2. In the **High Path Identifier (J1)** area, select **J1 Operation** to enable the identifier.

   J1 is used to continuously transmit a Path Access Point Identifier so that a path receiving terminal can verify its ongoing connection to the intended transmitter.

   Received J1 displays the identifier that is receieved for verification.

   For **Transmitted J1**, specify the J1 identifier that will be transmitted to the receiver.

   For **Expected J1**, specify the identifier that you expect to receive.

   For **High Path TIM Operation**, select **Send AIS** if you want Alarm Indication Signals to be sent in the event of TIM (Trace Identification Mismatch).

   For **High Path PLM & UNEQ Operation**, select **Send AIS** if you want Alarm Indication Signals to be sent in the event of PLM (Path Label Mismatch) or UNEQ.

3. In the Radio Thresholds area, for **Excessive Error**, select the level above which an Excessive BER alarm is issued.

   For **Signal Degrade**, select the level above which a Signal Degrade alarm is issued.

4. In the **Supplemetary Channel** area, select **EOW** (Enginnering Order Wire) or **User Channel** (64 Kbps).

5. For **Protocol**, select the protocol your radio is using.

6. Click **Apply** to save the settings.

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

General ADM Configuration

1. Select **Configuration**, **IDU**, **General ADM**.

   The General ADM Configuration window appears.

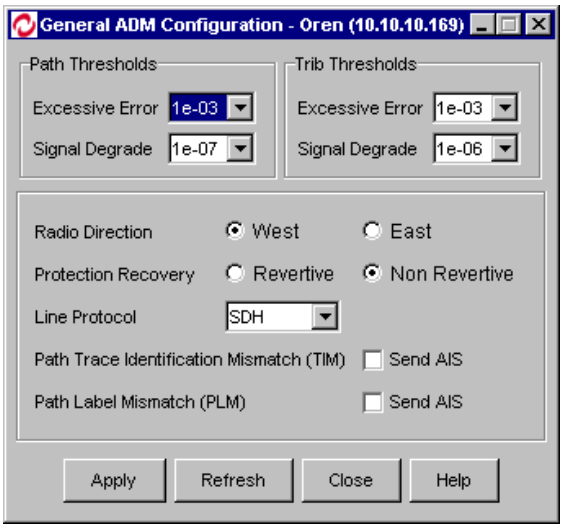


Figure 5-4 General ADM Configuration Window

2. In the **Path Thresholds** and **Trib Thresholds** areas, for **Excessive Error**, click the drop-down list and select the level above which an Excessive BER alarm is issued for errors detected over the radio link.

   For **Signal Degrade**, select the level above which a Signal Degrade alarm is issued for errors detected over the radio link.

3. Select the direction of the FibeAir radio.

4. The **Protection Recovery** options are as follows:

   Revertive - In this mode, normal traffic on the protection path is switched back to the original path after it is recovered from the fault.

   Revertive mode may be required to support specific services, whereby the shortest physical route offers better performance. For example, for synchronization of another network using protected E1. The main path will generally be shorter, and the protection path will be longer.

   Non-Revertive - In this mode, no switching to the original fault-cleared path is performed, to prevent unnecessary traffic hits and management event reports.

5. For **Line Protocol**, select SDH, Sonet, Sonet-C, or SDH-C.

6. For **Path Trace Identification Mismatch**, select **Send AIS** if you want Alarm Indication Signals to be sent in the event of TIM (Trace Identification Mismatch). (See explanation below.)

7. For **Path Label Mismatch**, select **Send AIS** if you want Alarm Indication Signals to be sent in the event of PLM (Path Label Mismatch). (See explanation below.)

8. Click **Apply** to save the settings.

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

Explanation of TIM Events

SDH provides path trace capability on different levels, as follows:

Regenerator Section Trace - J0
J0 is used to continuously transmit a Section Access Point Identifier so that a section receiver can verify its ongoing connection to the intended transmitter. In the FibeAir radio, the J0 byte is used for **Link ID**.

Path Trace - J1
J1 is used to continuously transmit a Path Access Point Identifier so that a path receiving terminal can verify its ongoing connection to the intended transmitter.

Path Trace - J2
J2 is used to continuously transmit a Low Order Path Access Point Identifier so that a path receiving terminal can verify its ongoing connection to the intended transmitter.

J2 allows the user to verify VC-12 paths, which is useful as a means of checking radio/optical connections whenever changes are made. The path trace ID can be determined by the user for VC-12 trails in each direction (receive/transmit) separately. The user can also display the actual received pattern for maintenance purposes.

The incoming string is checked against the expected receive string. A discrepancy between the strings generates a TIM alarm or an AIS, depending on what you decide for Path TIM Operation in the General ADM Configuration window.

If the trail is protected and you selected the AIS option, a switch to the protection path will be performed in the event of TIM, since AIS is one of the criteria for switching to protection.

Explanation of PLM Events

The SDH path overhead includes signal label information that indicates the composition of the signal. For FibeAir1500A/1528A, the signal labels are automatically set according to the traffic on/off status, as defined in the table below. If the received signal label is not as expected, a PLM alarm is generated.

Signal Label Data

VC Level	Value	Traffic On	Traffic Off
VC-12 (bits 5-7 of V5)	Transmit Value	010 - asynchronous floating	000 - unequipped
	Expected Receive Value	010 - asynchronous floating or 001 - equipped non-specific	000 - unequipped
VC-3 (C2 byte)	Transmit Value	04_H - asynchronous mapping of 34/45 Mbit/s	00_H - unequipped
	Expected Receive Value	04_H - asynchronous mapping of 34/45 Mbit/s or 01_H - equipped non-specific	00_H - unequipped

Trail

The Trail Table maps the VCs (Virtual Containers) representing the E1 lines.

Using this table, you can set several parameters for each line, such as the path name and protected configuration.

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

   The Trail Configuration window appears.

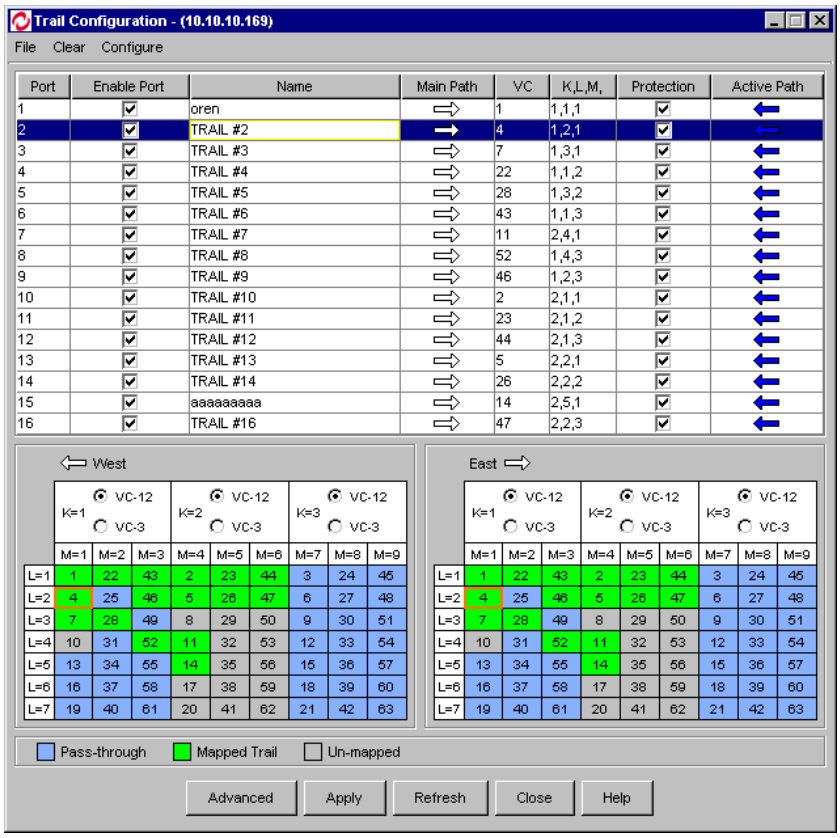


Figure 5-5 Trail Table Window

The table lists up to 16 E1 tributary lines. The VC map section of the table displays 63 VCs (entire STM-1 capacity) and the status of each, represented by different colors. Gray represents an unused VC, Green represents a VC used by an E1 trail, and blue represents a VC designated as *pass-through* (passes the relay frame as is).

Note that VC-3 trails can only be configured as *pass-through*.

2. For each trail, select or deselect the **Enable Port** box. Deselecting the box will block all traffic on that E1/T1 line.
3. In the **Name** column, click in the text box and enter the name you want for that E1/T1 line.
4. In the **Main Path** column, click in the box and select either east or west for the main path.
5. The **VC** and **K,L,M** columns are read-only. The values in those columns represent the Virtual Container mapping for the E1/T1 tributary lines.

6. In the **Protection** column, mark the box if you want the tributary line to run in Protected mode, whereby traffic will be delivered in both directions.
7. The **Active Path** column shows the current active path.
8. In the **West** and **East** sections of the window, select the payload type for each K number.
9. For each VC box, you can right-click the mouse to change the bi-directional connection of the line, as follows:

   Clear — No connection (the channel is not in use).

   No low order path (LP) alarms and TU alarms (TU-LOP and TU-AIS) will be reported, and no PM (Performance Monitoring) logs will be generated for the channel.

   Map Trail — A tributary signal is connected to a specific channel (TU) in the STM-1 signal. For non-protected connections, the tributary is connected to one of the aggregate ports. For protected connections, the tributary is connected to two aggregate ports for path protection.

   Note that for protected connections, the same channel number must be used for the two aggregates.

   Pass-Through — Matching channels are connected from one aggregate to the other.

10. For advanced trail parameters, select a trail and click **Advanced**.

    The Advanced Parameters window appears.

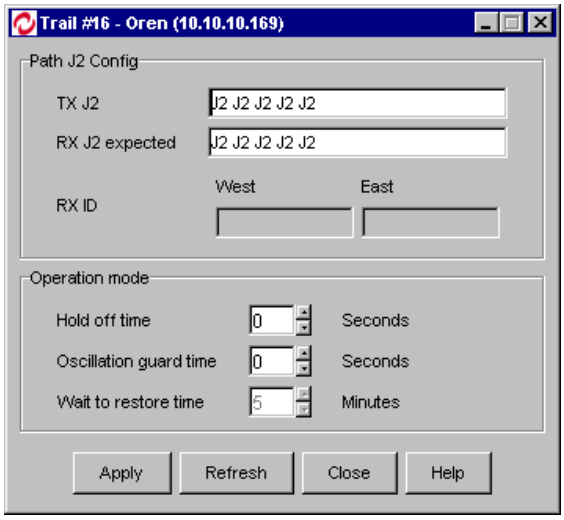


Figure 5-6 Advanced Trail Table Window

11. In the Advanced Parameters window, click in the **TX J2** field, and enter the transmitted path trace ID string.
12. In the **RX J2 Expected** field, enter the expected path trace ID string.
13. The **RX ID** field is read-only. For protected trails, it displays the actual received pattern from both directions. For non-protected trails it displays the actual received pattern from one direction.
14. For **Hold off Time**, use the arrow buttons to set the delay period between fault detection and path switching. The value can be from 0 to 10 seconds. The default is 0 seconds.

15. For **Oscillation Guard Time**, use the arrow buttons to set the period of time the inactive channel must be free of faults before it can carry traffic again. The value can be from 0 to 60 seconds. The default is 0 seconds.
16. For **Wait to Restore Time**, use the arrow buttons to set the period of time from switching to the protection path, back to the main path. This parameter is only relevant when the *Revertive* mode is active. The value can be from 5 to 12 minutes. The default is 5 minutes.
17. Click **Apply** to save the changes.
18. Click **Close** to close the window and return to the Trail Table window.
19. In the Trail Table window, click **Apply** to save the changes.
20. Click **Close** to close the window.

Synchronization

Synchronization configuration enables you to set values for the network's clock synchronization.

1. Select **Configuration**, **IDU**, **Synchronization**., or click the **Clock** area in the CeraView main window FibeAir physical view.

   The Synchronization Configuration window appears.

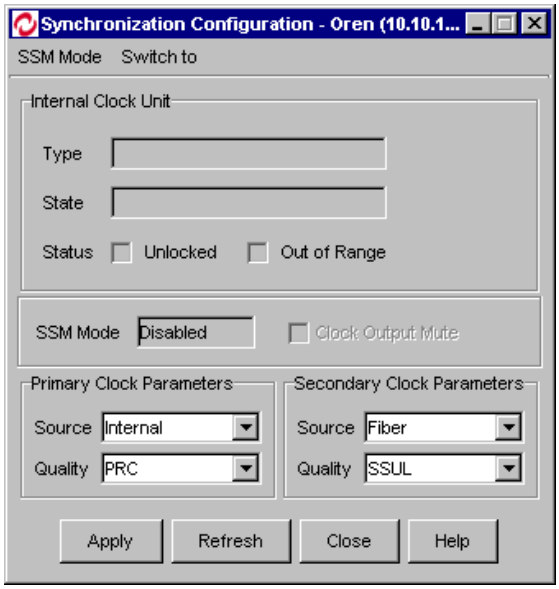


Figure 5-7 Synchronization Configuration Window

2. The **Internal Clock Unit** area displays the current clock unit type, state, and status. The type can be ST-3E, ST-3, or Sec.

   The status can be **Unlocked**, which indicates that the clock source is not locked to the primary or secondary path, or **Out of Range**, which indicates that the unit cannot be synchronized with the external clock signal. When this occurs, an Out of Range alarm is generated.
3. To enable/disable the SSM mode, click the **SSM Mode** menu and select enable or disable.

   Note that if the SSM mode is not enabled, each network element will need to determine the clock quality on its own.

4. In the **Primary Clock Parameters** area, for **Source**, click the drop-down list and select the clock source, which can be one of the following:
   - Internal
   - External 1.544 MB
   - Radio
   - Fiber
   - External 2MHz
   - External 1 and half MB
   - Tributary # (1-16)
5. The **Quality** parameter is used to set the quality level of the clock signal. Click the drop-down list and select the level, which can be one of the following:
   - PRC
   - SSUT
   - SSUL
   - SEC
   - STU
   - DNU
6. Repeat steps 4 and 5 for the **Secondary Clock Parameters** area.
7. Select **Clock Output Mute** if you do not want the internal clock to be used to synchronize other network elements.
8. Click **Apply** to save the settings.
9. Click **Close** to close the window.

ODU

1. Select **Configuration**, **ODU**, or click the ODU Configuration icon.

   The ODU Configuration window appears.

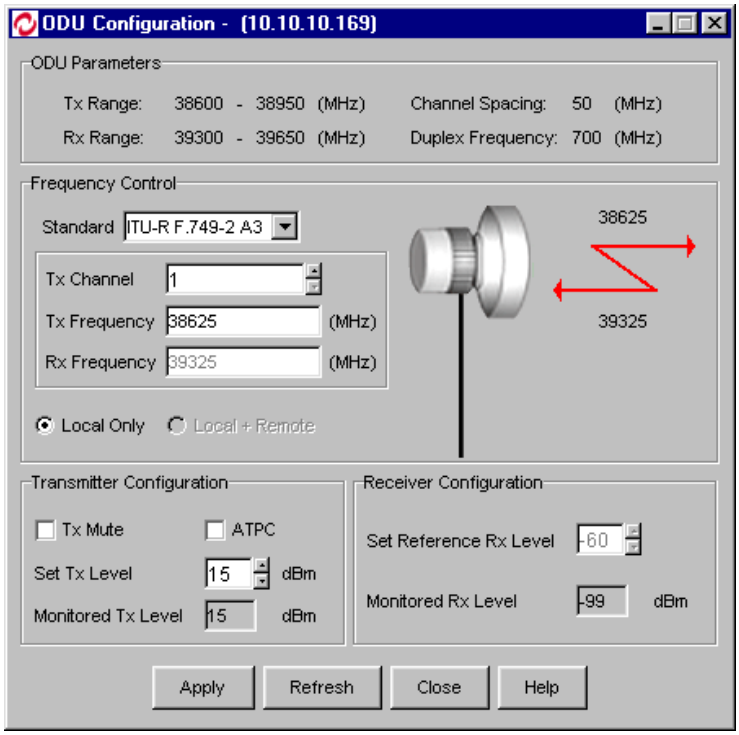


Figure 5-8 ODU Configuration Window

2. The **ODU Parameters** area is read-only.
3. For **Tx Channel**, click the up/down arrows to select the frequency channel you want to use.
4. For **Tx Frequency,** enter the frequency at which the system will transmit.
5. 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 the maximum power level (+15 to +22dBm, according to the frequency band).

   The **Monitored Tx Level** field (read-only) displays the system's transmitted power level.
6. In the **Receiver Configuration** area, the **Reference Rx Level** field should be set to the Rx level to which the actual level will be compared.

   The **Monitored Rx Level** field (read-only) displays the received power level.
7. Click **Apply** to save the settings.
8. Click **Close** to close the window.

Interfaces

STM1

1. Select **Configuration, Interfaces**, **STM1**, or click the **STM1** area in the physical view of the CeraView main window.

   The STM1 Configuration window appears.

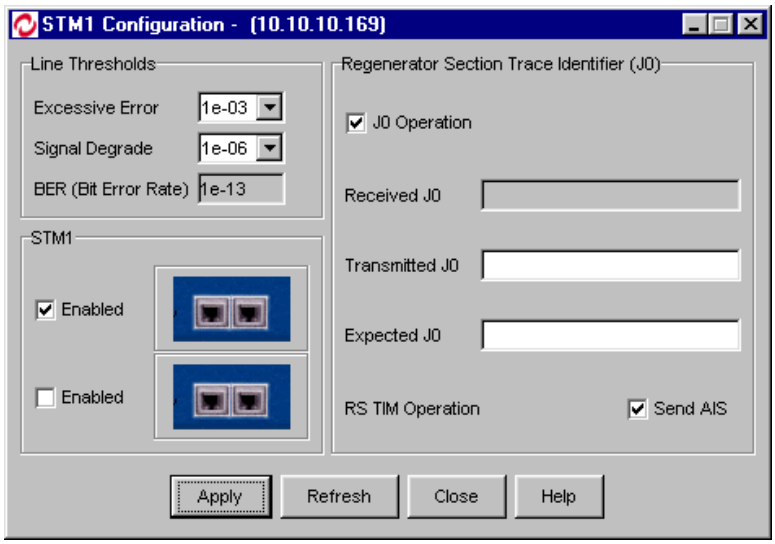


Figure 5-9 STM1 Interface Configuration Window

2. In the **Excessive Error** field, select the level above which an Excessive BER alarm is issued for errors detected over the radio link.
3. In the **Signal Degrade** field, select the level above which a Signal Degrade alarm is issued for errors detected over the radio link.
4. In the **BER** field, select the level above which a BER alarm is issued for errors detected over the radio link.
5. In the **STM1** field, select **Enabled** to activate the interface.
6. In the **Regenerator Section Trace Identifier** area, select **J0 Operation** to use the J0 byte as a trace identifier in the SDH RSOH.

   If you activate J0, use the **Transmitted J0** and **Expected J0** fields to define the IDU identifier string.

   Select **Send AIS** for **RS TIM Operation**.
7. Click **Apply** to save the settings.
8. Click **Close** to close the window.

E1

1. Select **Configuration, Interfaces**, **E1**, or click the **8xE1** area in the CeraView main window FibeAir physical view.

   The E1 Ports Configuration window appears.

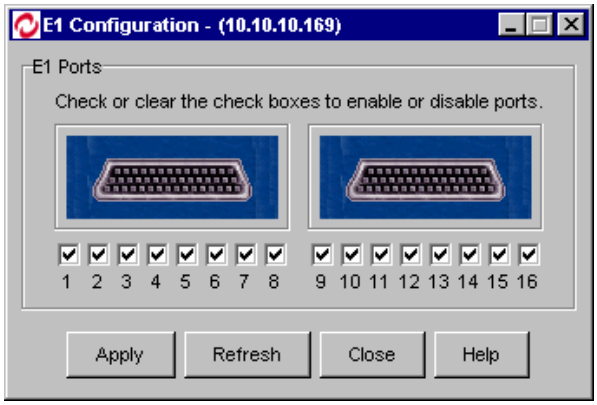


Figure 5-10 E1 Ports Configuration Window

2. Select or deselect the boxes to enable or disable the ports.
3. Click **Apply** to save the settings.
4. 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.

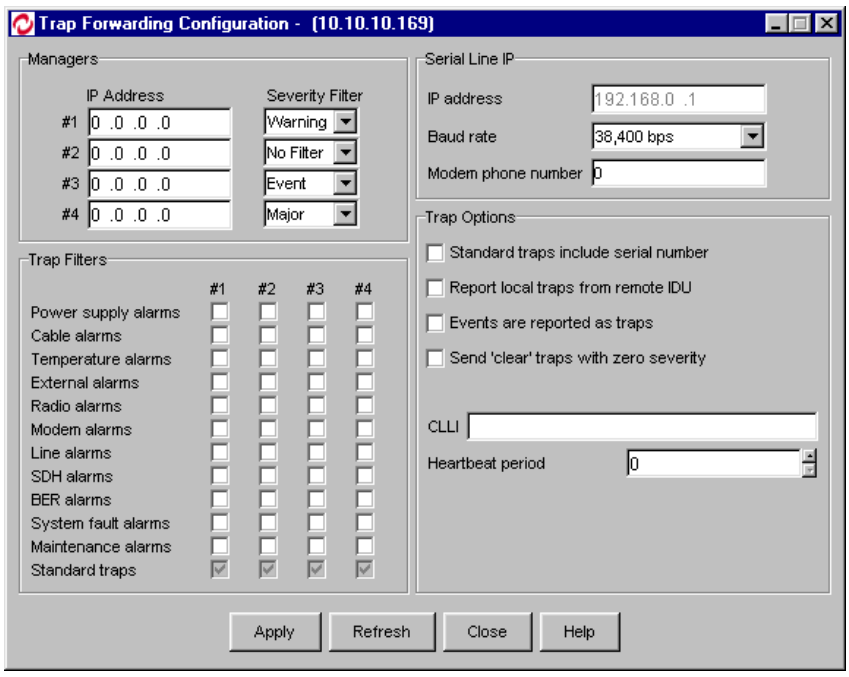


Figure 5-11 Trap Forwarding Configuration Window

2. In the **Managers** area, specify the IP addresses of the managers to which you want traps to be sent. For each manager, you can select a severity filter, which will block traps with the severity level you chose.
3. In the **Trap Filters** section of the window, 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. Select **Send "clear" traps with zero severity** if you want traps that were not assigned a severity level to be sent to managers.
11. For **CLLI** (Common Language Location Identifier), enter up to 18 characters that will represent your system ID when traps are sent.
12. 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 meachnism is working.
13. Click **Apply** to save the settings.
14. 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.

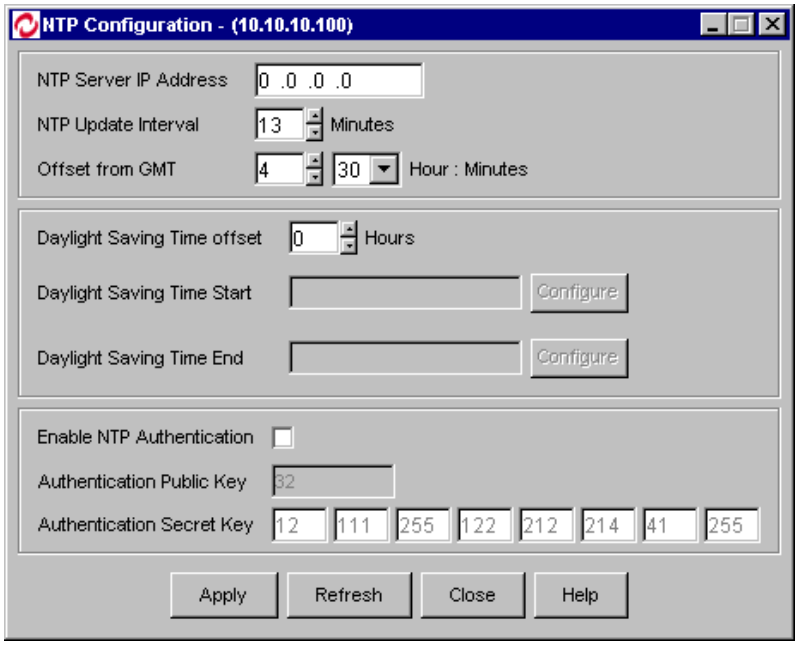


Figure 5-12 NTP Configuration Window

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.

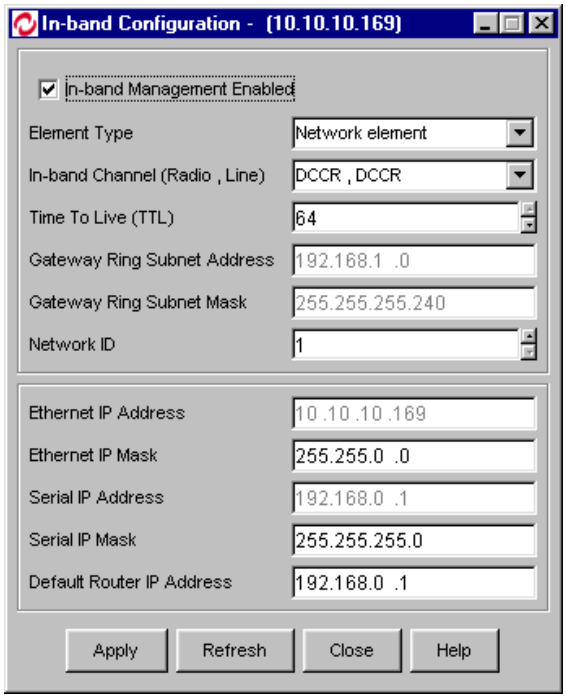


Figure 5-13 In-band Configuration Window

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 **Channel**, click the drop-down list and select the channel you want to use (DCCR or DCCM).
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 **Network ID**, use the arrow buttons to select the desired value.
9. In the second area of the window, enter the relevant IP addresses and masks.
10. Click **Apply** to save the settings.
11. Click **Close** to close the window.

Alarms Menu

Current Alarms

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

   The Current Alarms window appears.

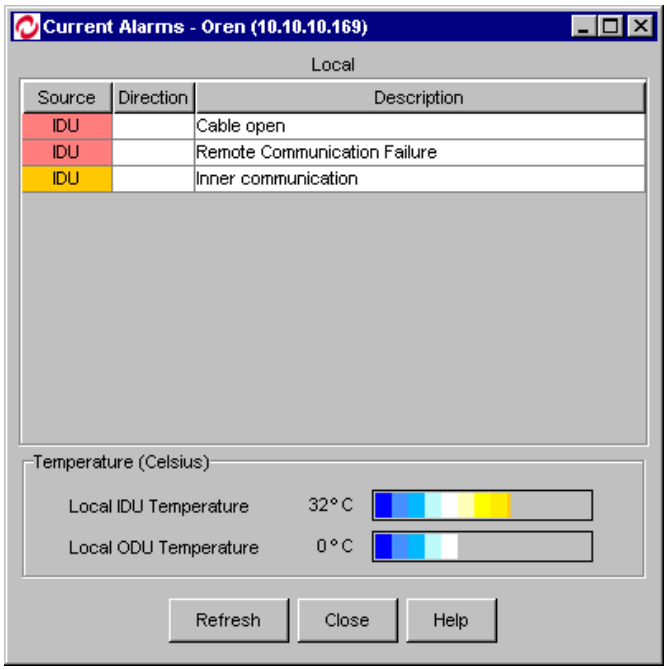


Figure 5-14 Current Alarms Window

Each line in the window describes a different alarm.

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

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

Red	Major alarm
Orange	Minor alarm
Yellow	Warning
Blue	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.

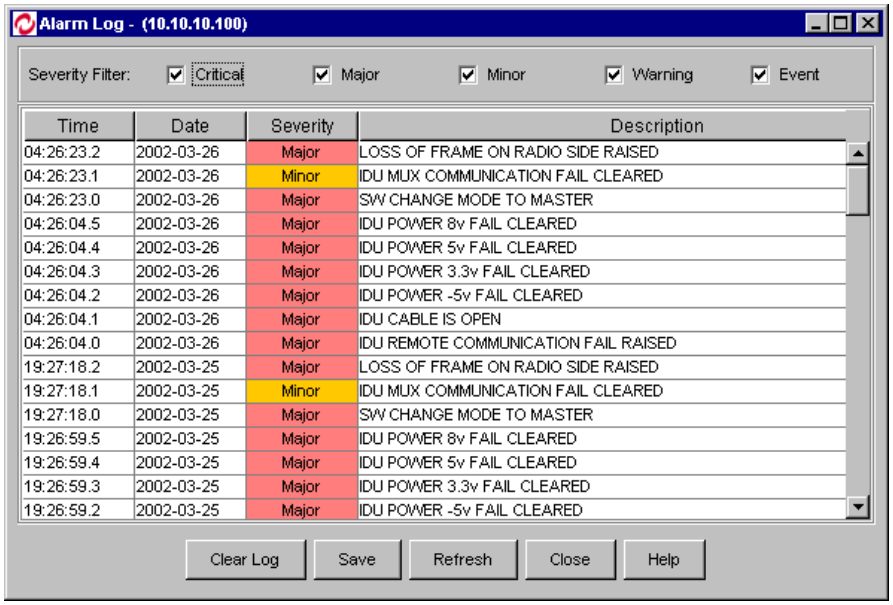


Figure 5-15 Alarm Log Window

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**, **RSL**.

   The Local or Remote RSL Monitoring graphic window appears.

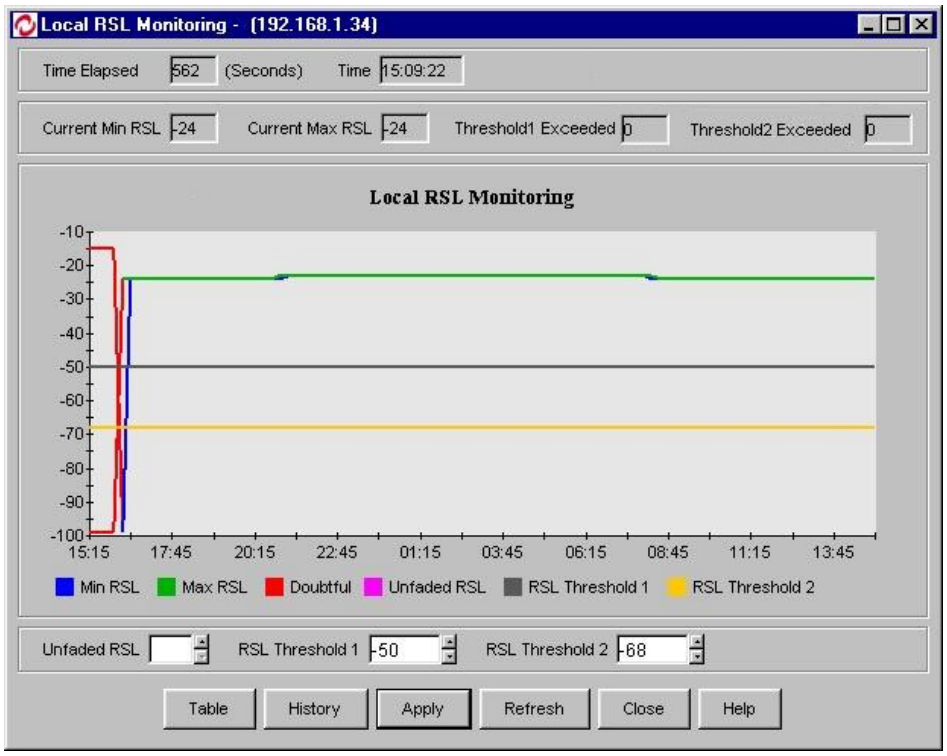


Figure 5-16 RSL Monitoring Graphic Window

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**.

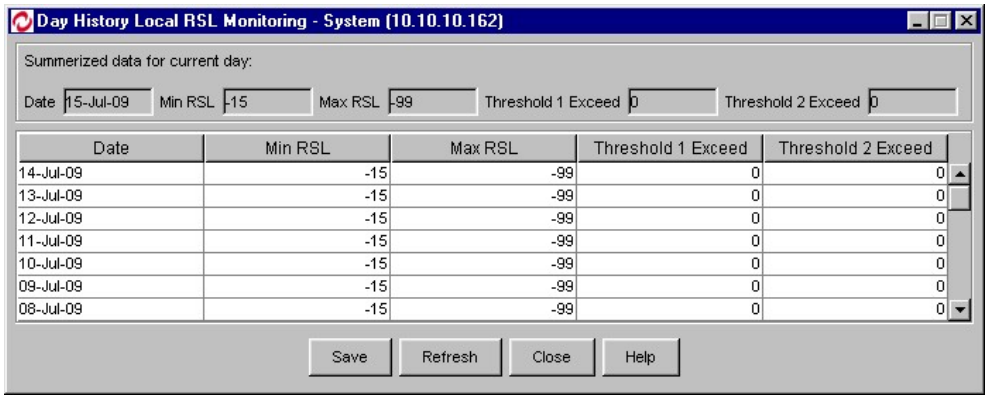


Figure 5-17 RSL Monitoring History Window

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

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

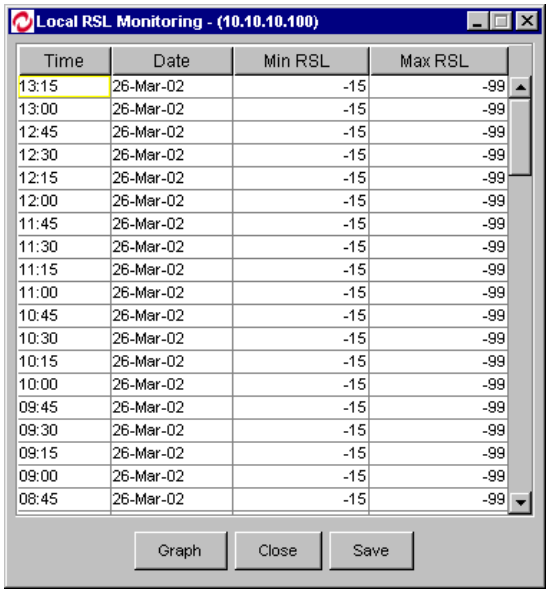


Figure 5-18 RSL Monitoring Table Window

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.

1. Select **Performance**, **Radio**, **TSL**.

   The TSL Monitoring graphic window appears.

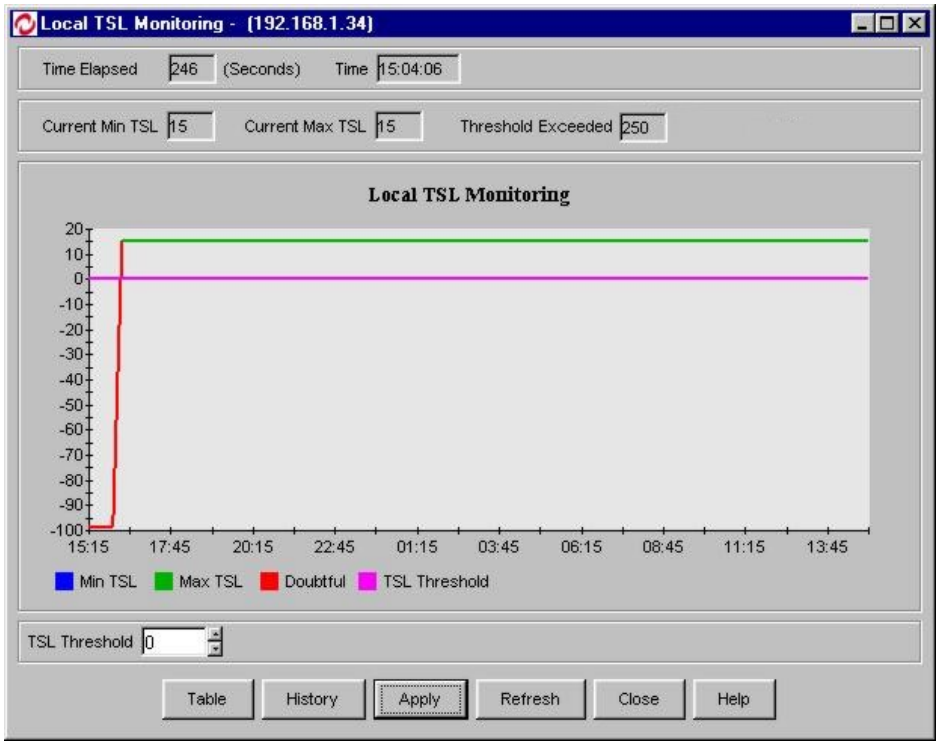


Figure 5-19 TSL Monitoring Graphic Window

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, SDH**.

   The SDH Monitoring graphic window appears.

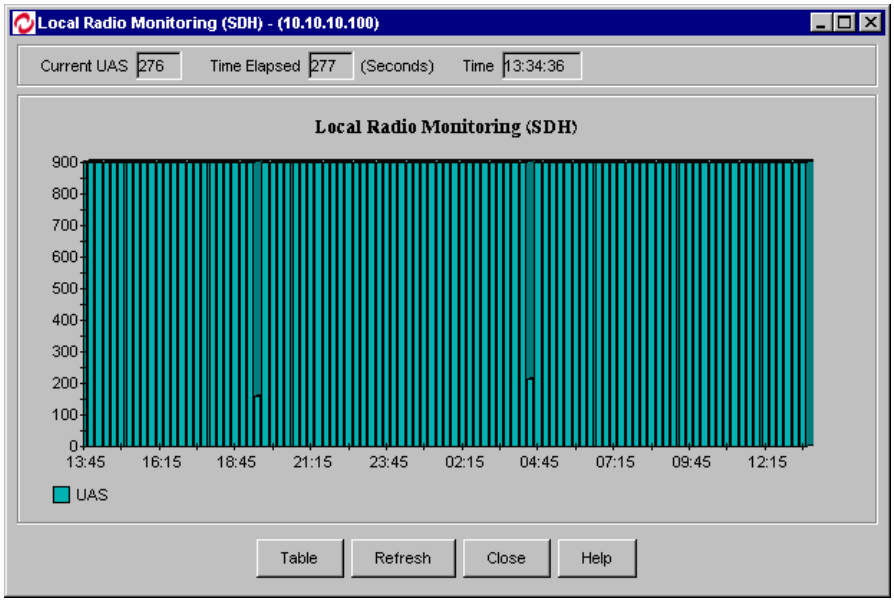


Figure 5-20 SDH Monitoring Graphic Window

The UAS value can be between 0 and 900.

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

2. 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.

1. Select **Performance**, **Tributaries, E1 #**

   The Tributary Monitoring graphic window appears.

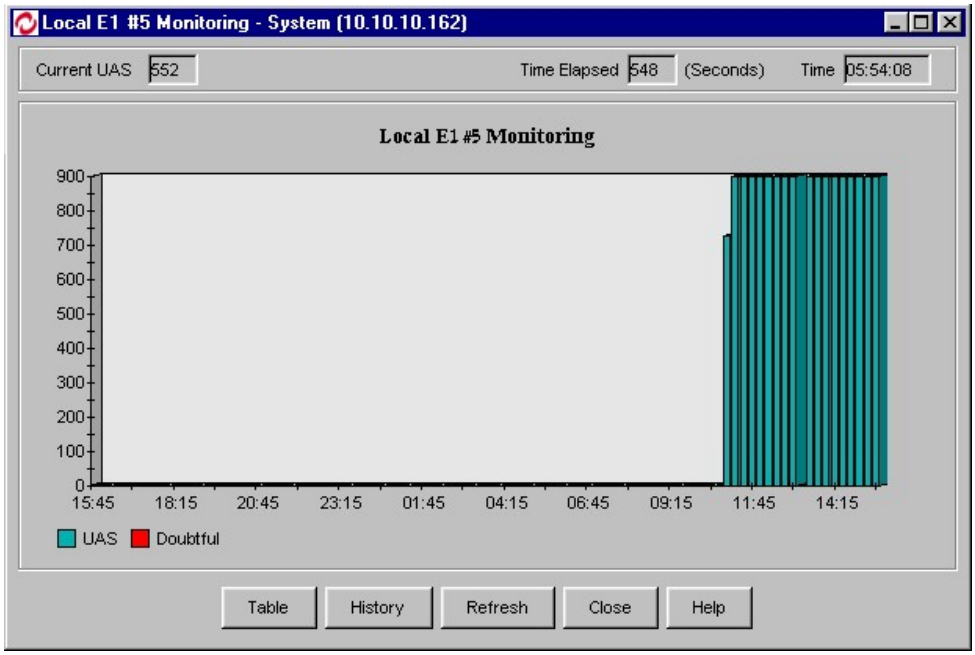


Figure 5-21 Tributary Monitoring Graphic Window

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.

Trail

The Trail Performance Monitoring window displays trail signal levels measured every 15 minutes over the last 24 hours.

1. Select **Performance**, **Trail**, ***Trail Number***, ***East/West***.

   The Trail Monitoring graphic window appears.

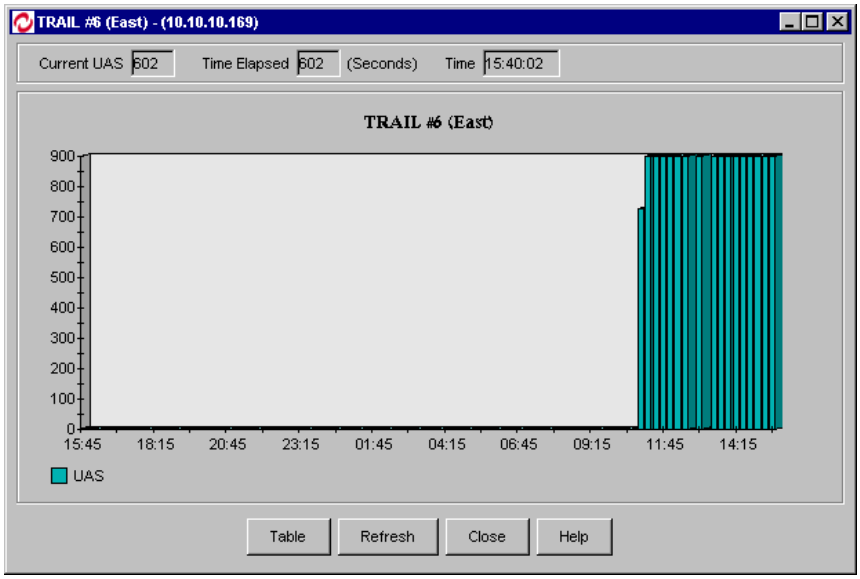


Figure 5-22 Trail Monitoring Graphic Window

2. Click **Table** to open the Trail Monitoring table window.

3. Click **Graph** to return to the Trail Monitoring graphic window.

Protection

Radio Protection

1. Select **Protection**, **Radio Protection** to configure the radio protection switch mechanism.

   The Radio Protection window appears.

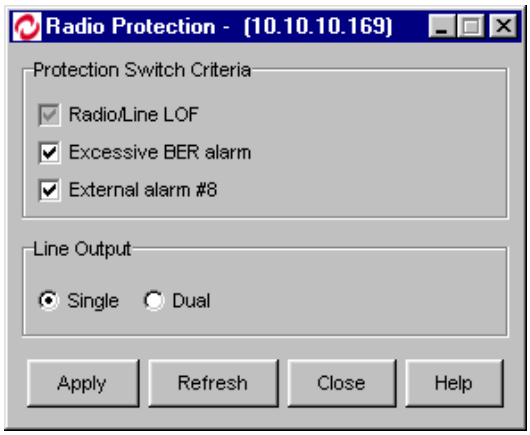


Figure 5-23 Radio Protection Window

2. In the **Protection Switch Criteria** area, select the criteria for which you want protection switching to occur.
3. For **Line Output**, select either **Single** or **Dual**.
4. Click **Apply** to save the changes.
5. Click **Close** to close the window.

Force Radio Protection Switch

Select **Protection**, **Force Radio Protection Switch** if you want to change between the Primary and Secondary links in a 1+1 system.

Trail Protection

1. Select **Protection**, **Trail Protection** to activate the protected path mechanism for the desired ports.

   The Protection window appears.

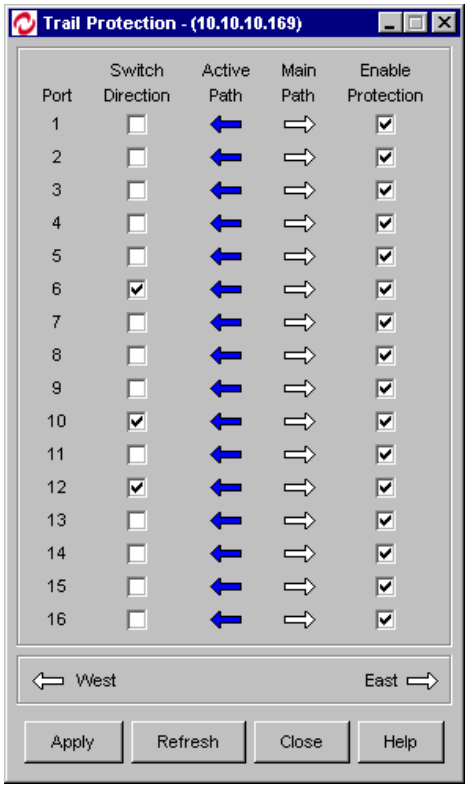


Figure 5-24 Trail Protection Window

2. Mark the **Switch Direction** box for the desired ports if you want data to be delivered in the opposite direction during a transmission failure.
3. Click the **Enable Protection** box for the desired ports to activate the protection mechanism.
4. Click **Apply** to run the test.
5. Click **Close** to close the window.

Maintenance

Loopback

1. Select **Maintenance**, **Loopback,** or click the Loopback icon.

   The Loopback window appears.

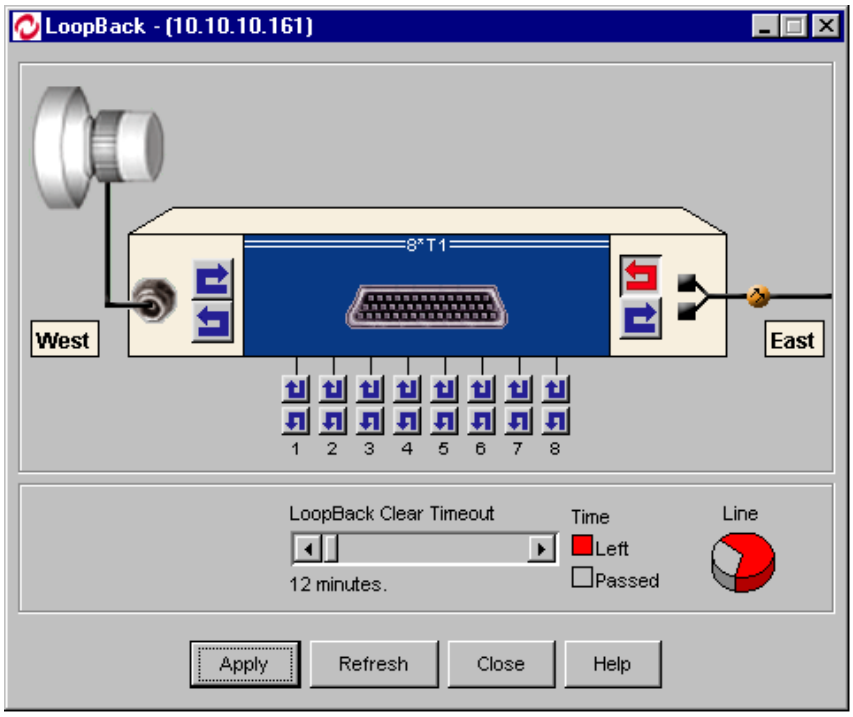


Figure 5-25 Loopback Window

2. Click the upper button on the west side  to perform an external radio loopback test.

   Click the lower button on the west side  to perform an internal radio loopback test.

   Click the upper button on the east side  to perform an external line loopback test.

   Click the lower button on the east side  to perform an internal line loopback test.

   Click the upper button in the trail list  to perform an external trail loopback test.

   Click the lower button in the trail list  to perform an internal trail loopback test.

3. 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 display to the right of the timeout scale shows how much time is left for the test (see the figure above).

   The Timeout scale is used only for radio and line loopbacks.

4. Click **Apply** to run the test.
5. 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

Select this item to clear the Performance Monitoring log files.

Force Remote Tx Level

Select this item to force the remote Tx level to the value set for the local IDU.

Force Remote Mute Off

Select this item to mute remote ODU transmission. This setting will override the setting in the Local ODU Configuration window.

Chapter 6
Troubleshooting

General

Ceragon designed FibeAir to be highly reliable and relatively maintenance free. In the event of a system failure, the system will provide detailed indications to assist troubleshooting and fault isolation.

This chapter explains the alarm indications of the FibeAir system, and contains procedures for troubleshooting and fault isolation.

Maintenance Policy

To ensure simple and efficient system maintenance, the on-site technician will only replace IDU or ODU modules, and not repair them. Under no circumstance will the technician be permitted to open the equipment in order to repair a module or circuit board. Opening equipment will terminate the Ceragon warranty.

Maintenance procedures the technician can perform include visual inspection, cleaning, cable/connector repair, link alignment/adjustment, and retorquing antenna mount bolts.

Visual Inspection

The following table lists the suggested preventive maintenance procedures, which include visual inspection of the equipment and verification of operational parameters.

It is recommended to perform the procedures as often as local environmental conditions require. It is recommended to notify the end customer prior to performing any preventive maintenance procedures that could affect service on the circuit.

What to check	Check for ...	Comments
IDU alarm LEDs	All Green	If not, perform troubleshooting
Coax cable connection	Tight, no corrosion or moisture	Clean/repair as required
Coax cable	No cracks or kinks	Replace as required
All equipment	Dust or dirt	Clean as required
Receive level (voltage in IDU/ODU, or using management)	Per installation records	Align/adjust as required
Torque on antenna mount bolts	Tight mount	Adjust as required

Troubleshooting

Troubleshooting Steps

Corrective maintenance consists of the steps described in the following sections. The steps provide a logical, sequential method for diagnosing and resolving system problems.

Step 1: Define the Symptom

This step is generally peformed by the customer's field technician or supervisor. Examples of symptoms include “IDU alarm is red”, “complete loss of service”, and “excessive errors”.

Symptoms may be constant or intermittent. Constant symptoms require immediate troubleshooting attention. Intermittent symptoms may require circuit monitoring or robust test procedures prior to troubleshooting.

Step 2: Isolate the Problem

After you have a clear definition of the symptom, the malfunction can be isolated using diagnostics, loopback testing, fault isolation tables/flow charts, test equipment, and manual procedures.

This step will identify the specific piece of equipment that is failing.

Although it may be difficult at times to immediately determine which part of a radio link is causing the fault, the initial suspicion should be focused on one of the following near-end or far-end issues:

- Power supplies
- Fading (due to heavy rain, new obstacle in path, antenna misalignment)
- External equipment (SONET/SDH, ATM, FastEthernet, etc.)
- Indoor Unit (IDU)
- Outdoor Unit (ODU)
- RF cable between the ODU and IDU
- Exposure of equipment to severe conditions (high temperature, etc.)
- System configuration

Step 3: Understand the Problem

Once the fault has been isolated, you will need to understand why the fault occurred and what is required to correct it. Use the tables provided in the following sections to understand the problem, and for suggestions of possible solutions.

Step 4: Solve the Problem

You can use the troubleshooting information in this chapter to help solve the problem.

IDU LED Indicators

The following table lists the LEDs on the IDU panel and their functions.

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

LED Color	Alarm Explanation
Yellow	Local unit receives LOF from a receive path currently *not* in use.
Red	Local unit receives LOF from a receive path currently in use.

LOF (Interface Panel) - ALRM

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

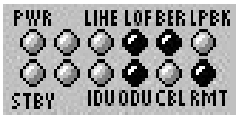
Local Receiver (Interface Panel) - Rx ACTV

LED Color	Alarm Explanation
OFF	Local receiver not in use.
Green	Local receiver in use.

General Troubleshooting Guide

The following table lists general system faults, related alarms, possible causes, and troubleshooting procedures.

Condition	Alarm Indication	Probable Cause	Corrective Action
IDU / Line			
IDU Power Supply Failure	PWR LED Red	One or more voltages in the IDU power supply are not correct	Replace IDU
Local IDU Failure	IDU LED **Red** - modulator failure **Yellow** - high temperature or cooling fan	Modulator failure High temperature Cooling fan	Check alarms. If *Modulator fail*, replace IDU Check air conditioning in facility Check alarms. If *High Temp*, check alarm log file for *FAN failure*. If it exists, replace IDU
Problem with line input (from external equipment)	LINE LED **Red** - loss of signal from line side, loss of frame, BER **Yellow** - signal degraded, J0 mismatch	External equipment Physical connection	Refer to Interface Troubleshooting procedures later in this chapter
ODU / Radio			
ODU Problem	ODU LED: **Red** - ODU power failure **Yellow** - Tx/Rx out of range, temperature The Yellow condition will usually include indications by the RMT, LOF, and		1. Check RSL level at the remote terminal. Compare it to the calculated unfaded Rx level. If there is a change of more than 3 dB in the Rx level, change the Tx power level in the Local ODU

	BER LEDs, as shown in the following figure.  		Configuration window. Check if the ODU is operating in extreme temperature conditions. Such conditions may cause a variation of the Tx output power level.

Condition	Alarm Indication	Probable Cause	Corrective Action
Cable Short or Open	CBL LED Red This stauts of this LED is refreshed every minute	Cable Short Cable Open	Check cable connection
Remote Unit warning/failure	RMT LED Color is same as most severe LED indications in the remote unit. **Red** - may also indicate a disconnected link		Check alarms and see if there is a connectivity problem. If a connectivity alarm exists, check remote unit alarms.
General			
Standby Mode (Protection Configuration)	STBY LED	The STBY LED illuminates to indicate that the link is operating in Protected Configuration mode, but is currently not transmitting	None - normal operation
IDU Loopback	LPBK LED LPBK + RMT LEDs	The LPBK LED illuminates when loopback is run for testing purposes. If loopback is run on the remote unit, both LPBK and RMT will illuminate.	You can cancel loopback in the Loopback window, or by turning the system off and on.

Interface Troubleshooting Guide

This section provides solutions to problems caused by input interface equipment. If, after radio link is installed, the payload is not received, there may be a problem either with the line interface connection to the FibeAir 1548, or with external equipment. In such cases, the table in this section may assist in determining the problem.

Prior to performing line interface troubleshooting, check the following items, which are common causes of line interface failures:

- External equipment Tx is connected to FibeAir Rx.
- External equipment Rx is connected to FibeAir Tx.
- Both external equipment and FibeAir are using the same interface (single mode, multi-mode).
- For multi-mode interfaces, check that you are using multi-mode fibers to connect the unit. For The single mode interfaces, check that you are using single mode fibers.

If no problem is detected with any of the items above, proceed with the following line interface troubleshooting table.

Symptom	Probable Cause	Corrective Measures
LINE LED is red, and SIG LED on Main Channel Interface is off	1. No input signal	Check that both ends of the Main Channel fiber or electrical cable are properly connected, and that the source of the 155 Mb/s stream is on, enabled, and operating.
	2. Incorrect input signal format	Verify that the input signal is a valid 155.52 Mb/s signal, with framing.
	3. Tx/Rx cables swapped	Verify that the line input stream to the FibeAir unit is connected to the Rx connector. If necessary, swap Rx and Tx cables.
	4. Incorrect optical power levels or wavelength	For optical interfaces: 1. Verify that the optical source, optical cables, connectors, and attenuators are compatible with the interface type. Typical problems: single-mode cables are used with multi-mode physical interface, 850 nm or 1550 nm optical sources are connected to a 1300 nm interface. 2. Verify that the optical input power levels are within the allowed range (use an optical power level meter if necessary). For multi-mode interface, the input optical power level must be within -14 dBm and -31 dBm. For single-mode interface, the input optical power level must be within -2 dBm and -32 dBm.

Symptom	Probable Cause	Corrective Measures
LINE LED is red, and SIG LED on Main Channel Interface is on	1. Line LOF (Loss of Frame)	Verify that the input signal is a valid 155.52 Mb/s signal, with framing.
	2. Line EXC (excessive BER)	1. Verify that the source of the 155.52 Mb/s signal does not generate errors on the B1 byte (e.g. for maintenance/testing purposes) 2. Verify that the connectors are connected properly, cable ends are in good condition, and that no excessive stress is applied to the cables, cable ends, and connectors (bent optical cables may cause communication failures). 3. Check the input 155.52 Mb/s line for cables in poor condition, cables that are too long, etc. For optical lines, verify that the optical input power level is within the allowed range (provided in step 1 of the previous troubleshooting procedure).

Symptom	Probable Cause	Corrective Measures
LINE LED illuminates yellow	1. Line SD (Signal Degrade)	Same as for EXC (described in step 2 of the previous troubleshooting procedure).
	2. J0 mismatch alarm	Verify that the input stream is connected to the correct FibeAir unit. (Check that there are no errors in the routing or connections of your 155.52 Mb/s streams.) *-or-* Change the J0 trace message, in the equipment transmitting to the FibeAir unit, to the J0 trace message expected by the unit. *-or-* Change the FibeAir expected J0 trace message to match its received trace message. *-or-* Disable the Section Trace function of the FibeAir unit (set J0 Operation to Passthrough in the SDH/SONET Configuration window).
LINE and SIG LEDs are green, but equipment connected to FibeAir is malfunctioning	1. Interoperability problem	Try bypassing the FibeAir unit or running the loopbacks to locate the source of the problem. *-or-* Try disabling the FibeAir SONET/SDH features (set Operation to Passthrough mode in the SDH/SONET Configuration window). *-or-* Consult the documentation provided with the other equipment.
	2. The fault may be caused by the other equipment	Try bypassing the FibeAir unit or running the loopbacks to locate the source of the problem. *-or-* Consult the documentation provided with the other equipment.

Fault Isolation Using Loopbacks

The loopback function provides a means of testing the link at various points. During the procedure, the external equipment sends a data pattern and monitors its receipt. If the received pattern is identical to the sent pattern, the connection between the equipment and the loop is confirmed.

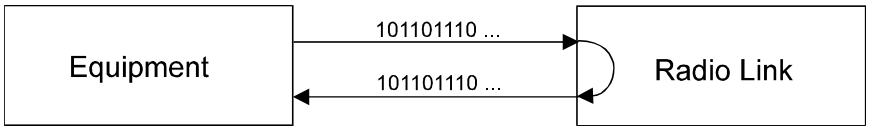


Figure 6-1 Loopback

FibeAir is capable of performing loopback testing at several points in the link. The test is run from the CeraView management software, or via the SNMP protocol.

During the loopback test, an alarm indication will appear to remind you to cancel the test when you are done.

The following loopback tests can be performed from the window:

Local:

- 155 MB/s Line Interface
- Wayside Channel
- 64 KB/s User Channel

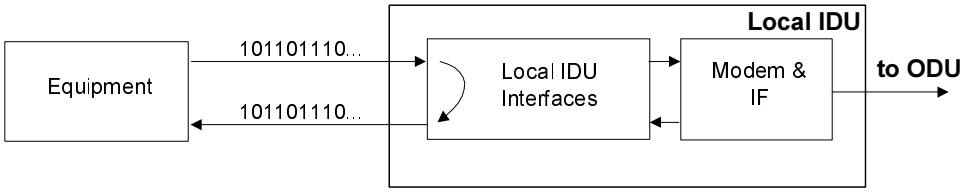


Figure 6-2 Local Loop

- Full IDU (all three inputs through the IDU, modulator, and looped in the IF).

Remote:

- 155 MB/s Line Interface
- Wayside Channel
- 64 KB/s User Channel

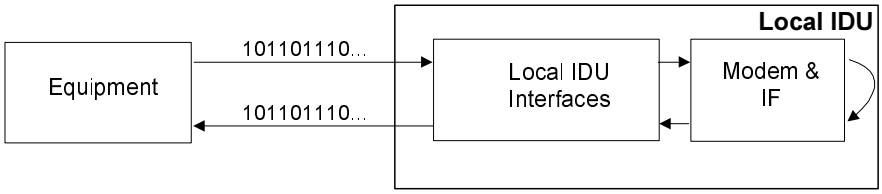


Figure 6-3 Remote Loop

- Full Radio Link Loopback (local external equipment through the radio link, to the remote line interface module, back through the radio link, to the local external equipment).

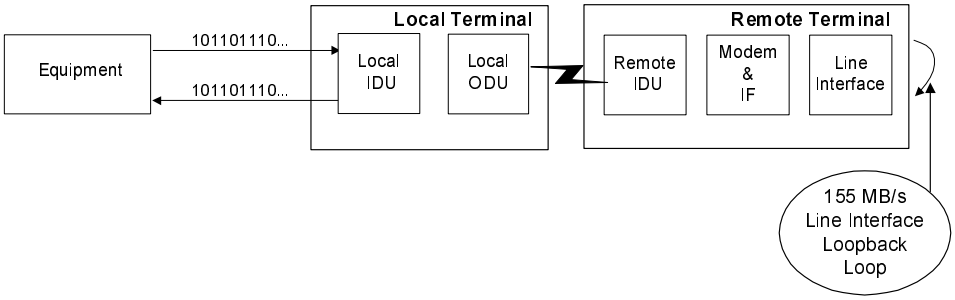


Figure 6-4 Remote Terminal Loop

Connection Configuration Troubleshooting Guide

Problems that occur when trying to connect to the FibeAir system using CeraView, may be due to incorrect cable configuration. If there is a connection problem in the system, CeraView will start, but an hour glass will appear when the software is loading to indicate that a problem exists.

The following steps will help you identify and correct such problems.

Check the Cables

Refer to the figure below for the following procedures.

1. For Ethernet connection between FibeAir and a PC network card, use a cross cable.

   For Ethernet connection between FibeAir and an Ethernet hub (for example, connecting to a LAN jack in a wall) use a straight cable.

2. For serial connection between FibeAir and a PC serial port, use a straight cable.

   For serial connection using a dial-up modem, use a cross cable.

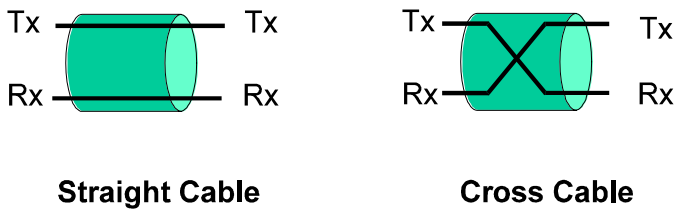


Figure 6-5 Cable Connections

Check Read and Write Communities

1. Ping FibeAir.

   If ping succeeds, the problem may be with the CeraView software installation, or the computer TCP\IP stack. Check the read and write communities in FibeAir and in the management station configuration.

   If ping fails, there may be a network connectivity problem.

   A typical conflict may occur between the IDU configuration shown in the terminal window below, and the related CeraView parameter.

   According to the example below, the user needs to enter “netman” in the **Write Community** field.

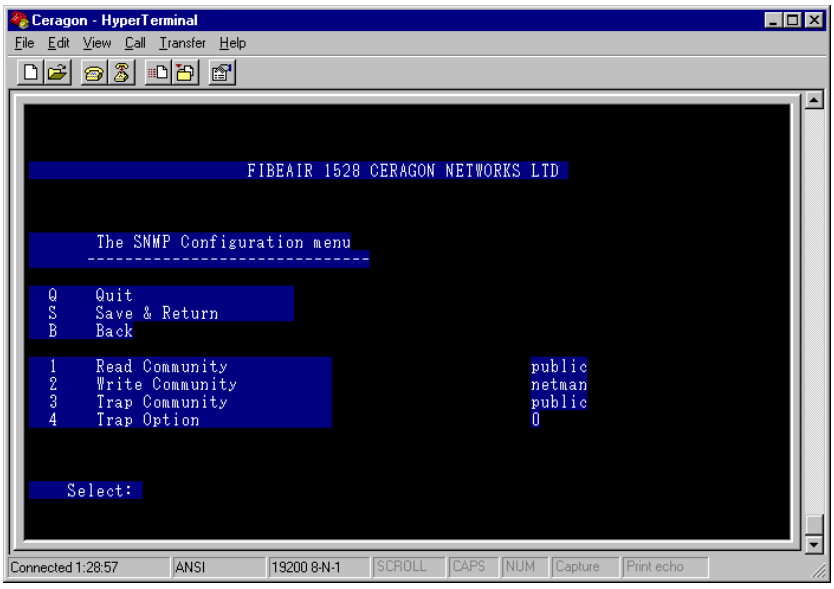


Figure 6-6 Typical Configuration Conflict

In addition, the Agent Address must be identical to the IDU IP address, and the source address must be identical to the computer's address.

The following figure shows a typical example of IP addresses and network configuration.

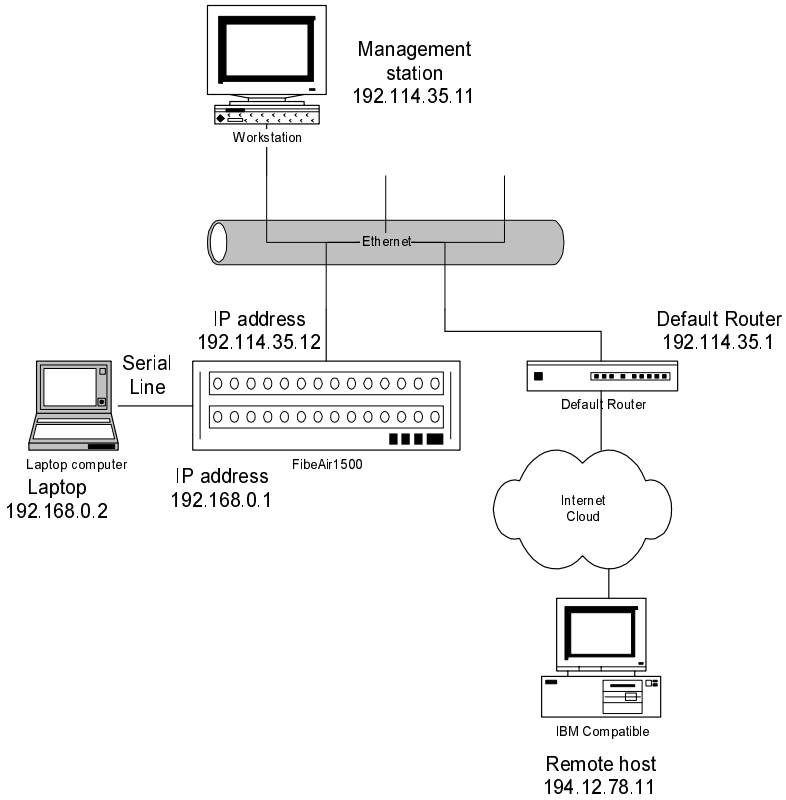


Figure 6-7 Typical Network Configuration

Check the Serial Connection

If the connection is via serial line, check the serial line speed in FibeAir, and in the Management station configuration. In the terminal, the serial line speed is specified using the IP Configuration menu.

Check the Ethernet Connection

Verify that the Management station and FibeAir IP interfaces have the same net ID. If they should not be included in the same network, check the default router address.

After performing the verifications above, if there is still a problem with network connectivity, together with the system administrator check for firewalls and routing configuration errors.

Alarm Messages

The following table lists FibeAir system alarm messages. (For messages specific to FibeAir 1500A/1528A, see *FibeAir 1500A/1528A Alarm Messages* at the end of this chapter.)

Message	Severity
ODU	
Power Supply status	Major
Synthesizer lock status	Major
TX level status	Minor
RX level status	Minor
Temperature status	Warning
IDU	
Power status	Major
Cable open status	Major
Modem Lock status	Major
Temperature	Warning
Loopback status	Major
External alarm 1 status	
External alarm 2 status	
External alarm 3 status	
External alarm 4 status	
External alarm 5 status	
External alarm 6 status	
External alarm 7 status	
External alarm 8 status	
Remote connectivy status	Major
Inner communication status	Minor
RST	
Line loss of frame status	Major
Radio loss of frame status	Major
Line EXC status	Major
Radio EXC status	Major
Line SD status	Minor
Radio SD status	Minor
Loss of signal status	Major
J0 mismatch	Minor

Alarm Log File Messages

The following table lists alarm messages that may appear in the FibeAir alarm log file, the trap issued to network management, and possible corrective actions.

Remember to check active alarms to verify which faults are still active and require attention.

Message	Trap Issued	Cause / Corrective Action
ODU POWER *xx* FAILURE	Power supply	Problem in one of the power supplies in the ODU (except the +5v). To correct: Check current alarm status
ODU POWER *xx* OK	Power supply	1. Power supplies are checked periodically. If there was a failure, or during unit power-up the power supply is OK, this message is issued.
ODU XBAND SYNTHESIZER IS UNLOCKED	Radio	Synthesizer is unlocked. This can either be a momentary synchronization loss, or a hardware failure. If this alarm does not clear in a short while, the ODU needs to be replaced.
ODU XBAND SYNTHESIZER IS LOCKED	Radio	Previous error is cleared. To correct: Check current alarm status.
ODU IF CONVERTER *xx* LOCKED	Radio	Synthesizer is unlocked. This can either be a momentary synchronization loss, or a hardware failure. If alarm does not clear in a short while, the ODU needs to be replaced. Suggested: Check current alarm status.
ODU IF CONVERTER *xx* UNLOCKED	Radio	Previous error is cleared.
ODU TX LEVEL IS OUT OF RANGE	Radio	Actual transmitted power differs by more than 3 dB from the required power. This can be due to one of the folowing: 1. Extreme temperature conditions 2. Hardware failure Note: This warning does not always require immediate action, the data may still be OK on the radio link. To correct: 1. Check RSL level at the remote terminal, and compare it to the calculated unfaded Rx level. If there is a change of more than 3 dB in the Rx level, change the Tx power level in the local ODU Configuration window. 2. Check if the ODU is operating in extreme temperature conditions. Such conditions may cause variations in the Tx output power level.

Message	Trap Issued	Cause / Corrective Action
ODU TX LEVEL IS IN RANGE	Radio	Previous error is cleared.
ODU RX LEVEL IS OUT OF RANGE	Radio	The actual received level (after AGC circuits) differs from the expected level. This may be caused by one of the following: 1. The received signal is too weak or too strong. 2. Hardware failure. To correct: 1. Check current alarm status. 2. If the radio alarm is still active, contact your Ceragon distributor.
ODU RX LEVEL IS IN RANGE	Radio	Previous error is cleared.
ODU ATPC IS NOT ACTIVE	Radio	Future use only.
ODU ATPC IS ACTIVE	Radio	Future use only.
ODU EXTREME TEMPERATURE CONDITIONS	Temperature	ODU temperature is either above +67 C (152 F) or below -37 C (-34 F). To correct: 1. Check current alarm status. 2. If the Temperature alarm is still active, contact your Ceragon distributor.
ODU NORMAL TEMPRATURE CONDITIONS	Temperature	ODU temperature was restored to normal operating conditions: -33 C (-27 F) < T < 63 C (145 F)
ODU LOOPBACK IS NOT ACTIVE	Maintenance	Future use only.
ODU LOOPBACK IS ACTIVE	Maintenance	Future use only.
MUX LINE LOSS OF FRAME (LLOF)	SONET/SDH	After three consecutive SONET/SDH (main channel only) frame losses, this alarm is issued. To correct: 1. Check current alarm status. 2. If the Sonet alarm is still active, contact your Ceragon distributor.
MUX NO LINE LOSS OF FRAME	SONET/SDH	Issued when a valid frame is recognized following an LLOF state.
MUX LINE LOSS OF SIGNAL (LOS)	Line	Main channel does not receive a valid input signal. To correct: 1. Check current alarm status. 2. If the Line alarm is still active, contact your Ceragon distributor.

Message	Trap Issued	Cause / Corrective Action
MUX NO LINE LOSS OF SIGNAL	Line	Issued when a signal is resent to the main channel.
MUX JO MISMATCH	SDH	The received J0 string is different than the expected string. To correct: 1. Check current alarm status. 2. If the Sonet alarm is still active, contact your Ceragon distributor.
MUX NO JO MISMATCH	SDH	The received J0 string is now identical to the expected one.
MUX RADIO LOSS OF FRAME (RLOF)	SONET/SDH	After three consecutive radio channel frame losses this alarm is issued (link disconnected). To correct: 1. Check current alarm status. 2. If the Sonet alarm is still active, contact your Ceragon dealer.
MUX NO RADIO LOSS OF FRAME	SONET/SDH	Issued when a valid frame is recognized following an RLOF state
MUX LINE SIGNAL DEGRADE	BER	Issued when the SDH/SONET line BER drops below the defined level for “signal degrade” (SDH/Sonet Configuration menu). To correct: 1. Check current alarm status. 2. If the BER alarm is still active, contact your Ceragon distributor.
MUX NO LINE SIGNAL DEGRADE	BER	Issued when the SDH/SONET line BER returns to a level above the defined level for “signal degrade” (SDH/Sonet Configuration menu).
MUX LINE EXCESSIVE ERRORS	BER	Issued when the SDH/SONET line BER drops below the defined level for “excessive errors” (SDH/Sonet Configuration menu). To Correct: 1. Check current alarm status. 2. If the BER alarm is still active, contact your Ceragon distributor.
MUX NO LINE EXCESSIVE ERRORS	BER	Issued when the SDH/SONET line BER returns to a level above the defined level for “excessive errors” (SDH/Sonet Configuration menu).
MUX RADIO SIGNAL DEGRADE	BER	Issued when the radio BER drops below the defined level for “signal degrade” (SDH/Sonet Configuration menu). To correct: 1. Check current alarm status.

Message	Trap Issued	Cause / Corrective Action
		2. If the BER alarm is still active, contact your Ceragon distributor.
MUX NO RADIO SIGNAL DEGRADE	BER	Issued when the radio BER returns to a level above the defined level for “signal degrade” (SDH/Sonet Configuration menu).
MUX RADIO EXCESSIVE ERRORS	BER	Issued when the radio BER drops below the defined level for “excessive errors” (SDH/Sonet Configuration menu). To correct: 1. Check current alarm status. 2. If the BER alarm is still active, contact your Ceragon distributor.
MUX NO RADIO EXCESSIVE ERRORS	BER	Issued when the radio BER returns to a level above the defined level for “excessive errors” (SDH/Sonet Configuration menu).
IDU POWER 5V FAILURE	Power Supply	Problem in the IDU +5V power supply. To correct: 1. Check current alarm status. 2. If the Power supply alarm is still active, contact your Ceragon distributor.
IDU POWER 5V OK	Power Supply	Power supplies are checked periodically. If a failure occurs, or during unit power-up when the power supply is OK, this message is issued.
IDU POWER 8V FAILURE	Power Supply	Problem in the IDU +8V power supply. To correct: 1. Check current alarm status. 2. If the Power supply alarm is still active, contact your Ceragon distributor.
IDU POWER 8V OK	Power Supply	Power supplies are checked periodically. If a failure occurs, or during unit power-up when the power supply is OK, this message is issued.
IDU POWER 3.3V FAILURE	Power Supply	Problem in the IDU +3.3V power supply. To correct: 1. Check current alarm status. 2. If the Power supply alarm is still active, contact your Ceragon distributor.
IDU POWER 3.3V OK	Power Supply	Power supplies are checked periodically. If a failure occurs, or during unit power-up when the power supply is OK, this message is issued.

Message	Trap Issued	Cause / Corrective Action
IDU POWER –5V FAILURE	Power Supply	Problem in the IDU -5V power supply. To correct: 1. Check current alarm status. 2. If the Power supply alarm is still active, contact your Ceragon distributor.
IDU POWER –5V OK	Power Supply	Power supplies are checked periodically. If a failure occurs, or during unit power-up when the power supply is OK, this message is issued.
IDU CABLE IS OPEN	Cable	A sensor in the IDU detects that the IDU-ODU cable is disconnected. To correct: Verify that the cable is connected properly.
IDU CABLE IS SHORT	Cable	A sensor in the IDU detects that the IDU-ODU cable is shorted. To correct: 1. Disassamble the RF connector on both sides. 2. Check for shorts in the cable (DVM). 3. Reassemble the RF connectors.
IDU CABLE IS OK	Cable	Previous error is cleared.
IDU MODULATOR FAILURE	Modem	Unsynchronized SDH/Sonet clock with a large frequency offset (this can happen also in loopbacks with external equipment in loop-timing “slave” mode). Internal hardware failure. To correct: 1. Check current alarm status. 2. If the Modem alarm is still active, contact your Ceragon distributor.
IDU MODULATOR OK	Modem	Previous error is cleared.
IDU DEMODULATOR FAILURE	Modem	Issued after several consecutive radio channel frame losses (link disconnected). To correct: 1. Check current alarm status. 2. If the Modem alarm is still active, contact your Ceragon distributor.
IDU DEMODULATOR OK	Modem	Previous error is cleared.

Message	Trap Issued	Cause / Corrective Action
IDU DEMODULATOR FIFO OVERFLOW	Modem	To correct: 1. Check current alarm status. 2. If the Modem alarm is still active, contact your Ceragon distributor.
IDU DEMODULATOR FIFO OK	Modem	None - normal operation.
IDU DEMODULATOR PLL FAILURE	Modem	To correct: 1. Check current alarm status. 2. If the Modem alarm is still active, contact your Ceragon distributor.
IDU DEMODULATOR PLL OK	Modem	None - normal operation.
IDU DEMODULATOR TIMING LOOP FAILURE	Modem	To correct: 1. Check current alarm status. 2. If the Modem alarm is still active, contact your Ceragon distributor.
IDU DEMODULATOR TIMING LOOP OK	Modem	None
IDU DEMODULATOR PHASE LOOP FAILURE	Modem	To correct: 1. Check current alarm status. 2. If the Modem alarm is still active, contact your Ceragon distributor.
IDU DEMODULATOR PHASE LOOP OK	Modem	None
IDU DEMODULATOR SYMBOL ESTIMATE ERROR	Modem	To correct: 1. Check current alarm status. 2. If the Modem alarm is still active, contact your Ceragon distributor.
IDU DEMODULATOR SYMBOL ESTIMATE OK	Modem	None
IDU EXTREME TEMPERATURE CONDITIONS	Temperature	IDU temperature is either above +50C (122 F). To correct: 1. Check current alarm status. 2. If the Temperature alarm is still active, contact your Ceragon distributor.
IDU NORMAL TEMPERATURE CONDITIONS	Temperature	IDU temperature was restored to normal condition: T > 47 C (116 F).
IDU FAN FAILURE	Temperature	There is a fault in one of the IDU venting fans. To correct: 1. Check current alarm status.

Message	Trap Issued	Cause / Corrective Action
		2. If the Temperature alarm is still active, contact your Ceragon distributor.
IDU FAN OK	Temperature	There was a fault in one of the IDU venting fans, but the problem no longer exists.
IDU LOOPBACK IS ACTIVE	Maintenance	To correct: If not in maintenance test, terminate the loopback from the CeraView Loopback window.
IDU NO LOCAL LOOPBACK	Maintenance	None - normal operation
IDU REMOTE LOOPBACK	Maintenance	The remote IDU is now in loopback mode. To correct: If not in maintenance test, terminate the loopback from the CeraView Loopback window.
IDU NO REMOTE LOOPBACK	Maintenance	The remote IDU is running normally (after being in Loopback mode).
IDU LINE LOOPBACK	Maintenance	To correct: If not in maintenance test, terminate loopback from the CeraView Loopback window.
IDU NO LINE LOOPBACK	Maintenance	None - normal operation
IDU REMOTE COMMUNICATION FAULT	System Fault	Communication between the local and remote terminals was disconnected (data may still be exchanged with BER). To correct: 1. Check cable. 2. If the System Fault alarm is still active, contact your Ceragon distributor.
IDU REMOTE COMMUNICATION OK	System Fault	Communication between the local and remote terminals returned to normal.
IDU ODU COMMUNICATION FAULT	System Fault	Communication between the IDU and ODU was disconnected (channel data may still be exchanged without BER). To correct: If the System Fault alarm is still active, contact your Ceragon distributor.
IDU ODU COMMUNICATION OK	System Fault	Communications between the IDU and ODU returned to normal.

Message	Trap Issued	Cause / Corrective Action
IDU MUX COMMUNICATION FAULT	System Fault	Internal IDU failure. IDU may require corrective maintenance. Main channel data may still be exchanged, but loopbacks may not be possible. To correct: 1. Check current alarm status. 2. If the System Fault alarm is still active, contact your Ceragon distributor.
IDU MUX COMMUNICATION OK	System Fault	Previous alarm is cleared.

FibeAir 1500A/1528A Alarm Messages

The following table lists alarm messages that may appear in the FibeAir alarm log file, the trap issued to network management, and possible corrective actions.

Message	Severity
Fiber-LOS	Critical
RADIO-LOF	Critical
Fiber-LOF	Critical
RADIO-EXBER	Major
Fiber-EXBER	Major
RADIO-SD	Minor
Fiber-SD	Minor
Fiber-TIM	Minor
Radio-TIM	Minor
Radio-MS-AIS	Critical
Fiber-MS-AIS	Critical
Radio-MS-RDI	Major
Fiber-MS-RDI	Major
Radio-MS-EXBER	Major
Fiber-MS-EXBER	Major
Radio-MS-SD	Minor
Fiber-MS-SD	Minor
Radio-AU-LOP	Major
Fiber-AU-LOP	Major
Radio-AU-AIS	Major (see note 1 below)
Fiber-AU-AIS	Major (see note 1 below)
Radio-HP-UNEQ	Warning (see note 1 below) Relevant only for SONET 3xVC3, where the tributaries are DS3s, not only T1s
Fiber-HP-UNEQ	Warning (see note 1 below) Relevant only for SONET 3xVC3, where the tributaries are DS3s, not only T1s
Radio-HP-RDI	Major (see note 1 below)
Fiber-HP-RDI	Major (see note 1 below)
Radio-HP-TIM (1)	Minor
Fiber-HP-TIM (1)	Minor
Radio-HP-PLM (1)	Minor (see note 1 below)
Fiber-HP-PLM (1)	Minor

Message	Severity
Radio-HP-EXBER	Major
Fiber-HP-EXBER	Major
Radio-HP-SD	Minor
Fiber-HP-SD	Minor
Radio-TU-LOP	Minor
Fiber-TU-LOP	Minor
Radio-TU-AIS	Minor
Fiber-TU-AIS	Minor
Radio-TU-LOM (2,3)	Minor
Fiber-TU-LOM (2,3)	Minor
Radio-LP-UNEQ	Warning
Fiber-LP-UNEQ	Warning
Radio-LP-RDI	Minor
Fiber-LP-RDI	Minor
Radio-LP-TIM	Minor
Fiber-LP-TIM	Minor
Radio-LP-PLM	Minor
Fiber-LP-PLM	Minor
Radio-LP-EXBER (4)	Minor
Fiber-LP-EXBER (4)	Minor
Radio-LP- SD	Warning (see note 1 below)
Fiber-LP- SD	Warning (see note 1 below)
Tribs LOS	Major
Tribs UNEXP-Signal	Warning (see note 1 below)
Tribs AIS	Major
Tribs EXBER	Minor
Tribs SD	Warning
Unlock	Major (see note 1 below)
OOR	Major (see note 1 below)

Notes:

1. HP-TIM, HP-PLM, LP-TIM, and LP-PLM can be configured to prevent consequent actions.
2. TU_LOM (H4) causes LP-RDI, tributary AIS, and path protection switching for VC-12s/VC-11s and 2 Mbps/1.544 Mbps tributaries only, **not** for VC-3s and 34/45 Mbps tributaries.
3. TU_LOM (H4) causes pass-through TU AIS for TU-12s/VC-11s only, **not** for TU-3s.