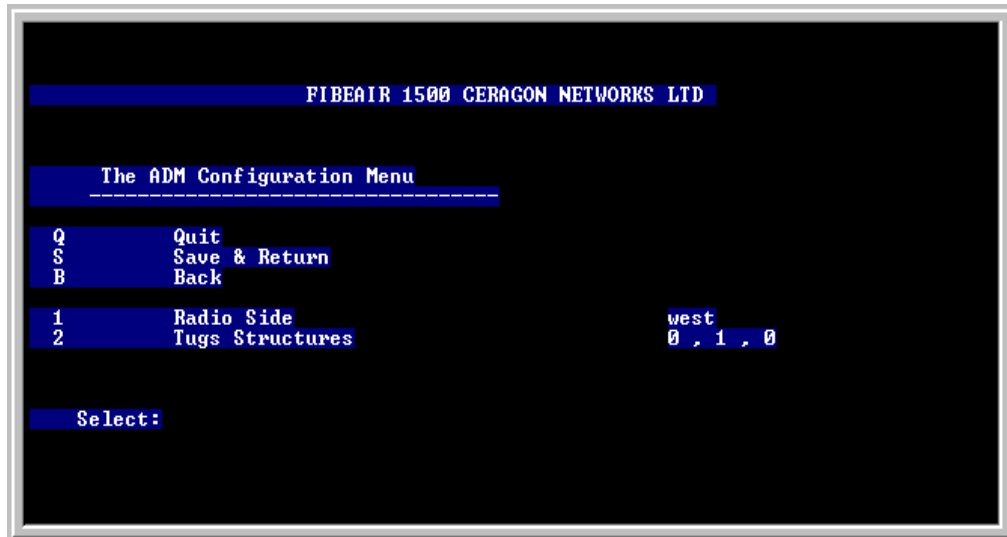


Figure 4-12 FibeAir 1500A/1528A Terminal - ADM Configuration Menu

Note that changing the value of the Radio Side parameter causes the initialization of three other parameters located in the Interfaces menu: KLM Index, Low-Path Side, and Protection.

Tug Structure parameter values must be set for all three together (tug structures 1, 2, and 3). One or two cannot be changed without changing the others.

## Interfaces Configuration

The interfaces configuration consists of several screens, one for each interface. Screen content depends on the interface type.

Configuration (1) → Full Configuration (2) → IDU Configuration (7) → Access Configuration (4) → Left Interface Configuration (1) / Right Interface Configuration (2).

The following are examples of screens for different interfaces.

**Screen for the Left Interface Configuration (8 E1 interfaces):**

```

FIBEAIR 1500 CERAGON NETWORKS LTD

Left Interface Configuration Menu
-----
Q      Quit
B      Back

1      E1\T1 Interface # 1
2      E1\T1 Interface # 2
3      E1\T1 Interface # 3
4      E1\T1 Interface # 4
5      E1\T1 Interface # 5
6      E1\T1 Interface # 6
7      E1\T1 Interface # 7
8      E1\T1 Interface # 8

Select: _

```

Figure 4-13 FibeAir 1500A/1528A Terminal - Example of 8 E1/T1 Interfaces Configuration

**Screen for one E1 interface configuration:**

```

FIBEAIR 1500 CERAGON NETWORKS LTD

Interface # 5
-----
Q      Quit
S      Save & Return
B      Back

1      Interface Enable                off
2      Cable Length                    any length
3      Line Coding                     hdb3
4      Trail Name                      TRAIL #5
5      Protection                      protected
6      K.L.M index, Low Path Side      0 , east
7      Protection Option, Reversion Mode auto , non revertive
8      Times: Hold off, Oscilation, Wait to Restore 0 , 0 , 5
9      Protection User Command        no action

Select: _

```

Figure 4-14 FibeAir 1500A/1528A Terminal - Example of one E1/T1 Configuration

Note the following:

- If there is no left/right interface, the left/right interface screen will still be available.
- Changing the Standard Protocol value (IDU Configuration → Radio Configuration → Standard Protocol) causes the initialization of KLM Index and Low Path Side.
- Since the KLM Index, Low Path Side, and Protection parameters are related, in order to prevent redundancy, the following combinations should not be used:
  - Two (or more) trails with the same KLM Index and Low Path Side.

- Two (or more) trails with the same KLM Index, whereby at least one of them is in protected mode (its Protection Option value is “Protected”).
- Some lines in the screens include more than one parameter. In such cases, the parameters must be set together.

## Connecting to the IDU

You can perform the physical connection to the IDU using one of the following methods:

- Connecting via the Ethernet port
- Connecting via the serial port using PPP/SLIP
- Connecting via the serial port using a dial-up modem

### Connecting Via the Ethernet Port

1. Connect an Ethernet cable to the Ethernet port of the IDU. If the IDU is connected directly to the computer, use a cross cable. If the IDU is connected to a LAN (wall socket), use a standard straight cable.
2. Set the Ethernet IP address and mask to the IDU using the HyperTerminal. The default Agent/Ethernet IP address is 192.168.1.1 and the Agent/Ethernet IP mask is 255.255.255.0
3. Make Sure the Ethernet IP address of your PC is on the same sub-net as the IDU's Ethernet IP address, and that the masks are identical.
4. Check and change the Ethernet address of the PC as follows:

#### Windows 95/98/2000:

- Select Start ➤ Settings ➤ Control Panel ➤ Network.
- Select the TCP/IP Ethernet component that was installed on the PC and click Properties.
- On the IP Address tab select Specify an IP Address and enter the appropriate IP address and mask.

#### Windows NT:

- Select Start ➤ Settings ➤ Control Panel ➤ Network.
- Select **Protocols**, then select **TCP/IP** protocol and then click **Properties**.
- On the IP Address tab select **Specify an IP Address** and enter the appropriate IP address and mask.

5. To verify connectivity, ping the IDU's Ethernet IP address and make sure you have a reply as follows:
  - Select **Start ➤ Run**.

- Type **ping** followed by the IP address, and click **OK**.
6. Run the CeraView management application.

## ***Connecting Via the Serial Port Using PPP/SLIP***

1. Connect an RS-232 9-pin cable to the serial port of the IDU.
2. Install a PPP or SLIP driver. Refer to Appendix A for details.

Set the serial IP address and mask of the IDU using the Hyper-Terminal. The default serial IP address is 192.168.10.1 and the serial IP mask is 255.255.255.0.

Make sure that the serial IP address of your PC is on the same sub-net as the IDU's serial IP address, and that the masks are identical.

### Windows 95/98/2000:

3. Check and change the serial address of the PC as follows:
  - Select Start ➤ Settings ➤ Control Panel ➤ Network.
  - Select the TCP/IP Dial-up Adapter component that was installed on the PC and click **Properties**.
  - On the IP Address tab select **Specify an IP Address** and enter the IP address and mask that are on the same sub-net as the IDU you want to connect to.

Make sure that the serial IP address of the PPP/SLIP driver you have installed is on the same sub-net as the IDU's serial IP address, and the masks are identical.

4. To check and change the serial address of the PPP/SLIP driver double-click **My Computer**.
5. Double-click **Dial-up Networking**.
6. Click the icon that was added after the installation of the PPP/SLIP driver, and select **Properties**.
7. Verify that the protocol (PPP or SLIP) and the baud rate match the serial configuration that was set on the HyperTerminal.
8. Select **Server Type** and click **TCP/IP Setting**.
9. Select **Specify IP Address** and enter address on the same sub-net as the serial address of the IDU.
10. Double-click this icon whenever you would like to establish communication with the IDU.

### Windows NT:

3. To check and change the serial address of the PPP/SLIP driver double-click **My Computer**. Double-click **Dial-Up Networking**.

4. Click **More**, select **Edit entry** and **modem properties**.
5. On the Basic tab verify that you are dialing using **NT Direct Connection**.
6. Click **Configure** and verify that the Initial speed (bps) is as configured on the HyperTerminal.
7. Select **Server** tab and chose **PPP** or **SLIP** as your **Dial-up server type**. Verify that the protocol (PPP or SLIP) and is in accordance to the serial configuration that was set on the Hyper Terminal.
8. Check only **TCP/IP** then Click **TCP/IP Settings**.
9. Select **Specify IP Address** and enter address on the same sub-net as the serial address of the IDU.
10. Make sure that **Server assigned name server addresses** is selected and **Use IP header compression** and **Use default gateway on remote network** are unchecked.
11. Whenever you wish to connect to the IDU, double-click **Dial-Up Networking** and select the number you wish to dial at the **Phonebook Entry**.
12. To verify connectivity, ping the IDU's Ethernet IP address and make sure you have a reply: Select **Start** → **Run** and open **ping IP address**.

Once communication is established, run the CeraView management application.

## ***Connecting Via a Serial Port Using a Dial-Up Modem***

1. Double-click **My Computer** and then double-click **Dial-up Networking**.
2. Double-click **Make New Connection**. Type a name for the new connection (Ceragon, for example), and select the modem you are using to dial.
3. Click **Configure**. On the **General** tab, set the maximum speed available and uncheck the **Only connect at this speed** box.
4. On the **Connection** tab set Data bits =8, Parity = none, and Stop bits =1.
5. Check the **Wait for dial tone** box and uncheck the **Call if not connected in 90 seconds** box.
6. Uncheck **Disconnect a call if idle for more than ... seconds**.
7. Click **Port Settings** and check **Use FIFO Buffers** and then click **OK**.
8. Click **Advanced** and uncheck the **Use error control** and **Use flow control** boxes.
9. Make sure that **Modulation type** is set to **Standard**.
10. Click **Server Type** and select **PPP** or **SLIP** as Dial-up Server. Check only **TCP/IP**.

11. Make sure that you select the serial interface that was configured in the Hyper Terminal.
12. Click **TCP/IP Settings** and specify an IP address. The IP address should be on the same sub-net as the serial address of the IDU.
13. Select **Server assigned name server addresses** and uncheck the **Use IP header compression** and **Use default gateway on remote network** boxes.

### Modem

1. Connect the modem to the serial port of the IDU and to an analog telephone line.
2. Make sure that the cable for the modem has the following pin-out:

DB9	DB25
1	20
2	2
3	3
4	8
5	7
7	5
8	4
Isolated shields	

3. When using a standard modem, the dip-switch configuration should be set as follows: Switches 3 & 8-down (Display results codes & Smart mode).

## Logging In

To perform management operations, start the management software as follows.

1. Select **Start** > **Programs** > **CeraView**.

After the RunEnv Parameters window, the Login window appears.

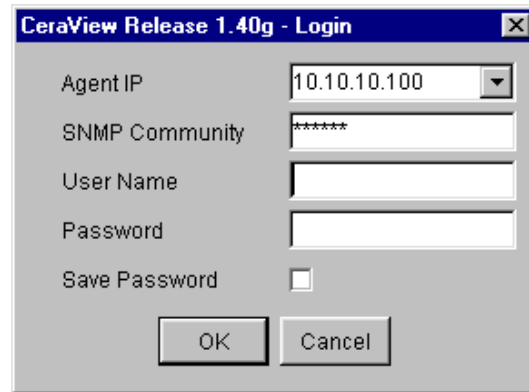


Figure 4-15 Login Window

2. Enter the IP address of the IDU you want to log in to, the SNMP community (for SNMP protocol access), your user name and password, and click **OK**.

The default password is **Ceragon**, but it can be changed later.

After you log in, the Main CeraView window appears.

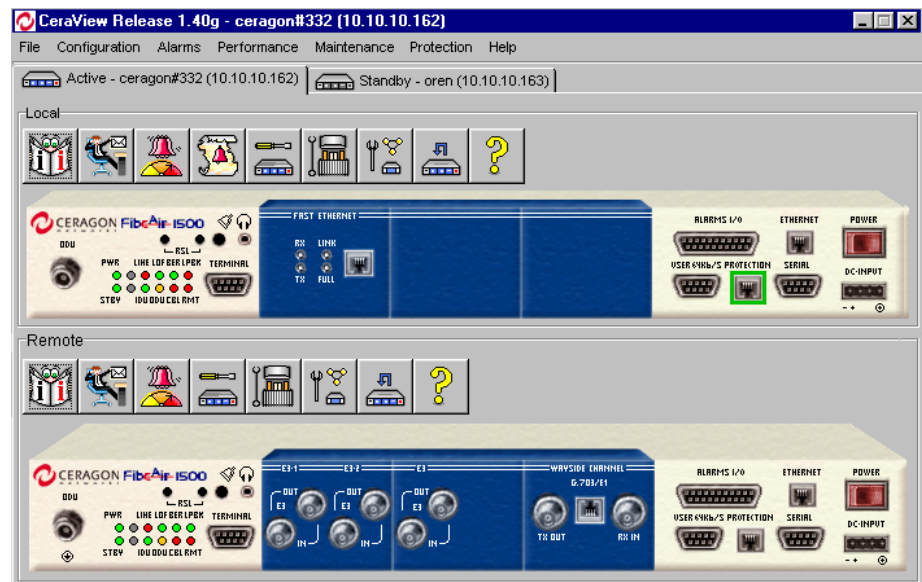


Figure 4-16 Main CeraView Window

## Setting System Information

To define system information:



1. Select **File, System Information.**, or click the System Information icon.

The screenshot shows a window titled "System Information - (10.10.10.100)". It contains several sections:

- Current Time:** A text box showing "Mon Mar 25 17:14:48 IST 2002" and a "Configure Time" button.
- System Parameters:**
  - Description:** "FibeAir 1500 agent" (read-only)
  - Name:** Empty text box
  - Contact:** Empty text box
  - Location:** Empty text box
  - Up Time:** "4 days, 0 hours, 7 minutes, 35 seconds." (read-only)
- Software Versions:**
  - IDU:** "14.09v" (read-only)
  - ODU:** Empty text box
  - MUX:** "M3.57pdA067" (read-only)
- Serial Numbers:**
  - IDU:** Empty text box
  - ODU:** Empty text box
- Link Parameters:**
  - Link ID:** "123" (read-only)

At the bottom are buttons for "Apply", "Refresh", "Close", and "Help".

Figure 4-17 System Information Window

2. In the **Current Time** area, click **Configure Time** and set the time in the format HH:MM:SS.
3. The read-only **Description** field provides information about the FibeAir system.
4. (Optional) In the **Name** field, enter a name for this link. By convention, this is the node's fully-qualified domain name.
5. (Optional) In the **Contact** field, enter the name of the person to be contacted when a problem with the system occurs. Include information on how to contact the designated person.
6. (Optional) In the **Location** field, enter the actual physical location of the node or agent.
7. The **Up Time** field, **Software Versions** area, and **Serial Numbers** area are read-only.
8. For **Link ID**, enter the ID of the link you are working with.  
Note that for the link to operate, the link ID must be identical on both sides.
9. Click **Apply**. The settings are saved.
10. Click **Close**.



## Local/Remote Transport Configuration (Optional)

The Local/Remote Transport Configuration window allows you to change threshold levels for the radio and alarms, and to configure special transmission parameters. This is recommended for advanced users only.



1. Select **Configuration, IDU, Local/Remote Transport**, or click the Local/Remote Transport Configuration icon.

The Local/Remote Transport Configuration window appears.

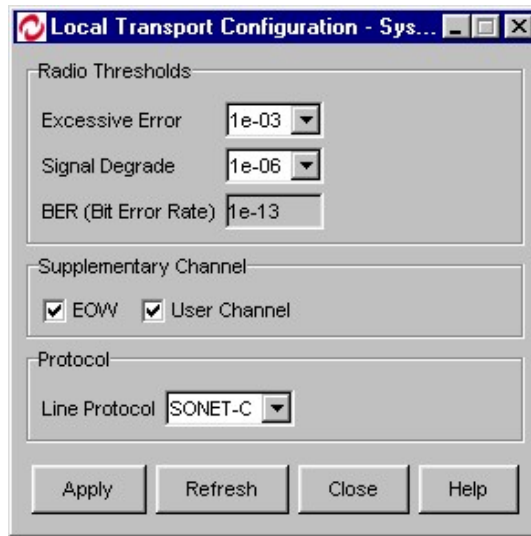


Figure 4-18 Local Transport Configuration Window

2. In the **Excessive Error** field, select the level above which a radio Excessive BER alarm is issued. This is a major alarm.
3. In the **Signal Degrade** field, select the level above which a radio Signal Degrade alarm is issued. This is a minor alarm.
4. The BER field is read-only.
5. In the **Supplementary Channel** area, select EOW and/or User Channel if those channels are used.

EOW - Engineering Order Wire

User Channel - 64 Kbps

6. The **Line Protocol** field displays the current data transfer protocol in use. To change the protocol, click the drop down list and select either SDH, SONET, or SONET-C.
7. Click **Apply** to save the settings.
8. Click **Close**.

## Trap Forwarding Configuration

This section explains how to set up a trap forwarding plan. If your application does not require trap forwarding, you can skip the following procedure.



1. Select **Configuration, System, Trap Forwarding**, or click the Trap Forwarding icon.

The Trap Forwarding Configuration window appears.

Trap Filters	#1	#2	#3	#4
Power supply alarms	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Cable alarms	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Temperature alarms	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
External alarms	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Radio alarms	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Modem alarms	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Line alarms	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
SDH alarms	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
BER alarms	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
System fault alarms	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Maintenance alarms	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Standard traps	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Figure 4-19 Trap Forwarding Configuration Window

2. In the **Managers** section of the window, specify the IP addresses of the managers to which traps will be forwarded.
3. In the **Trap Filters** section, you determine which alarms will be sent as an SNMP trap to each manager.

In each manager column, select the alarm types you want to include for that manager.

4. In the **Serial Line IP** area, the **IP Address** field shows the IP address of the modem or SLIP/IPP driver connected to the serial port.
5. In the **Baud rate** field, select the appropriate baud rate for serial port data transfer.
6. For **Modem phone number**, enter the number the modem will dial for serial data transfer.
7. In the **Trap Options** area, select **Standard traps include serial number** if you want trap messages to include the IDU serial number.

8. Select **Report local traps from remote IDU** if you want remote IDU trap messages to be reported locally.
9. Select **Events are reported as traps** if you want events to appear as trap messages.
10. For **CLLI** (Common Language Location Identifier), enter up to 18 characters that will represent your system ID when traps are sent.
11. For **Heartbeat period**, a heartbeat signal will be generated every x minutes (the number you enter in the field) to tell your system that the trap mechanism is working.
12. Click **Apply** to save the settings.
13. Click **Close** to close the window.

## External Alarms Setup

The procedure detailed in this section is required only if alarms generated by external equipment are connected to the IDU, or if the IDU alarm outputs are connected to other equipment (using the alarms I/O connector).



1. Select **Configuration, IDU, Local/Remote I/O External Alarms**, or click the **Local/Remote I/O External Alarms** icon.

The Local/Remote Input/Output External Alarms window appears.

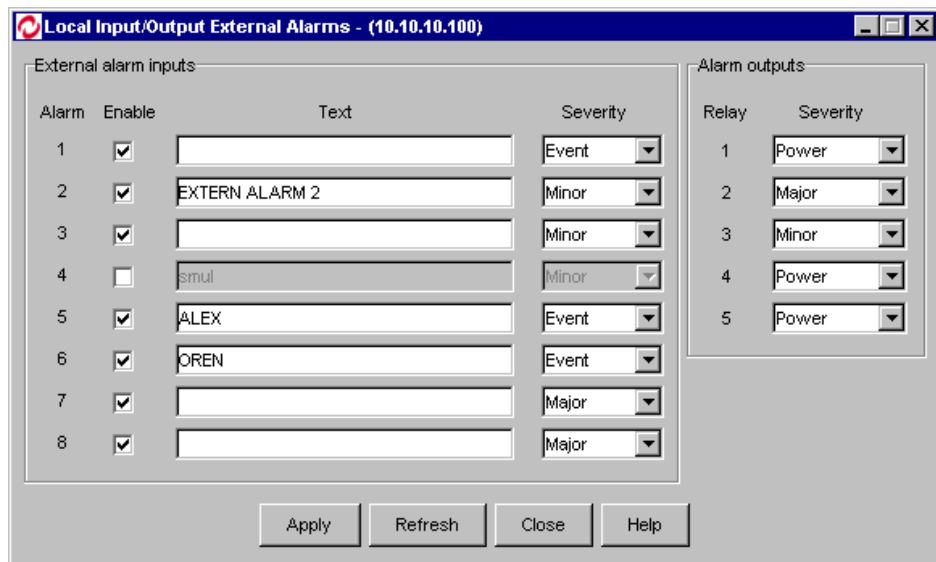


Figure 4-20 Local Input/Output External Alarms Window

Follow the steps below for both the Local and Remote sides.

The microcontroller in the IDU reads alarm inputs (dry contact) and transmits them to the CeraView management system. This allows FibeAir to report external alarms that are not related to its own system.

For each alarm on the left side of the window, do the following:

2. Click on the box next to the alarm number to enable/disable the alarm.
3. If you enable an alarm, enter a description of the alarm in the text field.
4. Select the alarm's severity level from the drop-down list (Major, Minor, Warning, or Event).
5. FibeAir provides five alarm outputs that can be used by other systems to sense FibeAir alarms. The outputs are configured on the right side of the window.

The alarm outputs are Form C Relays. Each output relay provides three pins, as follows:

Normally Open (NO)

Normally Closed (NC)

Common (C)

Output alarms can be defined as any one of the following:

Major

Minor

Warning

External

Power

BER

Line

Loopback

LOF

IDU

ODU

Cable

Remote

The default alarm output setting for each relay is "Power".

The relays may be connected to customer-specific applications. Refer to Appendix B for details concerning the alarm connector pin assignments.

5. After you complete the external alarm configuration, click **Apply** to save the settings.
6. Click **Close**.

The window is closed and you are returned to the Main window.

## ***Line Interface Connection***

After configuring the system in accordance with the previous sections, the Line Interfaces can be connected to the IDU.

For a description of all available FibeAir line interfaces, see Chapter 8.

Note the following interface terminology:

- For connectors or signals labeled TX, the signals are sent from the FibeAir system.
- For connectors or signals labeled RX, the signals are sent to the FibeAir system.

# Chapter 5

---

## Operation

### General

This chapter explains how Ceragon's CeraView management software is used to configure and monitor FibeAir systems.

### Logging in to CeraView

To log in to CeraView:

1. Select **Start, Programs, CeraView**.

The Login window appears.

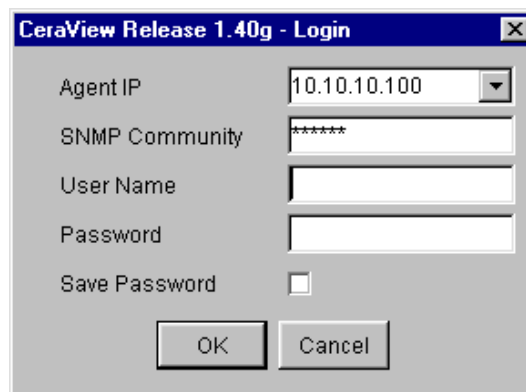


Figure 5-1 CeraView Login Window

2. Enter the information and click **OK**.

Mark the **Save Password** box if you want CeraView to remember the password you entered.

Note that there are two types of passwords, each with a different security level for authorized activities:

*Read Only* - user is permitted to perform monitoring activities only.

*Read/Write* - user is permitted to change system configuration and system administrator parameters, and perform monitoring activities.

## CeraView for FibeAir 1500/1528

The following sections describe the CeraView application for FibeAir 1500/1528. For a description of CeraView for FibeAir 1500A/1528A, see *CeraView for FibeAir 1500A/1528A* at the end of these sections.

### Main Window

The Main window is your starting point for all operations.

Below is a description of the menus, toolbars and other features of the Main window.

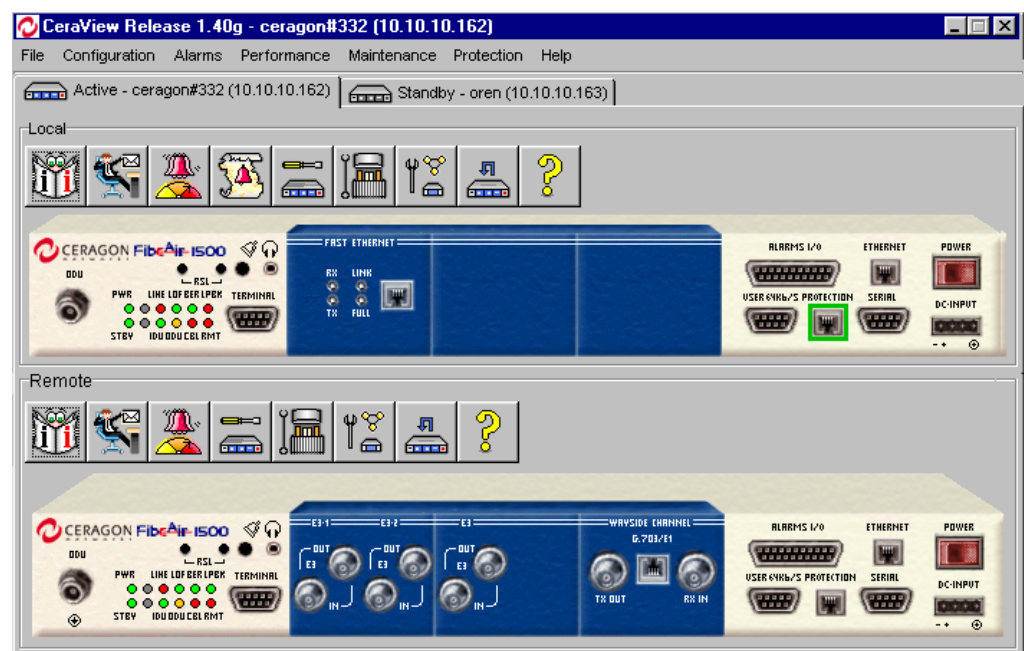


Figure 5-2 Main Window

### Title Bar

The Title Bar displays the CeraView version and the IP address of the IDU being accessed.

### Active/Standby

The Active/Standby tabs appear for protected (1+1) systems. You can click on the tabs to configure the respective units.

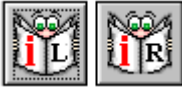



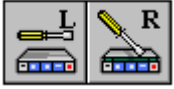
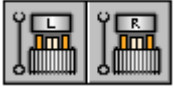

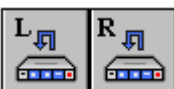

### Menu Bar

The Menu Bar contains menus and menu items used to perform CeraView operations.

## Toolbar

The Toolbar includes several icons that you can click to perform different operations.

Each icon in the Toolbar is described below.

Icon	Operation
	<i>System Information</i> - used to view and define system information, such as contact personnel and system up time.
	<i>Trap Forwarding Configuration</i> - used to designate managers to which traps will be forwarded.
	<i>Current Alarms</i> - used to view current active alarms.
	<i>Alarm Log</i> - used to view historical alarm records.
	<i>Local/Remote Input/Output External Alarms</i> - used to configure alarms sent to/from external sources.
	<i>Local/Remote ODU Configuration</i> - used to configure the local and remote ODUs.
	<i>Local/Remote Transport Configuration</i> - used to configure local and remote radio, line, RSOH, and security parameters.
	<i>Local/Remote Loopback</i> - used to configure and run local and remote loopbacks for testing and troubleshooting.
	<i>Online Help</i> - used to view the online help file.

## Physical View

Physical views of the FibeAir local and remote units are displayed in the Main window. The views provide a real-time virtual display of the IDU front panel.

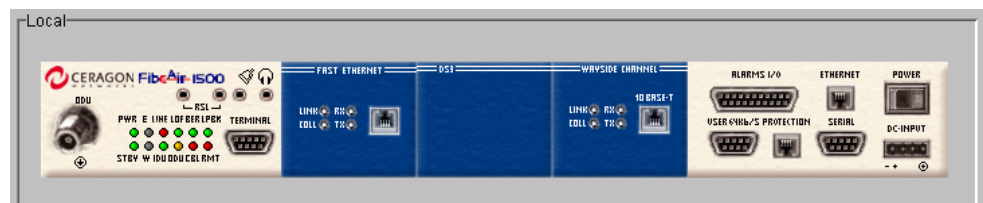


Figure 5-3 Physical View in Main Window



The LEDs that appear in the physical view indicate the actual real-time status of the LEDs on the front panel of the IDU. (LED changes on the actual front panels of the units will be updated in the physical views after a slight delay.)

The LED colors are as follows:

**Green** - indicates proper operation

**Yellow** - indicates a warning

**Red** - indicates a major alarm or severe malfunction

The following table lists the LEDs and their indications.

LED	Color			Description
	Red	Yellow	Green	
Power	X		X	<b>Red</b> - power supply problem, system not functional
Line	X	X	X	<b>Red</b> - no input to main channel / High BER <b>Yellow</b> - J0 mismatch / BER
LOF (Loss of Frame)	X		X	<b>Red</b> - radio did not recognize information frame (radio link problem/radio LOF)
BER (Bit Error Ratio)	X	X	X	<b>Red</b> - radio BER higher than radio excessive error threshold definition (see Sonet/SDH configuration window) <b>Yellow</b> - radio BER higher than radio signal degrade threshold definition (see Sonet/SDH configuration window)
LPBK (Loopback)	X		X	<b>Red</b> - loopback is active
STBY (Standby)		X	X	<b>Yellow</b> - Protected configuration. The unit is currently passive or Tx mute is operating
IDU	X	X	X	<b>Red</b> - modem unlocked / link ID mismatch <b>Yellow</b> - high temperature / fan problem
ODU	X	X	X	<b>Red</b> - no link / ODU power / ODU unlocked <b>Yellow</b> - radio interference / high temperature / Rx/Tx out of range
CBL (Cable)	X		X	<b>Red</b> - IF cable open / IF cable short
RMT (Remote Unit)	X	X	X	<b>Red</b> - no link / remote unit problem (red LED is lit in the remote unit) <b>Yellow</b> - warning in remote unit (yellow LED is lit in the remote unit)

**LED Indications for Hitless Systems**

For Hitless systems the following table lists the LEDs and their indications:

**LOF (LED Panel) - LOF**

<b>LED Color</b>	<b>Alarm Explanation</b>
Yellow	Local unit receives LOF from a receive path currently <i>not</i> in use.
Red	Local unit receives LOF from a receive path currently in use.

**LOF (Interface Panel) - ALRM**

<b>LED Color</b>	<b>Alarm Explanation</b>
OFF	Hitless mode is disabled.
Red	Local unit receives LOF from the mate unit.
Green	Hitless switching can be performed, if necessary.

**Local Receiver (Interface Panel) - Rx ACTV**

<b>LED Color</b>	<b>Alarm Explanation</b>
OFF	Local receiver not in use.
Green	Local receiver in use.

## Menus

The following sections describe the CeraView window menus.

### File Menu

#### System Information

This option allows you to view and define information for the FibeAir system.



1. Select **File, Local/Remote, System Information**, or click the System Information icon.

The System Information window appears.

Figure 5-4 System Information Window

2. In the **Current Time** area, click **Configure Time** and set the time in the format HH:MM:SS.
3. The read-only **Description** field provides information about the FibeAir system.
4. (Optional) In the **Name** field, enter a name for this link. By convention, this is the node's fully-qualified domain name.
5. (Optional) In the **Contact** field, enter the name of the person to be contacted when a problem with the system occurs. Include information on how to contact the designated person.
6. (Optional) In the **Location** field, enter the actual physical location of the node or agent.
7. The **Up Time** field, **Software Versions** area, and **Serial Numbers** area are read-only.

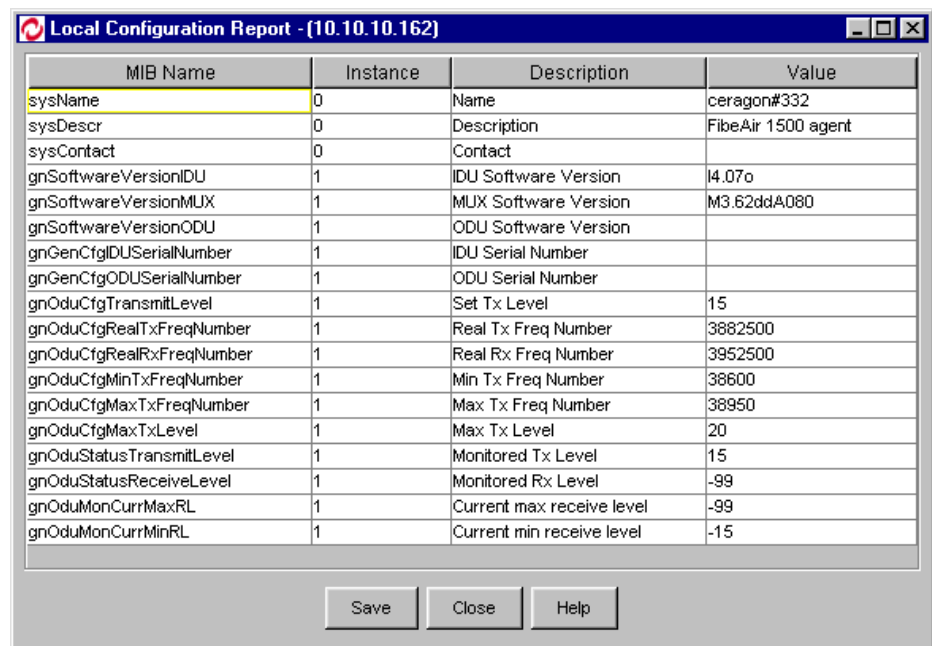
8. For **Link ID**, enter the ID of the link you are working with.
9. Click **Apply**.  
The settings are saved.
10. Click **Close**.

## Configuration Report

This option generates a report that includes various parameters and their values, such as system description, software versions, and Tx/Rx frequencies.

1. Select **File, Local/Remote, Configuration Report**.

The Local/Remote Configuration Report window appears.



MIB Name	Instance	Description	Value
sysName	0	Name	ceragon#332
sysDescr	0	Description	FibeAir 1500 agent
sysContact	0	Contact	
gnSoftwareVersionIDU	1	IDU Software Version	4.07o
gnSoftwareVersionMUX	1	MUX Software Version	M3.62ddA080
gnSoftwareVersionODU	1	ODU Software Version	
gnGenCfgIDUSerialNumber	1	IDU Serial Number	
gnGenCfgODUSerialNumber	1	ODU Serial Number	
gnOduCfgTransmitLevel	1	Set Tx Level	15
gnOduCfgRealTxFreqNumber	1	Real Tx Freq Number	3882500
gnOduCfgRealRxFreqNumber	1	Real Rx Freq Number	3952500
gnOduCfgMinTxFreqNumber	1	Min Tx Freq Number	38600
gnOduCfgMaxTxFreqNumber	1	Max Tx Freq Number	38950
gnOduCfgMaxTxLevel	1	Max Tx Level	20
gnOduStatusTransmitLevel	1	Monitored Tx Level	15
gnOduStatusReceiveLevel	1	Monitored Rx Level	-99
gnOduMonCurrMaxRL	1	Current max receive level	-99
gnOduMonCurrMinRL	1	Current min receive level	-15

Figure 5-5 Configuration Report Window

2. Click **Save** to save the report in a file for analysis or downloading.

## Configuration File Upload/Download

This option enables you to upload a configuration file to another FibeAir unit, or download a file to replace the current one.

1. Select **File, Local/Remote, Configuration File, Upload/Download**.

A window appears for you to locate and select the file you want to upload or download.

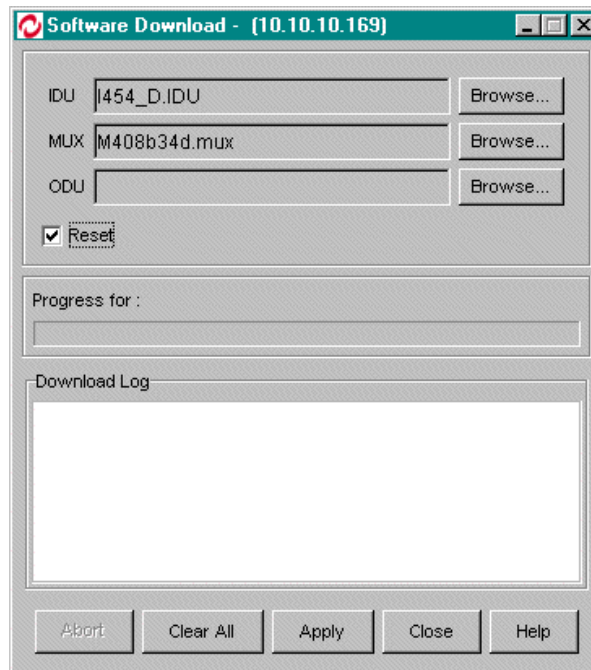
2. Select the file, and click **Upload** or **Download**.

## Software Download

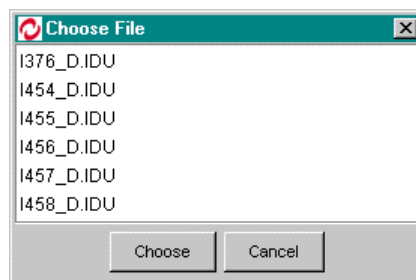
This option enables you to download IDU, ODU, and MUX software updates.

1. Select **File, Software Download**.

A window appears for you to define the software download procedure.



2. Click **Browse** to choose the software file you want to download.



3. Select the file you want, and click **Choose**.
4. In the Software Download window, click **Apply**.

The software file you chose is downloaded and a progress report appears in the Download Log area.

### New Session

Select this item to log in for a new CeraView session. The new session will appear in addition to the current session.

When you select this item, the CeraView login window appears for you to specify the IP address of the FibeAir unit you want to access.

### Exit

Select this item to exit the CeraViewr application. You can also exit by clicking on the Close icon (x) in the title bar.

When you exit CeraView, you will be prompted to confirm the exit. Click **OK** to confirm the operation.

## Configuration Menu

### IDU

#### Local/Remote I/O External Alarms

The procedure detailed in this section is required only if alarms generated by external equipment are connected to the IDU, or if the IDU alarm outputs are connected to other equipment (using the alarms I/O connector).



1. Select **Configuration, IDU, Local/Remote I/O External Alarms**, or click the **Local/Remote I/O External Alarms** icon.

The Local/Remote Input/Output External Alarms window appears.

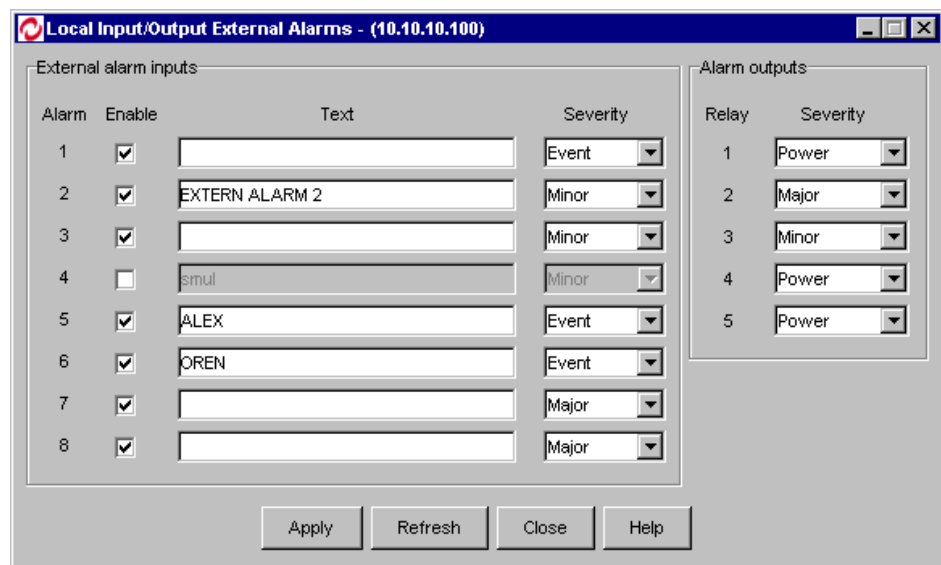


Figure 4-1 Local Input/Output External Alarms Window

Follow the steps below for both the Local and Remote sides.

The microcontroller in the IDU reads alarm inputs (dry contact) and transmits them to the CeraView management system. This allows FibeAir to report external alarms that are not related to its own system.

For each alarm on the left side of the window, do the following:

2. Click on the box next to the alarm number to enable/disable the alarm.
3. If you enable an alarm, enter a description of the alarm in the text field.
4. Select the alarm's severity level from the drop-down list (Major, Minor, Warning, or Event).
5. FibeAir provides five alarm outputs that can be used by other systems to sense FibeAir alarms. The outputs are configured on the right side of the window.

The alarm outputs are Form C Relays. Each output relay provides three pins, as follows: Normally Open (NO), Normally Closed (NC), Common (C).

Output alarms can be defined as Major, Minor, Warning, External, Power, BER, Line, Loopback, LOF, IDU, ODU, Cable, or Remote.

The default alarm output setting for all relays is "Power".

The relays may be connected to customer-specific applications. Refer to Appendix B for details concerning the alarm connector pin assignments.

6. After you complete the external alarm configuration, click **Apply** to save the settings.
7. Click **Close**.

The window is closed and you are returned to the Main window.

### Local/Remote Transport

The Local/Remote Transport Configuration window allows you to change threshold levels for the radio and alarms, and to configure special transmission parameters. This is recommended for advanced users only.



1. Select **Configuration, IDU, Local/Remote Transport**, or click the Local/Remote Transport Configuration icon.

The Local/Remote Transport Configuration window appears.

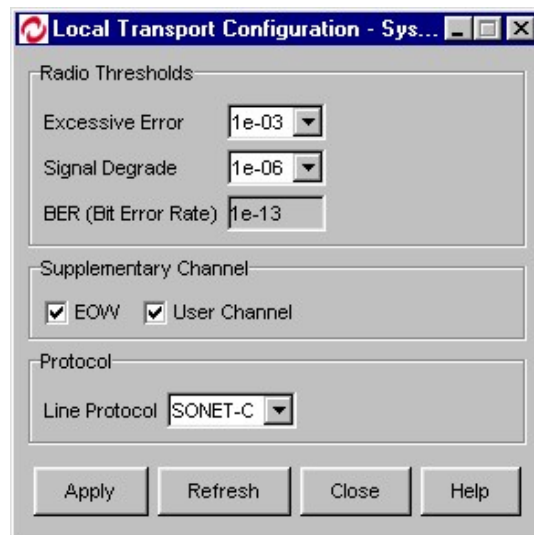
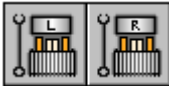


Figure 4-2 Local Transport Configuration Window

2. In the **Excessive Error** field, select the level above which an Excessive BER alarm is issued.
3. In the **Signal Degrade** field, select the level above which a Signal Degrade alarm is issued.
4. The BER field is read-only.
5. In the **Supplementary Channel** area, select EOW and/or User Channel if those channels are used.  
EOW - Engineering Order Wire  
User Channel - 64 Kbps
6. The **Line Protocol** field displays the current data transfer protocol in use. To change the protocol, click the drop down list and select either SDH, SONET, or SONET-C.
7. Click **Apply** to save the settings.
8. Click **Close**.

### ODU

## Local/Remote



1. Select **Configuration, ODU, Local/Remote**, or click the Local/Remote ODU Configuration icon.

The Local/Remote ODU Configuration window appears.

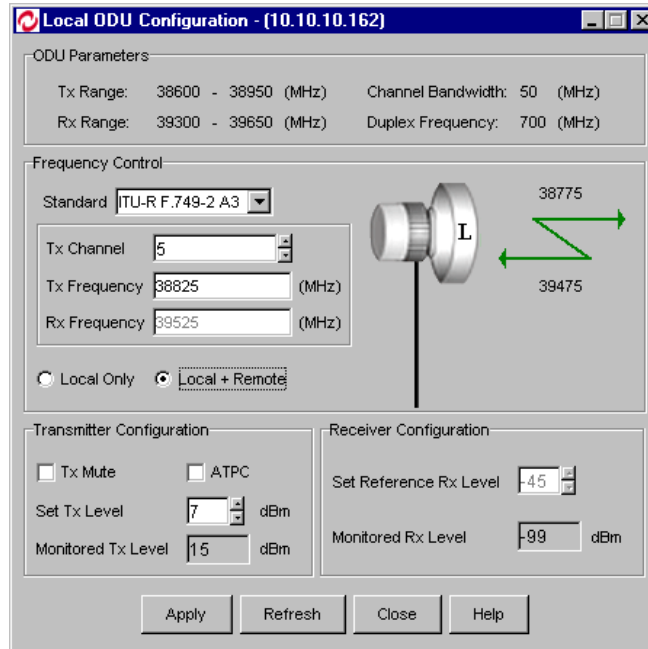


Figure 5-6 Local ODU Configuration Window

2. The **ODU Parameters** area is read-only.
3. In the **Frequency Control** area, select **Local Only** if you want to set the frequency only for the local side. Select **Local + Remote** to set the frequency for both sides of the link. (The Local + Remote option is available only when the link is operational.)
4. For **Tx Channel**, click the up/down arrows to select the frequency channel you want to use.
5. For **Tx Frequency**, enter the frequency at which the system will transmit.
6. The **Rx Frequency** field is read-only for frequencies above 8 GHz.  
For 7/8 GHz, values must be entered in the field.
7. In the **Transmitter Configuration** area, select **Tx Mute** to block transmission to the remote unit. By default, this option is not selected.  
Select **ATPC** to activate the Automatic Transmit Power Control feature.  
For **Set Tx Level**, enter or select the designated signal level. Possible range is -10 to max power level. By default, the transmit signal level is set to +15 dBm.  
The **Monitored Tx Level** field (read-only) displays the system's transmitted power level.
8. In the **Receiver Configuration** area, the **Reference Rx Level** field should be set to the desired Rx level in ATPC mode.  
The **Monitored Rx Level** field (read-only) displays the received power level.
9. Click **Apply** to save the settings.



10. Click **Close** to close the window.

## **Interfaces**

### *Interface Type*

**Note:** Each interface is configured in a different window.

1. Select **Configuration, Interfaces**.

The Interface Configuration window appears. (The figure below is the window for an STM1 interface.)

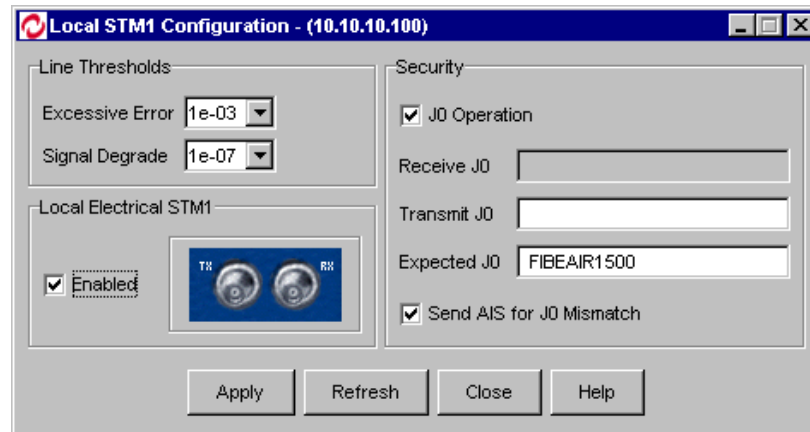


Figure 5-7 STM1 Interface Configuration Window

2. In the **Excessive Error** field, select the level above which a line Excessive BER alarm is issued for errors detected over the radio link.
3. In the **Signal Degrade** field, select the level above which a line Signal Degrade alarm is issued for errors detected over the radio link.
4. In the **Local Electrical STM1** field, select **Enabled** to activate the interface. Selecting Disabled will clear the line alarms.
5. In the **Security** area, select **J0 Operation** to use the J0 byte as a trace identifier in the SDH RSOH.

If you activate J0, use the **Transmit J0** and **Expected J0** fields to define the IDU identifier string, and select **Send AIS for J0 Mismatch**.

6. Click **Apply** to save the settings.
7. Click **Close** to close the window.

## System

### Trap Forwarding



1. Select **Configuration, System, Trap Forwarding**, or click the Trap Forwarding icon.

The Trap Forwarding Configuration window appears.

Managers				
	#1	#2	#3	#4
IP Address	0 .0 .0 .0	10 .10 .12 .22	0 .0 .0 .0	0 .0 .0 .0

Trap Filters				
	#1	#2	#3	#4
Power supply alarms	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Cable alarms	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Temperature alarms	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
External alarms	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Radio alarms	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Modem alarms	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Line alarms	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
SDH alarms	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
BER alarms	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
System fault alarms	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Maintenance alarms	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Standard traps	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Serial Line IP	
IP address	192.168.0 .1
Baud rate	19,200 bps
Modem phone number	0

Trap Options	
<input type="checkbox"/> Standard traps include serial number	
<input type="checkbox"/> Report local traps from remote IDU	
<input checked="" type="checkbox"/> Events are reported as traps	
CLLI	
Heartbeat period	1

Figure 5-8 Trap Forwarding Configuration Window

2. In the **Managers** section of the window, specify the IP addresses of the managers to which traps will be forwarded.
3. In the **Trap Filters** section, you determine which alarms will be sent as an SNMP trap to each manager.  
In each manager column, select the alarm types you want to include for that manager.
4. In the **Serial Line IP** area, the **IP Address** field shows the IP address of the modem or SLIP/IPP driver connected to the serial port.
5. In the **Baud rate** field, select the appropriate baud rate for serial port data transfer.
6. For **Modem phone number**, enter the number the modem will dial for serial data transfer.
7. In the **Trap Options** area, select **Standard traps include serial number** if you want trap messages to include the IDU serial number.
8. Select **Report local traps from remote IDU** if you want remote IDU trap messages to be reported locally.
9. Select **Events are reported as traps** if you want events to appear as trap messages.
10. For **CLLI** (Common Language Location Identifier), enter up to 18 characters that will represent your system ID when traps are sent.

11. For **Heartbeat period**, a heartbeat signal will be generated every x minutes (the number you enter in the field) to tell your system that the trap mechanism is working.
12. Click **Apply** to save the settings.
13. Click **Close** to close the window.

## NTP Configuration

NTP (Network Time Protocol) configuration is performed when an NTP server is used to synchronize network activity.

1. Select **Configuration, System, NTP**.

The NTP Configuration window appears.

The screenshot shows the 'NTP Configuration - (10.10.10.100)' window. It has a title bar with a red icon and standard window controls. The main area is divided into several sections. The first section contains 'NTP Server IP Address' (text box with '0 . 0 . 0 . 0'), 'NTP Update Interval' (spin box with '13' and 'Minutes' label), and 'Offset from GMT' (spin box with '4', a dropdown with '30', and 'Hour : Minutes' label). The second section contains 'Daylight Saving Time offset' (spin box with '0' and 'Hours' label), 'Daylight Saving Time Start' (text box with 'Configure' button), and 'Daylight Saving Time End' (text box with 'Configure' button). The third section contains 'Enable NTP Authentication' (checkbox, unchecked), 'Authentication Public Key' (text box with '52'), and 'Authentication Secret Key' (text box with '12', '111', '255', '122', '212', '214', '41', '255'). The bottom of the window has four buttons: 'Apply', 'Refresh', 'Close', and 'Help'.

Figure 5-9 NTP Configuration Window

2. Enter the IP of the NTP server.
3. For **NTP Update Interval**, use the up/down arrows to select the amount of time (minutes) between synchronization updates.
4. For **Offset from GMT**, use the arrow buttons and the drop-down list to select the amount of time required to compensate for offset from the GMT (Greenwich Mean Time).
5. For **Daylight Saving Time Offset**, click the arrow buttons to set the amount of time required to compensate for daylight saving.
6. For **Daylight Saving Time Start**, click **Configure** to set the beginning of the daylight saving time period.
7. For **Daylight Saving Time End**, click **Configure** to set the end of the daylight saving time period.
8. Select **Enable NTP Authentication** for secure access to the NTP server.

If you enable NTP, enter the **Authentication Public Key**, and the **Authentication Secret Key** numbers.

9. Click **Apply** to save the settings.
10. Click **Close** to close the window.

### In-band Configuration

In-band configuration is performed when you want to work with In-band Management. In-band Management refers to a method whereby the network management software sends management packets through the same network it is managing. This differs from out-of-band management in which the network management software uses a different network (overlay network) in order to communicate with the managed elements.

1. Select **Configuration, System, In-band**.

The In-band Configuration window appears.

Figure 5-10 In-band Configuration Window

2. Select **In-band Management Enabled** to activate In-band management.
3. For **Element Type**, click the drop-down list and select the desired element (Network Element or Gateway).
4. For **In-band Channel**, click the drop-down list and select the channel you want to use.
5. For **Time To Live (TTL)**, use the up/down arrows to select the desired value.
6. For **Gateway Ring Subnet Address**, enter the subnet address in the ring to which the gateway belongs.
7. For **Gateway Ring Subnet Mask**, enter the subnet mask of the gateway.
8. For **Line Interface**, click the drop-down list and select the desired value.
9. For **Network ID**, use the arrow buttons to select the desired value.
10. In the second area of the window, enter the relevant IP addresses and masks.
11. Click **Apply** to save the settings.

- Click **Close** to close the window.

## Alarms Menu

### Current Alarms



- Select **Alarms**, **Current Alarms**, or click the Current Alarms icon.

The Current Alarms window appears.

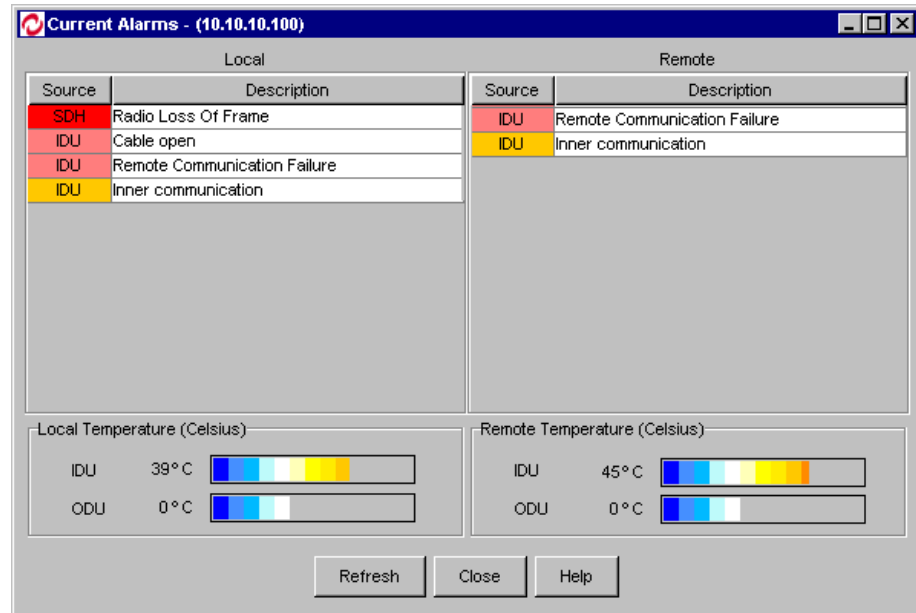


Figure 5-11 Current Alarms Window

Each line in the window describes a different alarm for the local and remote units.

The alarm type appears in the **Source** column.

The color in the Type column indicates the severity of the alarm, as follows:

<b>Red</b>	Major alarm
<b>Orange</b>	Minor alarm
<b>Yellow</b>	Warning
<b>Blue</b>	Event

In addition to the current alarms, the current IDU and ODU temperatures are shown at the bottom of the window.

## Alarm Log



1. Select **Alarms**, **Alarm Log**, or click the Alarm Log icon.

The Alarm Log window appears.

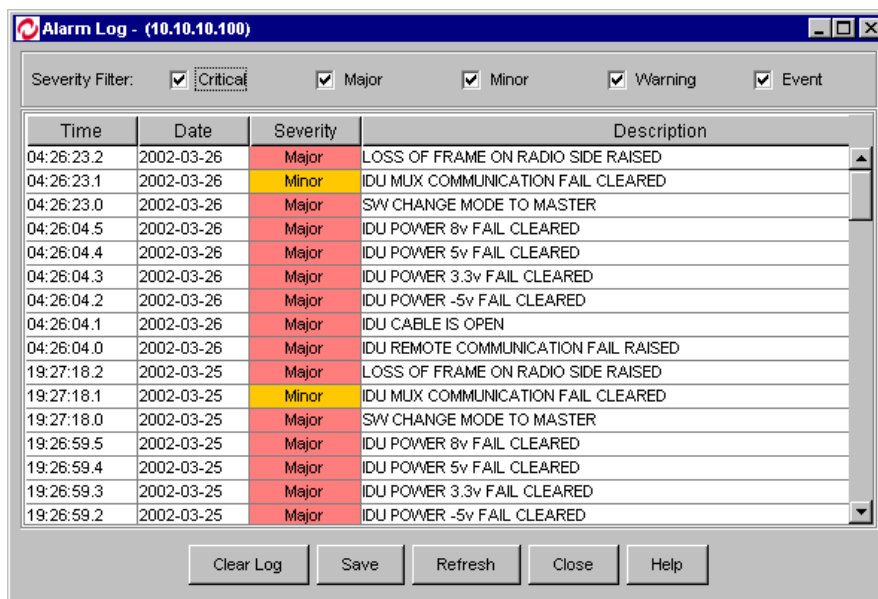


Figure 5-12 Alarm Log Window

When the system reaches 80% capacity, it automatically saves the current alarms in a log file. The files are stored in the directory C:\CERAVIEW\LOG, whereby C:\CERAVIEW is the directory in which you installed the CeraView software.

The Alarm Log window displays the following information:

**Time** - The time the alarm was triggered.

**Date** - The date the alarm was triggered.

**Severity** - The severity of the alarm. You can determine which severity levels will be displayed in the window by selecting the levels at the top of the window.

**Description** - A description of the alarm, and its status (RAISED, CLEARED).

To clear the log file, click **Clear Log**.

To close the window, click **Close**.

### Save Alarms to File

To save current alarms to a file, select **Alarms**, **Start Saving Log**.

In the Choose Alarm Log File window that appears, select the file you want to save the alarms to and click **Save**.

## Performance Menu

### Radio

### RSL

The RSL Performance Monitoring window displays received signal level values measured over the past 24 hours.

1. Select **Performance, Radio, Local/Remote RSL**.

The Local or Remote RSL Monitoring graphic window appears.

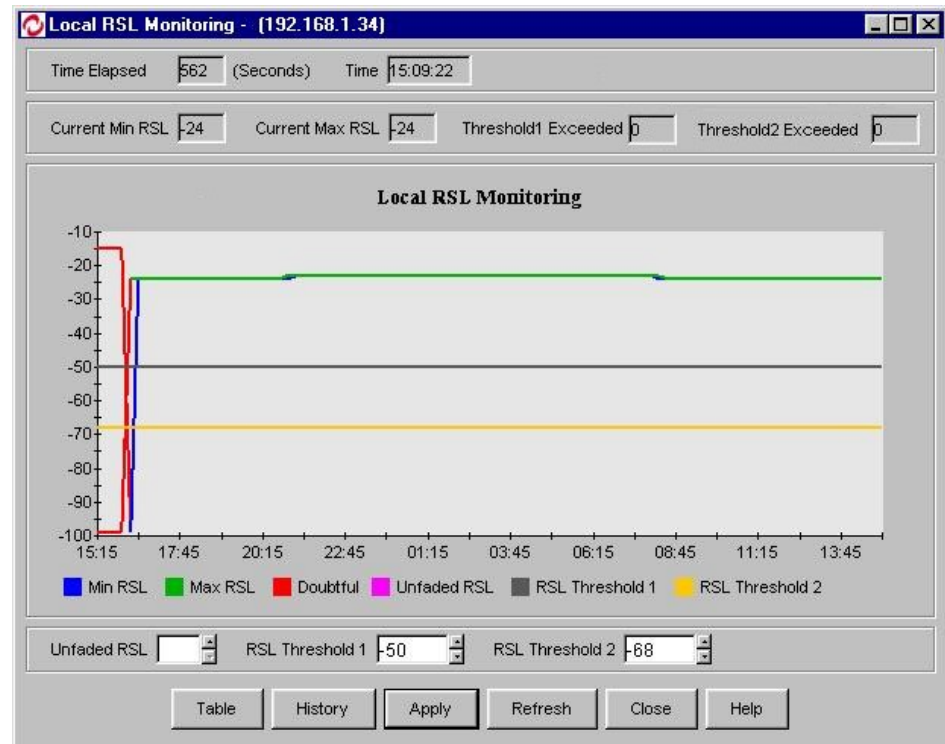


Figure 5-13 RSL Monitoring Graphic Window

Min RSL values are the minimum received level measured during the interval.

Max RSL values are the maximum received level measured during the interval.

RSL Threshold 1 and RSL Threshold 2 are values that you can set. When an RSL value exceeds the thresholds you set, the Threshold Exceeded counters at the top of the PM window will register and display the number of seconds the threshold values were exceeded.

Doubtful values are values that were not generated during normal system operation.

For example, the values may have been generated during a system reset or failure.

2. To view Historical RSL values, click **History**.

Summarized data for current day:

Date: 15-Jul-09    Min RSL: -15    Max RSL: -99    Threshold 1 Exceed: 0    Threshold 2 Exceed: 0

Date	Min RSL	Max RSL	Threshold 1 Exceed	Threshold 2 Exceed
14-Jul-09	-15	-99	0	0
13-Jul-09	-15	-99	0	0
12-Jul-09	-15	-99	0	0
11-Jul-09	-15	-99	0	0
10-Jul-09	-15	-99	0	0
09-Jul-09	-15	-99	0	0
08-Jul-09	-15	-99	0	0

Buttons: Save, Refresh, Close, Help

Figure 5-14 RSL History Window

The values shown in the columns are values that were received over the last 24 hours.

- To view current RSL values in table format, click **Table**.

Time	Date	Min RSL	Max RSL
13:15	26-Mar-02	-15	-99
13:00	26-Mar-02	-15	-99
12:45	26-Mar-02	-15	-99
12:30	26-Mar-02	-15	-99
12:15	26-Mar-02	-15	-99
12:00	26-Mar-02	-15	-99
11:45	26-Mar-02	-15	-99
11:30	26-Mar-02	-15	-99
11:15	26-Mar-02	-15	-99
11:00	26-Mar-02	-15	-99
10:45	26-Mar-02	-15	-99
10:30	26-Mar-02	-15	-99
10:15	26-Mar-02	-15	-99
10:00	26-Mar-02	-15	-99
09:45	26-Mar-02	-15	-99
09:30	26-Mar-02	-15	-99
09:15	26-Mar-02	-15	-99
09:00	26-Mar-02	-15	-99
08:45	26-Mar-02	-15	-99

Buttons: Graph, Close, Save

Figure 5-15 RSL Monitoring Table Window

The RSL Monitoring table window displays details about the received radio signal over the last 24 hours, in 15 minute intervals.

The Min RSL column shows the minimum received level measured during the interval.

The Max RSL column shows the maximum received level measured during the interval.

## TSL

The TSL Performance Monitoring window displays details about the transmitted signal level measured every 15 minutes over the last 24 hours.

- Select **Performance, Radio, Local/Remote TSL**.

The Local or Remote TSL Monitoring graphic window appears.



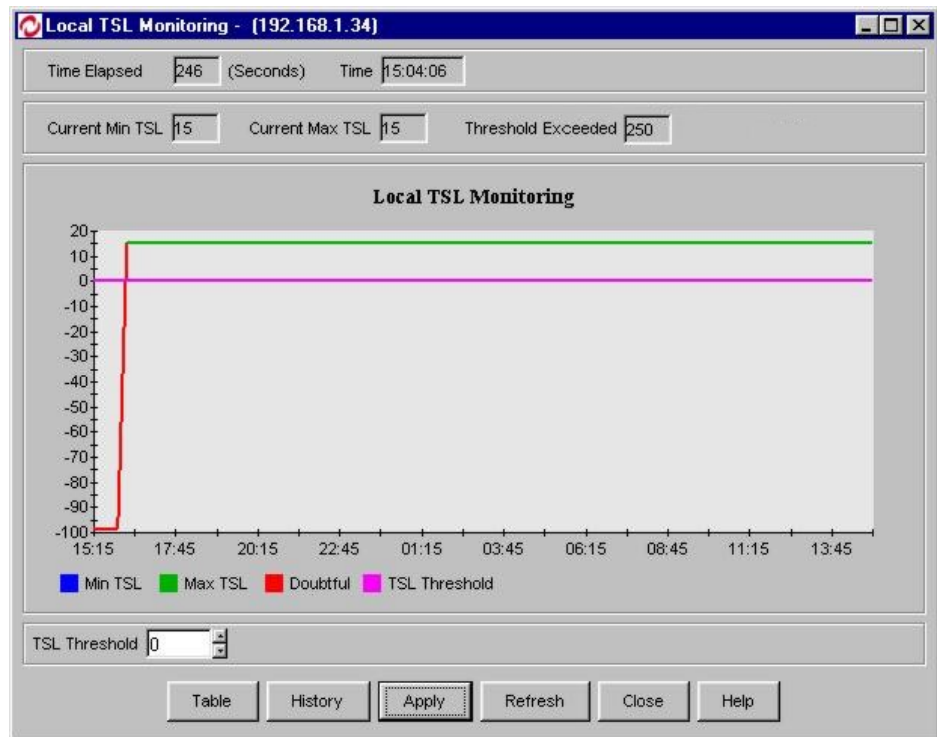


Figure 5-16 TSL Monitoring Graphic Window

Min TSL values are the minimum transmitted level measured during the interval.

Max TSL values are the maximum transmitted level measured during the interval.

TSL Threshold is a value that you can set. When a TSL value exceeds the threshold you set, the Threshold Exceeded counter at the top of the PM window will register and display the number of seconds the threshold value was exceeded.

Doubtful values are values that were not generated during normal system operation.

For example, the values may have been generated during a system reset or failure.

2. To view Historical RSL values, click **History**. The values shown in the window that appears are values that were received over the last 24 hours.
3. To view TSL values in table format, click **Table**. The format of the table is similar to the RSL table described above.

## SDH

The SDH Performance Monitoring window displays the number of radio UAS (unavailable seconds), measured every 15 minutes over the last 24 hours.

1. Select **Performance, Radio, Local/Remote SDH**.

The Local or Remote SDH Monitoring graphic window appears.

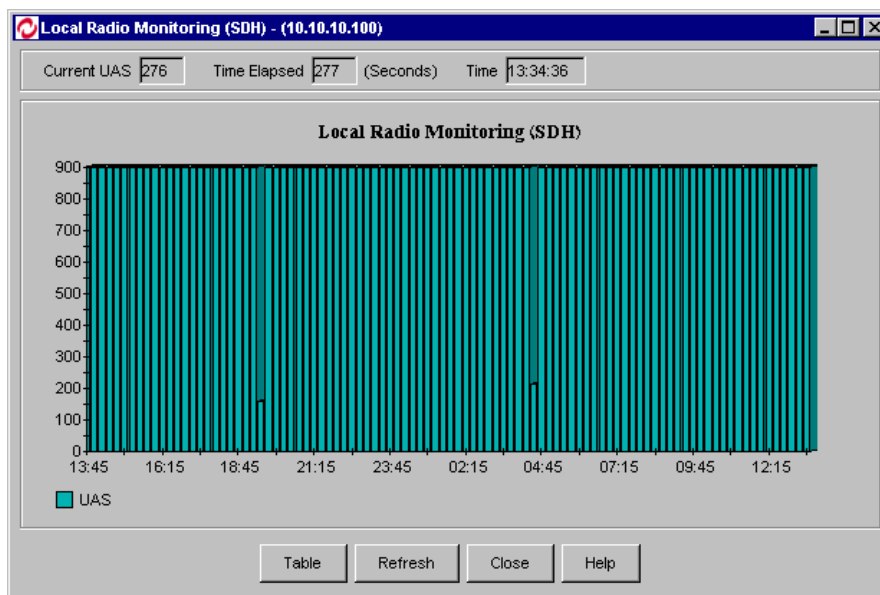


Figure 5-17 SDH Monitoring Graphic Window

The UAS value can be between 0 and 900.

The Time Elapsed field displays the number of seconds since the current monitoring period commenced.

- To view UAS values in table format, click **Table**. The format of the table is similar to the RSL table described above.

## Tributaries

### Local

The Tributaries Performance Monitoring window displays the UAS (number of Unavailable Seconds per interval) measured every 15 minutes over the last 24 hours, on the E1/T1 interface.

- Select **Performance, Tributaries, E1 #**

The Local Tributary Monitoring graphic window appears.

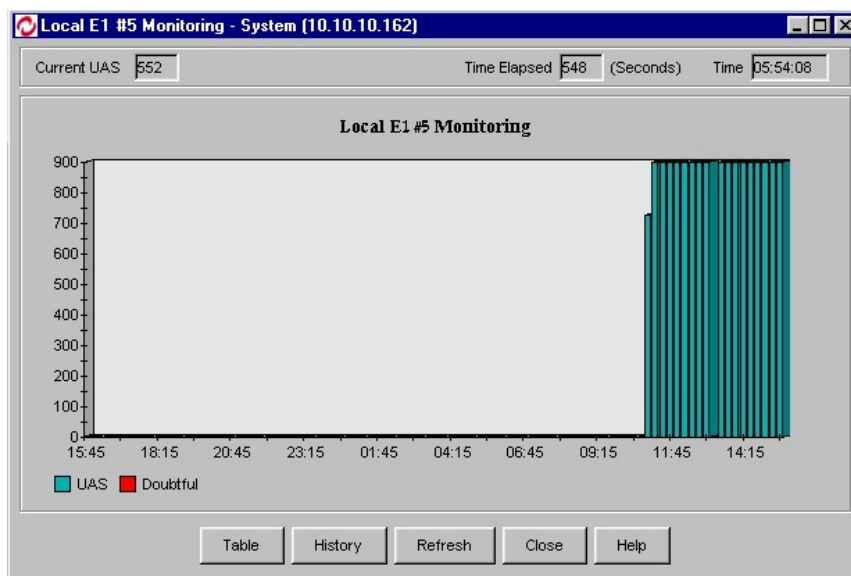
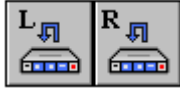


Figure 5-18 Tributary Monitoring Graphic Window

2. To view historical UAS values, click **History**. The values shown in the window that appears are values that were received over the last 24 hours.
3. To view UAS values in table format, click **Table**. The format of the table is similar to the RSL table described above.

## Maintenance

### Loopback



1. Select **Maintenance, Loopback, Local/Remote**, or click the Local/Remote Loopback icon.

The Loopback window appears.

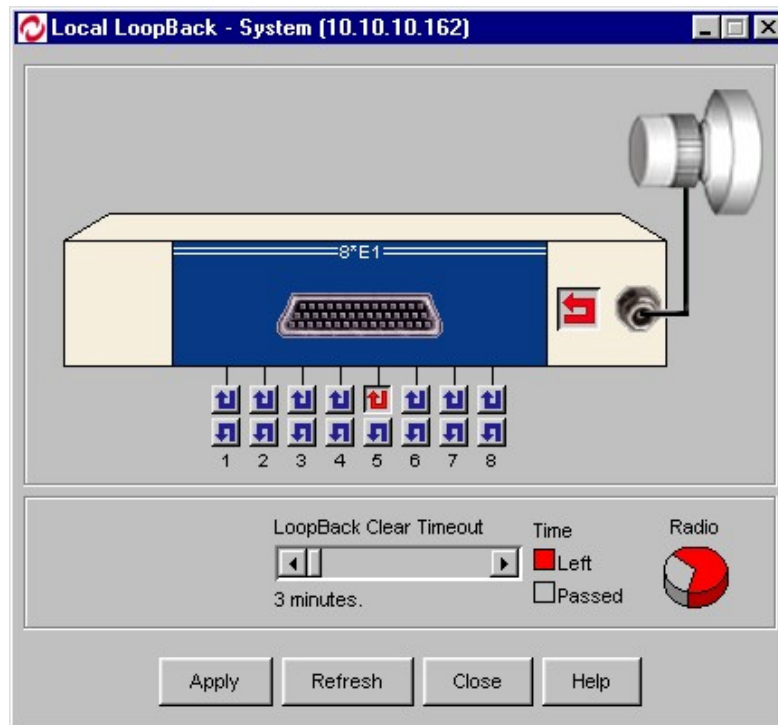





Figure 5-19 Loopback Window

Loopback test types depend on the type of interface in use. In the example shown above, you can click the button on the right side  to perform an internal IDU loopback test. For each E1 line, you can click the up arrow button  to perform an internal tributary test, or the down arrow button  to perform an external tributary test.

Set the **LoopBack Clear Timeout** scale to the amount of time you want the test to run.

When a radio or line loopback test is running, a pie graph displayed to the right of the timeout scale shows how much time is left for the test (as shown in the figure above).

Click **Apply** to run the test.

When you are done with loopback testing, click **Close** to close the window.

*Note that closing the window will not stop the loopback test. To stop a test, unmark it by clicking on the relevant arrow button, and then click Apply.*

**Software Reset**

Select **Maintenance, Software Reset, Local** or **Remote** to reset the IDU agent software for maintenance purposes.

**Clear PM**

To clear the Performance Monitoring log files, select **Maintenance, Clear PM, Local** or **Remote**.

**Force Remote Tx Level**

To force the remote transmission level to the level you set for the local IDU, select **Maintenance, Force Remote Tx Level**.

**Force Remote Mute Off**

To cancel the muting of the remote ODU, select **Maintenance, Force Remote Mute Off**.

## CeraView for FibeAir 1500A/1528A

The following sections describe the CeraView application for FibeAir 1500A/1528A.

To log in to CeraView, see the section *Logging in to CeraView* at the beginning of this chapter.

After you log in to CeraView, the Main window appears.

### Main Window

The Main window is your starting point for all operations.

Below is a description of the menus, toolbars and other features of the Main window.



Figure 5-1 CeraView for FibeAir 1500A/1528A Main Window

### Title Bar

The Title Bar displays the CeraView version and the IP address of the IDU being accessed.











### Menu Bar

The Menu Bar contains menus and menu items used to perform CeraView operations.

### Toolbar

The Toolbar includes several icons that you can click to perform different operations.

Each icon in the Toolbar is described in the table below.

Icon	Operation
	<i>System Information</i> - used to view and define system information, such as contact personnel and system up time.
	<i>Trap Forwarding Configuration</i> - used to designate managers to which traps will be forwarded.
	<i>Current Alarms</i> - used to view current active alarms.
	<i>Alarm Log</i> - used to view historical alarm records.
	<i>Input/Output External Alarms</i> - used to configure alarms sent to/from external sources.
	<i>ODU Configuration</i> - used to configure the local and remote ODUs.
	<i>Transport Configuration</i> - used to configure local and remote radio, line, RSOH, and security parameters.
	<i>Loopback</i> - used to configure and run local and remote loopbacks for testing and troubleshooting.
	<i>Trail Configuration</i> - used to configure the tributaries.
	<i>Online Help</i> - used to view the online help file.

## Physical View

A physical view of the FibeAir unit is displayed in the Main window. The view provides a real-time virtual display of the IDU front panel.



Figure 5-2 Physical View in Main Window

The LEDs that appear on the left side in the physical view indicate the actual real-time status of the LEDs on the front panel of the IDU. (LED changes on the actual front panels of the units will be updated in the physical views after a slight delay.)

The LED colors are as follows:

**Green** - indicates proper operation

**Yellow** - indicates a warning

**Red** - indicates a major alarm or severe malfunction

The following table lists the LEDs and their indications.

LED	Color			Description
	Red	Yellow	Green	
Power	X		X	<b>Red</b> - power supply problem, system not functional
Line	X	X	X	<b>Red</b> - no input to main channel / High BER <b>Yellow</b> - J0 mismatch
LOF (Loss of Frame)	X		X	<b>Red</b> - radio did not recognize information frame (radio link problem/radio LOF)
BER (Bit Error Ratio)	X	X	X	<b>Red</b> - radio BER higher than radio excessive error threshold definition (see Sonet/SDH configuration window) <b>Yellow</b> - radio BER higher than radio signal degrade threshold definition (see Sonet/SDH configuration window)
LPBK (Loopback)	X		X	<b>Red</b> - loopback is active
STBY (Standby)		X	X	<b>Yellow</b> - Protected configuration. The unit is currently passive or Tx mute is operating
IDU	X	X	X	<b>Red</b> - modem unlocked <b>Yellow</b> - high temperature / fan problem
ODU	X	X	X	<b>Red</b> - no link / ODU power / ODU unlocked <b>Yellow</b> - radio interference / high temperature / Rx/Tx out of range
CBL (Cable)	X		X	<b>Red</b> - RF cable open / RF cable short
RMT (Remote Unit)	X	X	X	<b>Red</b> - no link / remote unit problem (red LED is lit in the remote unit) <b>Yellow</b> - warning in remote unit (yellow LED is lit in the remote unit)
8xE1/T1			X	<b>Green</b> - Connected E1/T1 tributary

## Menus

The following sections describe the CeraView window menus.

### File Menu

This option allows you to view and define information for the FibeAir system.



1. Select **File, System Information.**, or click the System Information icon.  
The System Information window appears.

 A screenshot of a web-based window titled "System Information - (10.10.10.100)". The window has a blue title bar and standard window controls. The main content area is divided into several sections:
 

- Current Time:** A text box showing "Mon Mar 25 17:14:48 IST 2002" and a "Configure Time" button.
- System Parameters:** A section with several text boxes: "Description" (FibeAir 1500 agent), "Name" (empty), "Contact" (empty), "Location" (empty), and "Up Time" (4 days, 0 hours, 7 minutes, 35 seconds).
- Software Versions:** A section with three text boxes: "IDU" (4.09v), "ODU" (empty), and "MUX" (M3.57pdA067).
- Serial Numbers:** A section with two text boxes: "IDU" (empty) and "ODU" (empty).
- Link Parameters:** A section with one text box: "Link ID" (123).

 At the bottom of the window, there are four buttons: "Apply", "Refresh", "Close", and "Help".

Figure 5-3 System Information Window

2. In the **Current Time** area, click **Configure Time** and set the time in the format HH:MM:SS.
3. The read-only **Description** field provides information about the FibeAir system.
4. (Optional) In the **Name** field, enter a name for this link. By convention, this is the node's fully-qualified domain name.
5. (Optional) In the **Contact** field, enter the name of the person to be contacted when a problem with the system occurs. Include information on how to contact the designated person.
6. (Optional) In the **Location** field, enter the actual physical location of the node or agent.
7. The **Up Time** field, **Software Versions** area, and **Serial Numbers** area are read-only.



8. For **Link ID**, enter the ID of the link you are working with.
9. Click **Apply**.  
The settings are saved.
10. Click **Close**.

### Open Remote

Select this item to access the remote side of the link. If you select this item, a window appears prompting you to enter the IP address of the remote unit.

### Exit

Select this item to exit the CeraViewr application. You can also exit by clicking on the Close icon (x) in the title bar.

When you exit CeraView, you will be prompted to confirm the exit. Click **OK** to confirm the operation.

## Configuration Menu

### IDU

#### External Alarms

The procedure detailed in this section is required only if alarms generated by external equipment are connected to the IDU, or if the IDU alarm outputs are connected to other equipment (using the alarms I/O connector).



1. Select **Configuration, IDU, External Alarms**, or click the **External Alarms** icon.

The External Alarms window appears.

External alarm inputs				Alarm outputs	
Alarm	Enable	Text	Severity	Relay	Severity
1	<input checked="" type="checkbox"/>		Event	1	Power
2	<input checked="" type="checkbox"/>	EXTERN ALARM 2	Minor	2	Major
3	<input checked="" type="checkbox"/>		Minor	3	Minor
4	<input type="checkbox"/>	smul	Minor	4	Power
5	<input checked="" type="checkbox"/>	ALEX	Event	5	Power
6	<input checked="" type="checkbox"/>	OREN	Event		
7	<input checked="" type="checkbox"/>		Major		
8	<input checked="" type="checkbox"/>		Major		

Figure 4-1 Input/Output External Alarms Window

The microcontroller in the IDU reads alarm inputs (dry contact) and transmits them to the CeraView management system. This allows FibeAir to report external alarms that are not related to its own system.

For each alarm on the left side of the window, do the following:

2. Click on the box next to the alarm number to enable/disable the alarm.
3. If you enable an alarm, enter a description of the alarm in the text field.
4. Select the alarm's severity level from the drop-down list (Major, Minor, Warning, or Event).
5. FibeAir provides five alarm outputs that can be used by other systems to sense FibeAir alarms. The outputs are configured on the right side of the window.

The alarm outputs are Form C Relays. Each output relay provides three pins, as follows: Normally Open (NO), Normally Closed (NC), Common (C).

Output alarms can be defined as Major, Minor, Warning, External, Power, BER, Line, Loopback, LOF, IDU, ODU, Cable, or Remote.

The default alarm output setting for all relays is "Power".

The relays may be connected to customer-specific applications. Refer to Appendix B for details concerning the alarm connector pin assignments.

5. After you complete the external alarm configuration, click **Apply** to save the settings.
6. Click **Close**.

The window is closed and you are returned to the Main window.

## Transport

The Transport Configuration window allows you to change threshold levels for the radio and alarms, and to configure special transmission parameters. This is recommended for advanced users only.



1. Select **Configuration, IDU, Transport**, or click the Transport Configuration icon.

The Transport Configuration window appears.

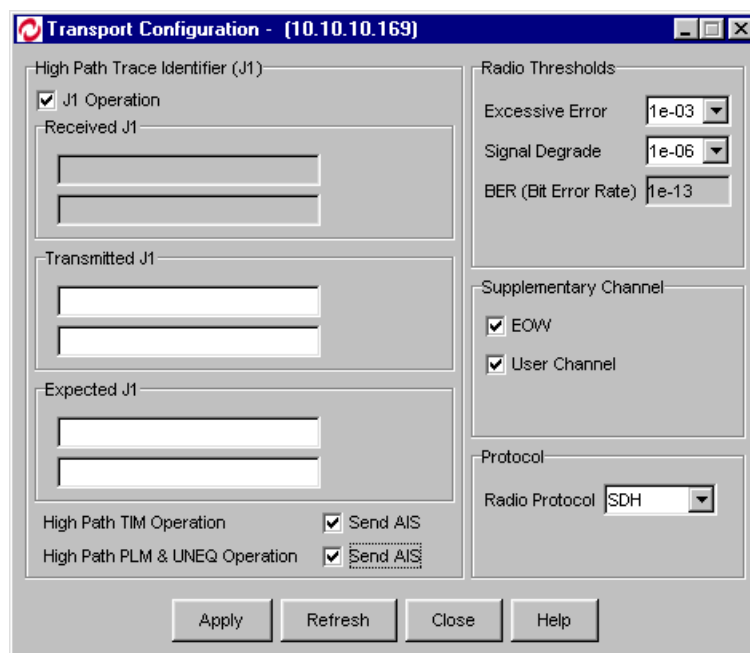


Figure 4-2 Transport Configuration Window