Troubleshooting Guide

OSIRIS®| OSIRIS-VUE™

203-008-05

POSITRON
Networks

Fifth Edition: October 2005

A publication of:
Positron Networks Inc.
5101 Buchan
Montreal, Quebec
Canada H4P 2R9
service@positronnetworks.com

Printed in Canada

The information contained in this publication is accurate to the best of our knowledge. However, Positron Networks Inc. (herein referred to as Positron) disclaims any liability resulting from the use of this information and reserves the right to make changes without notice. Furthermore, this document is subject to change without notice due to ongoing product development.

The information contained in this document is the property of Positron. Except as specifically authorized in writing by Positron, the holder of this document: 1) shall keep all information contained herein confidential and shall protect same in whole or in part from disclosure and dissemination to all third parties, and 2) shall use same for operating and maintenance purposes only.

The information contained in this publication should be used in conjunction with the latest Positron MCN Release Notes document that lists applicable operational considerations.

cETLus Listed /Certified

This equipment has been tested and complies with the requirements of the bi-national standards UL 1950 and CSA C22.2 No 950 entitled "Safety of Information Technology Equipment".

FCC Compliance

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can generate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his or her own expense.

Trademarks

OSIRIS is a registered trademark of Positron Networks Inc. ServiceOn and OSIRIS-VUE are trademarks of Positron Networks Inc.
CLEI is trademark of Telcordia.
All other trademarks are the property of their respective owners.

Table of Contents

Preface

This chapter explains the purpose of this guide and who should read it, provides some document conventions and safety precautions, and describes how the document is organized and how to get technical assistance.

About This Guide

This guide is intended to help network operators and field personnel to solve problems occurring in an operational network and to restore service promptly.

This guide addresses all problems reported by the Element Management System and the network element, presents the probable cause of the problems, and proposes step by step procedures to resolve them.

A reported indication assumes that a session can be established with the affected network element either with a direct connection through a local craft terminal or via the Element Management System. In cases where a session cannot be established, this document proposes problem resolution procedures to identify, isolate and resolve communication problems in order to access the Network Element.

Finally, this guide presents an overview of the Element Management System and the Network Elements for conveniences.

Using this Document

Each network element part of a SONET network reports events locally detected via the Element Management System or the craft tool. In addition, the Element Management System monitors the communication to each network element as well as communication to internal functions that interface with the SONET network.

Since impairment and failure in the network are reported through a communication channel, a section is dedicated to assist the operator in accessing the network. “Chapter 2, Communication Problems” provides useful information in troubleshooting serial and TELNET connections as well as guidance in isolating problem associated to an IP or OSI network.

The first sign of a failure event or network impairment is through a reporting mechanism. The OSIRIS® network elements reporting mechanism is discussed in “Chapter 1, Product Overview & Troubleshooting Concepts”. This section also presents Network Element functionality that is critical in operating or maintaining a network. Each event reported by the network element is defined in “Chapter 3, Alarms, Conditions & Error Messages”. With each definition a list of probable causes is presented and a problem resolution procedure is proposed.

Once a problem has been identified, some operations may be required to isolate the problem. The use of performance monitoring statistics and protection switch operations may help in isolating trouble conditions. A definition of each performance monitoring statistic is provided in “Chapter 6, Performance Monitoring”. For an overview of protection switch operation, refer to the appropriate protection scheme in “Chapter 5, Protection Switching”. This section also provides information on the protection switch request priorities as well as definitions for each switch request.

If a card has been identified as defective, follow the appropriate procedure provided in “Chapter 7, Replacing Hardware”. Refer to “Contacting Customer Service” on page 7 for information on how to return the defective equipment.

Important Messages

This document includes two types of messages designed to call attention to critical safety and equipment integrity information. These messages are used as follows:

WARNING

Warning messages provide critical instructions on how to ensure the personal safety of those working with the OSIRIS equipment. If the warning is not heeded, personal injury may occur.

CAUTION

Caution messages provide instructions on how to ensure the safe and viable operation of the OSIRIS-VUE™ software, and the OSIRIS equipment. If the caution is not heeded, the operation of the software may be disrupted, equipment may be damaged, communications may be disrupted.

Contacting Customer Service

Should a problem arise, please contact us:

Toll Free: 1-866-331-3003 (North America only)
International Line: +1-514-345-2202
Fax: +1-514-345-2304
E-mail: service@positronnetworks.com

Required Information

For level one support, which covers issues related to system operation, you will be asked to provide the following information:

- Name of your company
- Address of the site
- Contact person (name, telephone number & email address)
- Network element software version
- OSIRIS-VUE software version
- Operating system/platform

Returned Material Department

If equipment needs to be repaired or exchanged, please contact us. A representative will give you a Return Material Authorization (**RMA**) number. You must have an **RMA** number before you ship equipment to Positron for repair.

RMA Toll Free: 1-866-331-3003 (North America only)
RMA International Line: +1-514-345-2202
Fax: +1-514-345-2304
E-mail: service@positronnetworks.com

Pack all equipment in antistatic material with sufficient protection against shipping damage and ship the equipment back to Positron. It is highly recommended that you insure your package.

Make sure that the RMA number is clearly marked on the packaging.

For USA customers, send equipment to:

Positron Inc.
c/o Freeport Forwarding
1320 Route 9
Champlain, NY
12919

For non-USA customers, send equipment to:

Positron Networks Inc.
18107 Trans-canada Highway
Kirkland, Quebec
Canada H9J 3K1

Order Entry Department

If you wish to place an order for new equipment or to inquire about the status of an already placed order, please call the Order Entry department at 1-866-331-3003 or +1-514 345-2296.

Chapter 1

Product Overview & Troubleshooting Concepts

This chapter introduces some concepts that can help you troubleshoot problems with the OSIRIS, and the OSIRIS-VUE element management software.

About OSIRIS

OSIRIS SONET multiplexers are designed to map DS1, DS3, EC-1, OC3, Ethernet, Fast Ethernet, and packets over a fiber ring. The multiplexers benefit from a fully synchronous design. The complete payload is available to every backplane slot position in a one-step multiplexing approach. This method achieves full bandwidth flexibility and provides future growth and service potential at the lowest possible cost.

Built-in to the OSIRIS are common troubleshooting tools that allow the user to isolate problems. For example, protection switching, loopback testing, and test signal generation can help in fault isolation.

Specific troubleshooting tools are available for problems related to an OSI network and to an IP network. Also, the Performance Monitoring feature is a powerful tool for early detection of network impairment.

Protection Switching

OSIRIS shelves provide both equipment and path protection.

Equipment Protection Switching

Equipment protection switching ensures mapper protection. In a 1:N configuration, one mapper can serve as a protection card for several other working mappers. Equipment protection switching can be initiated automatically or manually.

Path Protection Switching

Path protection switching ensures fiber protection. The Dual-fed Unidirectional Path Switching Ring architecture uses two fibers. Optical signals are transmitted on both fibers simultaneously and the two signals propagate along the rings to a receiving node where both signals are monitored. If a failure occurs on one fiber, the receiving node automatically switches to the other fiber.

Line Protection Switching

Automatic protection switching (APS) adds a protection mechanism at the line level (fiber cuts, other transmission defects, or card removal). Designated mappers function as protection lines for other similar mappers (for example, an Alternate PAC mapper will protect a Working PAC mapper). In the event of a user request, or a signal disruption, traffic may be switched manually, or will occur automatically as a result of error detection, from the Working mapper to the Alternate mapper. This is called a “1+1” (one protection mapper for one working mapper) configuration, and is applied to a unidirectional architecture. The mode suppported will be non-revertive, which means that a switch to the protection line is maintained even after the working line has recovered from whatever disruption caused the switch, or until a FRCD or LOCK command is executed.

APS is available for OC3c, OC3 Tributary VT, STM-1, STM-1 TU12 and PAC155 (PacketPath OC3c/STM-1 ATM Concentrator) mappers.

Autonomous Reporting

Each second, all provisioned entities are polled for health status. This health status is analyzed for failure reporting and accumulation of performance monitoring data.

Events are reported through, automatic messages, visual indicators, and relay contact closure. Refer to "Network Element Hardware Notification" on page 95. All current active events can be queried in the NE Condition database. All current active alarms can be queried in the NE Alarm database. A log of past events is stored in the NE memory and can be accessed at anytime for analysis.

This reporting could be prevented under certain circumstances. Automatic messages can be prevented from being reported by setting the condition attribute. These attributes can be set on a per entity basis. In order to present the root cause of a problem, the reporting of the consequential effects is prevented. This is to avoid unnecessary message flooding.

System Configuration Database

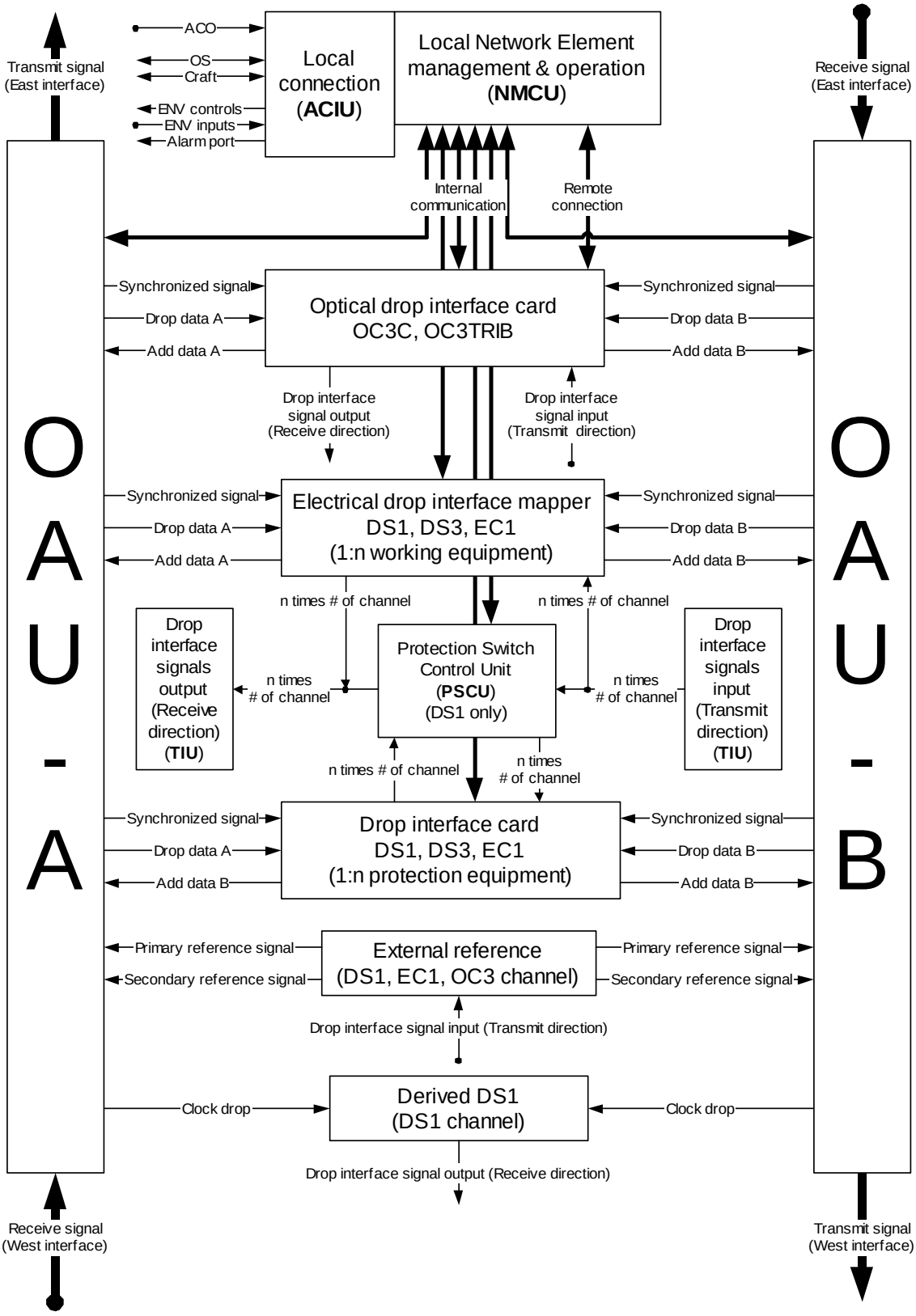
Automatic Configuration Upload

When a defective plug-in unit is replaced with a spare plug-in unit, the spare plug-in unit automatically provisions itself with the attributes of the unit that was removed.

Configuration Storage

The entire system configuration is stored in the NMCU memory, referred to as the Database. Upon changes to provisioned parameters, a complete copy of this database is saved in the NMCU non-volatile memory and a backup copy is distributed to the NE cards (the OAU's and the working mappers). Any physical manipulation of the NMCU, the OAU or the mapper cards must be performed with caution. Always replace one card at a time, and wait until the configuration is restored prior to performing a subsequent equipment manipulation.

Figure 1 OSIRIS Conceptual Diagram



OSIRIS Resource Access Controls

The OSIRIS network element provides group access controls based on the TL1 command verb. Most groups are categorized as either Information or Operation. Below is the list of OSIRIS resource access control groups.

Access Control Groups	Allowed Commands
Operation	System level Equipment Bandwidth Channel Switch Virtual path Virtual circuit Equipment switch to protection Equipment lockout Tnet shell
Information	All "retrieve" commands System level information Equipment information Bandwidth information T1/T3 channel information
Other / miscellaneous	Security administration Resource management Bus operation Service

Troubleshooting Flowcharts

The following flowcharts can help you determine which sections of this document to refer to, in order to find solutions for the particular problem you may be having. Refer to *"Figure 2: Troubleshooting Communication Problems"* if you are having difficulty connecting to the OSIRIS network element. Refer to "Figure 3: Troubleshooting Common Problems" to clear any reported alarms, error messages and conditions.

Figure 2 Troubleshooting Communication Problems

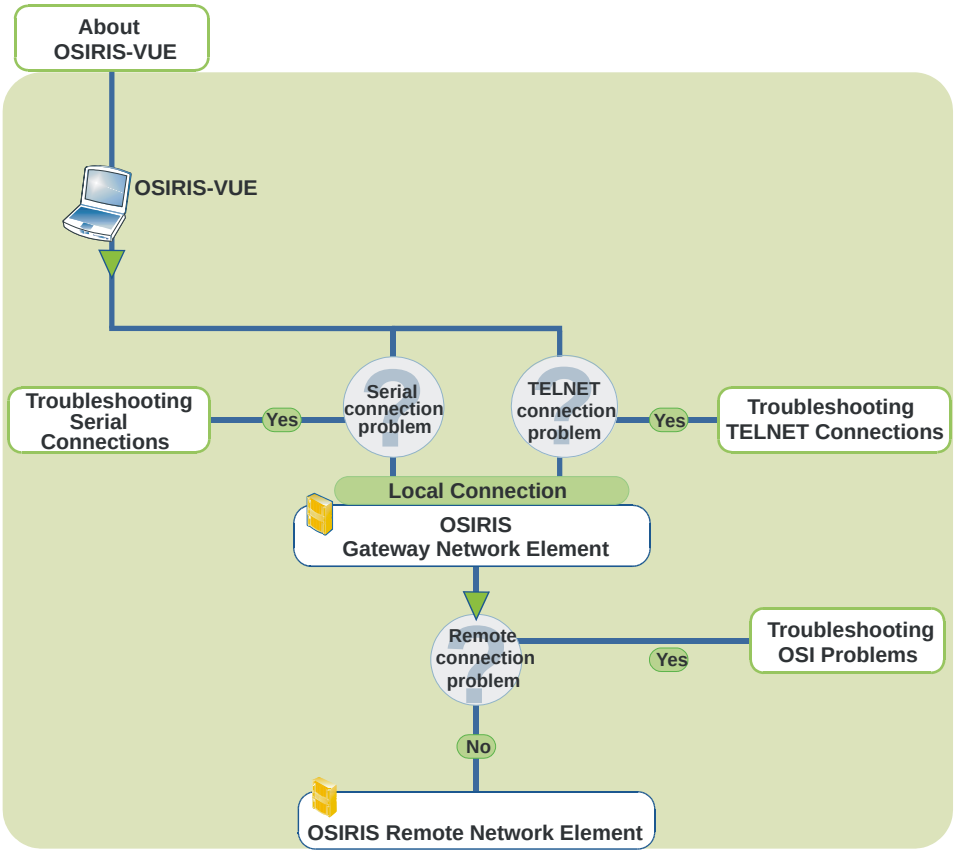
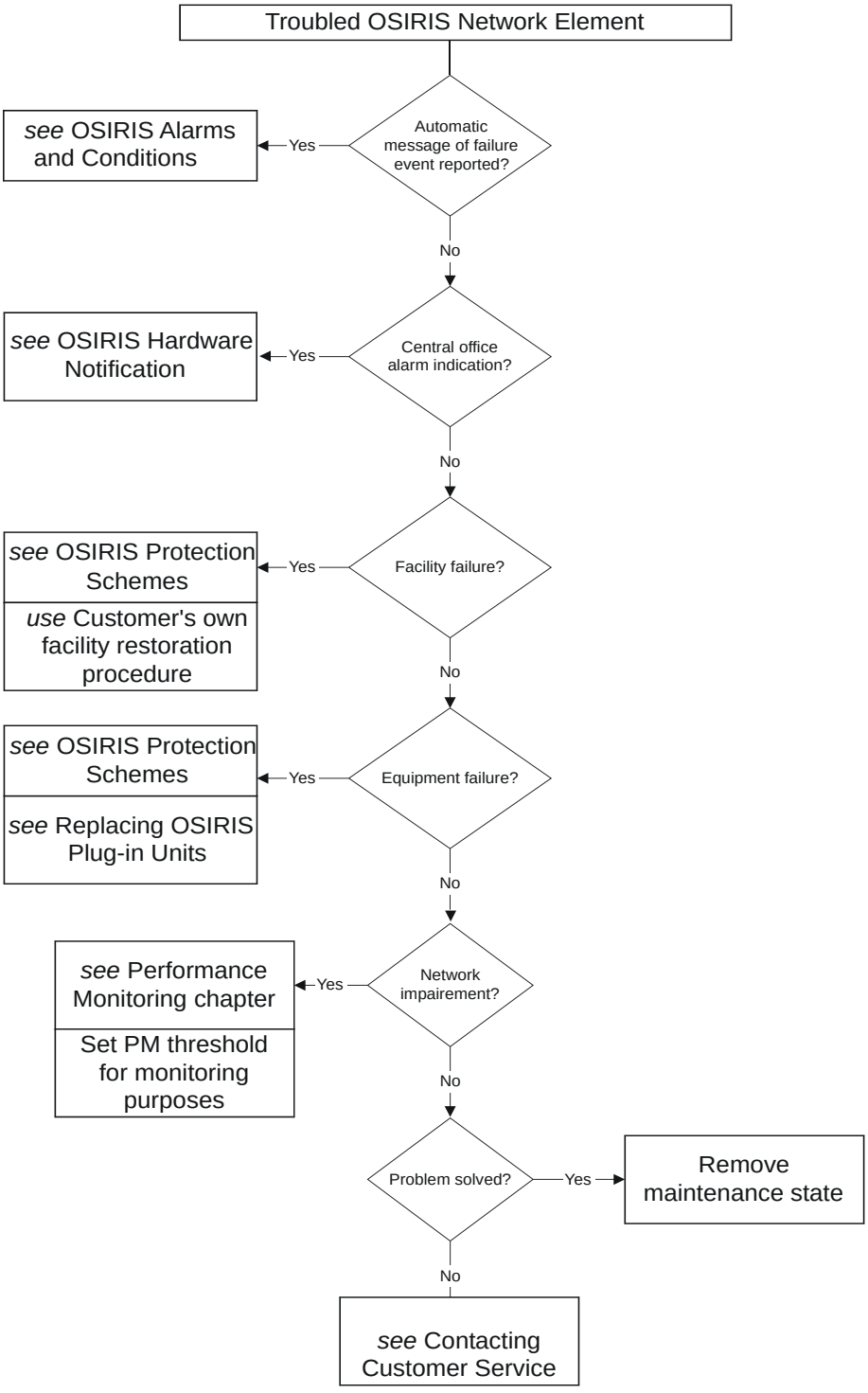


Figure 3 Troubleshooting Common Problems



Chapter 2
Communication Problems

This chapter provides guidelines on how to clear problems that may occur while attempting to establish or maintain a connection to the Network Element or a session with the Element Management System.

OSIRIS-VUE Problems

This section describes how to eliminate certain problems that may occur while using the OSIRIS-VUE software.

User cannot connect to Gateway NE

The operator cannot connect to the Gateway NE and cannot see any of the network elements.

Probable Causes

- User ID/Password is wrong. The NE validates the user ID and password and will only grant access to users that have the proper rights.
- IP address is wrong. The OSIRIS-VUE - client connects to the server using the IP stack. A valid IP address must be entered and a route must exist between the client and the server.
- Serial port setting is wrong.
- OSI configuration is wrong.

Troubleshooting TELNET Connections

The troubleshooting guidelines in this section provide techniques for investigation and resolving problems with TELNET connections. If you cannot resolve the problem using these guidelines, then the problem may be related to an IP fault.

These guidelines are for troubleshooting live problems, and not initial configuration problems.

When troubleshooting problems with TELNET, use the serial craft terminal connection to the shelf as most of the problems with TELNET will disallow any IP based communication with the shelf.

General IP/ Ethernet Diagnostic Tools

You can use the following commands, in conjunction with third party tools existing on non-OSIRIS nodes, to diagnose IP connection problems:

- PING request
- Trace route request
- ARP request
- Routing table request
- Port properties

Isolating the Problem

Typically TELNET problems fall into the following categories:

- Problems with connections
- Problems with TELNET ports
- Problems with TELNET clients

There is a specific problem resolution procedure for each of these categories of TELNET problems. As such, the first step in resolving any TELNET problem is to classify it in one of the above categories. Use the following procedure to classify TELNET problems.

1. Verify if it's possible to ping the shelf.

   - Ping remote nodes on the same subnet using IP addresses. If all pings timeout (per interface), the problem is probably related to configuration (see "Problems with Local Configuration" on page 26) or network setup (see LAN administrator).

     If some pings timeout, the problem may be on the remote node. In the case of the IP Tunneling interface, if the pings do not consistently return, there is either a system software problem or a DCC problem (see "Troubleshooting OSI Problems" on page 24).

   - Ping remote nodes on the same subnet using host names. If the pings timeout, the problem is related to the host table (see "Problems with Local Configuration" on page 26) or DNS server (see "Problems with Local Configuration" on page 26).
   - Ping remote nodes on different subnets. If the pings timeout, the problem is either related to route configuration (see "Problems with Local Configuration" on page 26) or system software. To get a better assessment of the situation, use the TRACE ROUTE REQUEST to identify the problematic gateway.

2. Try to re-connect with a craft tool for example, OSIRIS-VUE or TELNET client on a PC.

   It is possible that the connection rupture was due to a half-open or activity timeout.

   These are usually configuration mistakes with regards to interface and routing table configurations. In the case of dynamic routing (RIP), it is possible that a system software problem might arise.

   - Verify interface configuration (IP address, subnet mask)
     - Are there duplicate IP addresses? If so, correct the IP address.
     - Are the nodes on the same subnet? If not, configure to the proper subnet.
   - Verify routing entries (Routing table request)
     - Are the static gateways correctly configured? If not, edit the routing entries.
     - Is RIP updating table entries? If not, stop and re-start RIP (as a rule of thumb, wait for three minutes for proper update when re-starting RIP). If the problem persists, follow the system software failure procedure.
     - Are dynamic routing entries correct? If not, stop and re-start RIP. If the problem persists, follow the system software failure procedure.
     - Are there any conflicts between static and dynamic routes? If so, delete the static route or disable RIP.
   - Verify ARP entries (ARP request)
     - Are the IP/MAC associations correct? If not, reset the interface.

- Is the specific entry in the ARP table? If not, reset the interface and ping the specific node.

3. If the shelf is reachable and the configuration seems fine, it is very probable that the problem is due to the client terminal or an application on the client terminal.

Resolving the Problem

Use the procedures in this section to resolve TELNET connection problems.

Problems with Physical Connections

Physical connection problems are mostly related to the Ethernet cable or the Ethernet port configuration.

- Verify the condition of the Ethernet cable.
- Verify that NMCU supports 10M half-duplex.
- Remove and re-insert the Ethernet cable.

Problems with TELNET Ports

TELNET port problems arise due to modifications of the Ethernet port parameter. Values is port 23.

- Verify the configured TELNET port. Make sure it is the expected value and that the TELNET client is addressing the proper port. Refer to the appropriate user's guide for provisioning changes.

  Note: OSIRIS TCP port is 23.

Problems with TELNET Clients

TELNET disconnections can also occur because of client problems, such as, IP stack resets due to other applications.

- If you are using a regular craft terminal, verify the state of the terminal. If it was recently rebooted, try re-connecting. If the re-connect does not work, the problem can be related to internal software, especially if the terminal is running Windows 95. It is documented that ports might shut down incorrectly with Windows 95, thus rendering them unusable. In this case, reset the NMCU.

Troubleshooting Serial Connections

The troubleshooting guidelines in this section provide techniques for investigating and resolving problems with serial connections in a live network. However, the majority of problems occur during initial installation.

Isolating the Problem

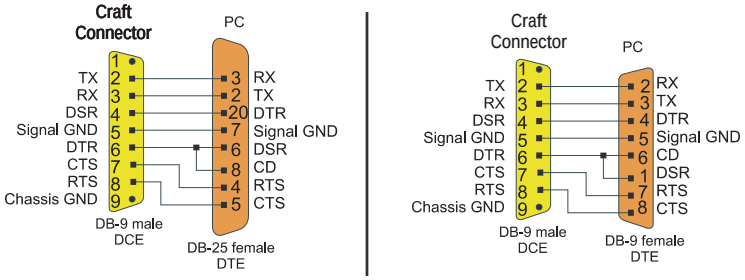
Problems with a serial connection can usually be narrowed down to a loose connection, defective cable line(s), defective equipment or improper setting of the PC terminal emulator. OSIRIS-VUE ensure proper configuration of the PC serial port.

Two serial ports are provided for access to the OSIRIS. The Craft located on the ACIU emulates a Data Communication Equipment (DCE) and provides a DB 9-pin connector. The OS emulates a Data Terminal Equipment (DTE) and provides a DB 25-pin connector.

Craft Serial Connector

The craft connector accepts two cable types: a cable ending in DB-9 to DB-25 connectors and a cable ending in DB-9 to DB-9 connectors. Refer to Figure 4 below for the wirings for these cables:

Figure 4 Craft Cable Wiring Diagram



OS Connector

The OS connector accepts two cable types: a cable ending in DB-25 to DB-25 connectors and a cable ending in DB-25 to DB-9 connectors. The cable must be a null modem when connected directly to a PC and straight when connected directly to a modem.

The connector is wired as follows:

TL1 Port	Pinouts
2	TX
3	RX
4	RTS
5	CTS
6	DSR
7	Digital Ground
8	CD
15	TXCKI
17	RXCKI
20	DTR
22	RI
24	TXCKO
25	N/C

Resolving the Problem

Use the procedures in this section to resolve serial connection problems.

Problems with Terminal Emulator Settings

If you are attempting to establish a session using a terminal emulator, make sure that the terminal emulator is configured for RTS/CTS hand shaking. The OSIRIS serial ports are set to RTS/CTS by default.

- Make sure that the hand shaking parameter on the terminal emulator is set to RTS/CTS.

Problems with Physical Connections

The problem could be related to either or both end connections of the cable.

- Verify that both end connectors are properly secured to the serial ports.

The problem could be related to a defective cable.

- Verify if there is tension in the cable. If by releasing the tension the communication can be established, the cable may be damaged and should be replaced.
- Verify if there are any signs of damage on either the connectors or the cable. If damaged, replace the cable.
- Verify if the cable functions properly with known working equipment. If the cable is apparently functional, the problem could be related to defective equipment. See "Problems with Defective Equipment" below.

Problems with Defective Equipment

The OS and Craft serial connections are directly connected to the NMCU through the ACIU.

Note: Before replacing any module, it is recommended to call customer service to validate defective equipment.

1. For a serial connection problem, replace the NMCU.

   Note: Communication will be lost while replacing the NMCU. The ACIU is responsible for the office alarms and environmental monitoring and control.

2. If replacing the NMCU does not solve the problem, proceed with the ACIU replacement.
3. If all above procedures have not resolved the problem, contact Customer Service. Refer to "Contacting Customer Service" on page 7.

Troubleshooting OSI Problems

The troubleshooting guidelines in this section provide techniques for investigating and resolving problems with OSI connections in a live network. However, the majority of problems occur during system start-up or configuration.

General OSI Diagnostic tools

You can use the following operations in conjunction with third-party tools existing on nodes to diagnose OSI connection problems.

- TARP Sequence
- Adjacency table
- ISIS table
- OSI Associations
- Target Identifier or (TID)
  (this can be a good "ping" substitute, since it does not rely on the TARP cache to retrieve the NSAP's TID, it queries the remote node)
- Network Service Access Point (NSAP)
  (this can be useful, as it queries the remote nodes when the TID is not in the TARP cache)

Isolating the Problem

There are two basic types of OSI connection problems: OSI stack problems and OSI stack application problems. OSI stack problems (including the LLSDCC and DCCLAN interfaces) are caused by the following:

- Problems with physical connections
- Problems with local configuration

There is a specific problem resolution procedure for each of these problem groups. As such, the first step in resolving any OSI connection problem is to classify it in one of the above groups. Use the following procedure to classify the OSI problems.

1. Verify if "osicfg" alarm is present. If so, NMCU must be reset to apply configuration changes.
2. Verify if the DCC Failure alarm is declared. If so, the problem is related to a LLSDCC interface—see "Problems with LLSDCC Physical Connections" on page 26.

   Sometimes, this alarm can be intermittent. This is probably because of incompatible configuration values between nodes. To resolve it see "Problems with Local Configuration" on page 26.
3. Verify that the OSI stack adjacency tables return valid data. This is to ensure that the system software is functional. If these commands timeout or return errors, the problem is in the system software.
4. Verify if the IS-IS and adjacency tables correspond to the expected network topology:

- Verify if the IS-IS (links) table is populated correctly. If not, the problem is related to configuration—see "Problems with Local Configuration" on page 26, or verify the network setup. Under normal circumstances, there should be two lines per LLSDCC link in the L1 area, and four lines per DCCLAN link (because of the pseudo-LAN).

5. Verify if the concerned node is reachable. Since the TID to NSAP resolution can be done with TARP (similar to DNS in IP, discrepancies in both tables can provoke problems under some conditions, depending on the network architecture and components:

- Obtain the NSAP with the concerned TID. If an invalid or unexpected value, such as another NSAP, is received, then the problem is related to configuration—see "Problems with Local Configuration" on page 26.

  For example, if the expected NSAP address is "39840F8000000000000000000000E09A10019600" and the returned NSAP is "39840F8000000000000000000000E09A10055400", then the TID is not assigned to the correct node. If the NSAP is not found, there must either be a network or system software problem.

- Obtain the TID using the concerned NSAP address. If an invalid or unexpected value, such as another TID, is received, then the problem is related to configuration—see "Problems with Local Configuration" on page 26.

  If the TID is not found, there must either be a network or system software problem. For example, if the expected TID address is "NODE1" and the returned TID is "NODE 4", then the TID is not assigned to the correct node.

6. Verify if the expected associations exist:

   Obtain the association. If the association is not present, there is either a configuration problem or the association needs to be re-instated—see "Problems with Local Configuration" on page 26. Under normal circumstances there should be one line per active INITIATOR connection and one line per active RESPONDER connection.

Resolving the Problem

Use the procedures in this section to resolve OSI problems.

Problems with DCCLAN Physical Connections

DCCLAN physical connection problems are mostly related to the Ethernet cable or the Ethernet port configuration for the OSLAN.

- Verify the condition of the Ethernet cable. Is it crossed, straight, or damaged?
- Verify that Ethernet port configuration supports 10M half-duplex.
- Remove and re-insert the Ethernet cable.

Problems with LLSDCC Physical Connections

LLSDCC physical connection problems are mostly related to the fiber optic cable and the L2SIDE parameter in the LLSDCC object. Fixing the problem will eliminate the DCC Failure alarm.

- Verify if the fiber optic cable is damaged. A LOS alarm is a clear indication that there is something wrong with the optical interface or cable.
- Verify if fibers are connected correctly. This is a common error especially with OSIRIS OAU-A and OAU-B (ring A/ring B).
- Verify if the neighbor LLSDCC is configured with the opposite L2SIDE value (USER-NETWORK or NETWORK-USER).

Problems with Local Configuration

Local configuration problems arise due to inconsistencies in parameter values between nodes. Fixing these types of problems requires in-depth knowledge of the OSI protocol and the effects of the parameters on connections.

CAUTION

Before you analyze the parameter values, make sure that there are no duplicate TIDs in the network. This can either break connections or establish associations with different nodes.

The following ULDCC and LLSDCC parameters can affect OSI connectivity:

LLSDCC Parameter	Description
L2SIDE	User/Network role; must be opposite to neighbor value
L2INFO	N201 – I field size; must match the neighbor value
L2IF	Outstanding I frame count; must match the neighbor value
L2SAPI	Service access point identifier; must match the neighbor value
L2TEI	Terminal Endpoint Identifier; must match the neighbor value
L2REX	N200 retry count; this value should be increased in case of transient link problems
L2WAIT	Ack timer; this value should be increased in case of transient link problems
L3ESHT	ES-IS Hello PDU configuration interval
L3ESHLD	ES-IS Hello PDU holding time
L3ISHT	IS-IS Hello PDU configuration interval
L3SIZE	Maximum NPDU size; must match the neighbor value

:

ULDCC Parameter	Description
L3ADD, L3IDP, L3ORG, L3RES, L3ROU, L3SYS	NSAP address parameters, must be in the correct format
L3SEL	NSAP selector, must match for routing
L3LSPGEN	Link state packet generation interval
L3L2SYS	Level 2 routing enabled
L4SEL, L5SEL	Transport and session selectors; must match remote values for association establishment

ULDCC Parameter	Description
L4LACK	Local acknowledgement timer, the Telcordia default is 5, Positron recommends 25
L4NOA	Transport inactivity time
L4REX	Transport retry count
L4WAIT	Retransmission timer; this value should be increased in case of transient link problems
L4ADAPT	Use adaptive retransmission algorithm
L4CONG	Use congestion avoidance

Chapter 3

Alarms, Conditions & Error Messages

This chapter describes the types of alarms, conditions and error messages you may encounter, with OSIRIS and OSIRIS-VUE, and how to deal with them.

OSIRIS Alarms and Conditions

This section contains descriptions, causes and problem resolution procedures for the OSIRIS system.

Viewing Alarms

When using OSIRIS-VUE software to administer the OSIRIS system, alarm conditions may occur. This software allows you to view all conditions, reported alarms, and events for and events for resources such as equipment, termination points and connection points. You can also view details about conditions, reported alarms, and events, such as location and the date and time of occurrence.

Condition Types

This section provides troubleshooting information for the following condition type categories:

- Equipment Condition Types
- OC-n Condition Types
- EC-n Condition Types
- STSn Condition Types
- VT Condition Types
- DS3 Condition Types
- DS1 Condition Types
- Security Condition Types
- Ethernet Condition Types
- VCG Condition Types
- OSI Association Condition Types
- File Transfer Access and Management Condition Types
- Trivial File Transfer Protocol Condition Types
- System Condition Types
- Network Element Condition Types
- Data Communication Channel Condition Types
- Session Condition Types

Equipment Condition Types

This section contains all Equipment condition types.

ACIUMISM (ACIU Card Mismatch)

This condition is reported to indicate an incompatibility between a replaceable equipment and the shelf it is seated in.

Probable Cause

- The Alarm and Control Interface Unit (ACIU) card type is not supported in this shelf.

Problem Resolution Procedure

- Upgrade your Alarm and Control Interface Unit (ACIU) card to a newer version supported by the shelf. See the equipment replacement procedure for the Alarm and Control Interface Unit (ACIU) card.

ALMCUTOFF (Alarm Cut Off)

- The ALMCUTOFF condition is reported when the audible alarm cut off (ACO) button is depressed or the audible alarm cut off command operation has been initiated.
- Depressing the ACO button or issuing the ACO command changes the state of the set of the audible alarm relay contact. It also indicates the acknowledgement, by an operator, of the warning sound.

Probable Causes

- The operator has inhibited the Alarm Audible.

Problem Resolution Procedure

- Clear alarms. Once all alarms are cleared, the ALMCUTOFF automatically clears.
- If another alarm of equal or higher severity is active, the audible relay contact is re-triggered and this alarm is cleared.

AUTOSWCMPL (Auto Switch Complete)

This condition is reported to indicate that an automatic switch request has been performed.

Probable Causes

- This is a status message.

Problem Resolution Procedure

- No action is required.

AUTOSWPNDG (Auto Switch Pending)

This condition is reported to indicate that an automatic switch request has been prevented.

Probable Cause

- The prevention of this automatic switch request is due to a defect of equal or higher priority being detected on the alternate path.

Problem Resolution Procedure

- Identify the defect of equal or higher priority on the alternate path and proceed with the appropriate problem resolution procedure.

AUTOSWWTR (Auto Wait To Restore)

The traffic of the working mapper that was automatically switched to the protection mapper has now been restored. The system waits five minutes before switching back. This message is displayed during the waiting period.

Probable Cause

- This is a status message.

Problem Resolution Procedure

- No action is required.

BERR (Bus Error)

This condition is reported by mapper equipment to indicate traffic corruption originating from the OAU towards the mapper.

Probable Cause

- Data parity errors have been detected on a mapper or on the OAU depending on which equipment is reporting the condition. This alarm is usually caused by a hardware failure.

Problem Resolution Procedure

1. Switch traffic to the protection mapper. If the alarm clears, then the mapper is defective.
2. If the alarm does not clear after more than 20 seconds, replace the OAU. Refer to "Replacing OSIRIS Plug-in Units" on page 116.
3. If you have tried using different OAUs and different mappers, the backplane may be defective. Replace the shelf.

COMLNKDWN (Communication Link Down)

This condition is reported to indicate that the MCU/NMCU cannot communicate with the equipment.

Probable Cause

- The equipment software may be resetting
- The equipment may be defective

Problem Resolution Procedure

- If the mapper was just inserted, wait at least two minutes.
- If the COMLNKDWN does not clear after two minutes, software on the mapper may be corrupted.
- Remove and replace the mapper. Refer to "Replacing OSIRIS Plug-in Units" on page 116.

CRDMISMAT (Card Mismatch)

This condition is reported to indicate that the provisioned equipment for a slot does not match the current equipment in the slot.

Probable Cause

- A card has been inserted in a shelf slot that is provisioned for another type of card.
- The wrong type of OAU is recognized by the shelf
- A secondary clock is provisioned on an OAU that does not support a secondary clock.
- The *Lock mode* is set on an OAU that does not support this mode.

Problem Resolution Procedure

OAU cards

- Verify that the MCU has the appropriate software.
- An OC-3 shelf must use NE software version 3.*n.xx*, and an OC-12 shelf must use 3.*nn.xx*, where both *n* and *x* represent single digits from 0 to 9. The second field is always a single digit for OC-3 systems and a double digit for OC-12 systems. NMCUs in SONET systems must use NE software 5.*n.xx* or 5.*nn.xx*.

  For release 10 and above, an OC-3 shelf must use NE software version *n*1.*xx.xx*, and an OC-12 shelf must use *n*2.*xx.xx*, where both *n* and *x* represent single digits from 0 to 9.
- If an EC1VT mapper card is provisioned in an OC-3 system, then the OAUs must be one of the following products to support the *Lock mode*.

  OC3 OAU product codes: 800310/3, 800310/4, 800311/3, 800311/4, 800317/2, 800317/4, 800318/2, 800318/4
- If you have provisioned a secondary clock on an OC-12 system that has older OAUs, de-provision the secondary clock or upgrade the OAUs.
- Older OC-12 OAU cards do not support the secondary clock feature. OC-12 OAUs that have product codes ending with "/2" fully support the secondary clock feature.
- If either the inventory or product number is missing, the shelf cannot recognize the card. Replace the OAU.

Mapper cards

- A mapper has been provisioned as a different type of mapper. Replace it with a mapper of the correct type.
- Re-provision the mapper.
- If either the inventory or product number is missing, the shelf cannot recognize the card. Replace the mapper.

CRDRMVD (Card Removed)

This condition is reported to indicate that provisioned equipment is not detected by the software.

Probable Cause

A Card Removed alarm can appear when:

- a provisioned card has been removed from its slot in the shelf

- the card was absent when it was provisioned
- the card's power supply has failed
- a single OAU is used for a point-to-point connection.

Problem Resolution Procedure

- Insert the appropriate card.
- If the card is inserted and the alarm remains, the card may be damaged. If this is the case, replace the card. Refer to "Replacing OSIRIS Plug-in Units" on page 116.
- If this is an OC-3 system, the BIU card may be missing or defective. If this is the case, replace the card. Refer to "Replacing OSIRIS Plug-in Units" on page 116.
- If you are using a single fiber for a point-to-point connection, the Card Removed alarm indicates that only one OAU is installed on the shelf. You can provision or filter out this alarm.

EQPT (Equipment Failure)

The EQPT failure is reported when a fault is detected in one or more hardware component.

Hardware faults are detected via diagnostic routines, and by monitored status and control points.

Probable Cause

- A hardware module has failed
- The 64-pin amphenol transmit/receive connectors are reversed (DS1 mapper only).

Problem Resolution Procedure

- If this is a DS1 mapper, make sure that the amphenol transmit connector is connected to *out* and that the receive connector is connected to *in*.
- If the connectors are reversed, the mapper is not defective.
- Verify the patch cord or cross-connection at the DSx patch panel. Make sure that *in* and *out* signals are connected correctly.
- Replace the failed card.

LED is amber when:

- The working mapper has failed and is protected.
- The protection mapper has failed
- The OAU has failed but a second OAU is present.

LED is red when:

- The working mapper has failed and is not protected.
- The OAU has failed but a second OAU is not present.
- An MCU or NMCU LED is red for approximately two minutes when software is being switched. If this is the case, do not remove the card, as this is normal behavior

EXBER (External Bus Error)

This condition is reported by the OAU equipment to indicate traffic corruption originating from the mapper towards the OAU.

Probable Cause

- Parity errors have been detected. This alarm can be caused by a failed mapper, a failed OAU, or a defective backplane

Problem Resolution Procedure

- Check for an OAU failure. Replace a defective OAU.
- Verify that at least one of the network elements in the ring is provisioned as the master reference clock (local or external clock).
- An EXBER alarm can occur if no master reference clock is provisioned.
- Check whether a mapper is defective. To do so, for each protected mapper, switch traffic to the protection mapper. If the alarm clears, you have most likely isolated the defective mapper.
- If you have tried using different OAUs and different mappers, the backplane is probably defective. Replace the shelf.

FEATMISM (Feature Mismatch)

- This condition is reported to indicate that the provisioned DS1 equipment type do not match the current equipage for that slot.

Probable Cause

- The DS1 card type is not provisioned correctly.
- The slot is equipped with the wrong equipment type.

Problem Resolution Procedure

- Make sure that a DS1 mapper is not provisioned as a DS1PM or as a DS1PM+ mapper.
- Also make sure that a DS1 or DS1PM mapper is not provisioned as a DS1PM+ mapper.
- Make sure that the T1 frame format is set correctly.
- Regular DS1 mappers can be used in unframed mode only, but DS1PM and DS1PM+ mappers can be used in unframed, super frame (SF) and extended super frame modes (ESF). Refer to the table below to match mapper product codes with supported frame formats.

	Product Code	Supported Frame Formats	Direction
DS1	800320/4	Unframed	none
	800320/4A	Unframed	none
	800320/4B	Unframed	none
	800320/7A	Unframed	none
	800320/7B	Unframed	none
DS1PM	800324	Unframed, SF, and ESF	Tx only
	800327	Unframed, SF, and ESF	Tx only
DS1PM+	800334	Unframed, SF, and ESF	Tx and Rx
	800337	Unframed, SF, and ESF	Tx and Rx

FRCDSWCMPL (Forced Switch Complete)

This condition is reported to indicate that a force switch request has been performed.

Probable Cause

- This is a status message.

Problem Resolution Procedure

- No action is required.

FRCDSWPNDG (Forced Switch Pending)

This condition is reported to indicate that an automatic switch request has been prevented.

Probable Cause

- The protection equipment missing
- The protection equipment is defective.
- For DS1 mapper, the Protection Switch Control Unit (PSCU) is missing.
- For DS1 mapper, the Protection Switch Control Uni (PSCU) is defective.
- For DS1 MICRO Shelf, the Alarm and Control Interface Unit (ACIU) is missing.
- For DS1 MICRO Shelf, the Alarm and Control Interface Unit (ACIU) is defective.

Problem Resolution Procedure

- The protection mapper may be absent. Insert a protection mapper.
- The protection mapper may be defective. Replace the defective mapper. Refer to "Replacing OSIRIS Plug-in Units" on page 116.
- If this is a DS1 mapper, verify that the PSCU is present.
- If this is a DS1 mapper, the PSCU may be defective. Replace the PSCU if necessary. Refer to "Replacing OSIRIS Plug-in Units" on page 116.
- If this is a DS1 MICRO Shelf, the Alarm and Control Interface Unit (ACIU) may be inserted improperly. Secure the Alarm and Control Interface Unit (ACIU) in position.
- If this is a DS1 MICRO Shelf, the Alarm and Control Interface Unit (ACIU) may be defective. Replace the Alarm and Control Interface Unit (ACIU) if necessary. Refer to "Replacing OSIRIS Plug-in Units" on page 116.

FRCDSWREQ (EQPT Force Switch Request)

An equipment force switch request has been initiated.

Probable Cause

- This is a status message.

Problem Resolution Procedure

- No action is required.

ICBLMISM (Input Cable Mismatch)

The ICBLMISM condition is reported to indicate a problem with the cable type or cable connection.

Probable Cause

- The Alarm and Control Interface Unit (ACIU) input cable on the MICRO shelf does not match the protection scheme.
- The Alarm and Control Interface Unit (ACIU) input cable on the MICRO shelf is disconnected

Problem Resolution Procedure

- Replace the Alarm and Control Interface Unit (ACIU) input cable with one that corresponds to the protection scheme. See the following table for product numbers.

Cable Type	Product Number
Protected	**800791**
Unprotected	**800790**

- Re-connect the Alarm and Control Interface Unit (ACIU) input cable.

INTPERR (Internal Parity Error)

This condition is reported by the Ethernet equipment to indicate that corrupted data has been detected within the equipment.

Probable Cause

- This alarm is usually caused by a hardware failure on the mapper card.

Problem Resolution Procedure

- The mapper is defective. Replace the mapper. Refer to "Replacing OSIRIS Plug-in Units" on page 116.

INTUNTRMVT (Interface Unit Missing)

The FASTE Ethernet mapper is available with an electric or optic interface. The interface unit is thus removable. This condition is reported when the interface is not detected on the equipment.

Probable Cause

- The connector interface unit on the Ethernet mapper is missing.

Problem Resolution Procedure

- Remove the Ethernet mapper from the shelf and secure the connector interface unit in place.

LCKOUTCMPL (Lockout Complete)

A lockout switch request has been initiated on the protection equipment.

Probable Cause

- This is a status message.

Problem Resolution Procedure

- No action is required.

LCKOUTREQ (EQPT Lockout Protection Request)

An equipment lockout request has been initiated on the protection equipment.

Probable Cause

- This is a status message.

Problem Resolution Procedure

- No action is required.

LCKOUTREQ (EQPT Lockout Working Request)

An equipment lockout request has been initiated on the working equipment.

Probable Cause

- This is a status message.

Problem Resolution Procedure

- No action is required.

LINE (OAU RX Line Clock Inactive)

This condition is reported to indicate that the OAU, configured for through timing, as lost its synchronization reference. Its synchronization reference is the optical signal received on its interface.

Probable Cause

- A LOS, a LOF, or an AIS-L is detected on the line interface for that OAU. This condition is reported when the OAU's are configured for through timing.

Problem Resolution Procedure

- Look for a fiber cut on the spans adjacent to the network element that is reporting the alarm.
- Check for an OAU failure. Replace a defective OAU.
- Examine higher priority alarms.

LOF (OAU Loss of Frame)

An LOF condition is reported when a Severely Error Frame (SEF) defect persists for a period of time.

A SEF defect is detected when the incoming signal has a minimum of four consecutive frames with framing error.

Probable Cause

- Incompatible signal type
- Excessive degradation of the optical fiber
- Coupling attenuation
- Failure on the far-end transmitter
- Internal equipment failure

Problem Resolution Procedure

1. Check the provisioning and make sure that the far end is transmitting the proper signal type expected by the near end.
2. Disconnect the Rx fiber. Measure the input power by optical power meter. Check if the input power is within the range between the minimum receiver sensitivity power and the overload power.
3. If the input power is within the range, clean the Rx connector on the OC-n line card, re-connect the Rx fiber. If the alarm remains active, replace the line card.
4. If the input power is too high, insert a proper attenuator in the fiber and re-connect the fiber to the OC-n interface.
5. If the input power is too low, disconnect the Tx fiber at the remote end. Measure the output power by the optical power meter at the remote end. Check if the output power is not lower than the minimum transmitter power specified for the relevant OC-n interface.
6. If the output power is too low, replace the line card at the remote end.
7. If the output power is not too low. Repair or replace the fiber from the remote end to the near end.

LOS (OAU Loss of Signal)

An LOS condition is reported when an "all-zeros pattern" persists for a period of time.

An "all-zeros pattern" corresponds to no light pulses for OC-n optical interfaces.

Probable Causes

- Fibre or cable cut
- Excessive degradation of the optical fibre
- Coupling attenuation
- Failure on the far-end transmitter
- Internal equipment failure
- A multi-mode transmitter is being used with a mono-mode fibre.

Problem Resolution Procedure

1. Disconnect the Rx fiber. Measure the input power by optical power meter. Check if the input power is within the range between the minimum receiver sensitivity power and the overload power.
2. If the input power is within the range, clean the Rx connector on the OC-n line card, re-connect the Rx fiber. If the alarm remains active, replace the line card.
3. If the input power is too low, disconnect the Tx fiber at the remote end. Measure the output power by the optical power meter at the remote end. Check if the output power is not lower than the minimum transmitter power specified for the relevant OC-n interface.
4. If the output power is too low, replace the line card at the remote end.
5. If the output power is not too low. Repair or replace the fiber from the remote end to the near end.

LOT (OAU Loss of Transmitter)

This condition is reported by the OAU equipment to indicate that the laser output level is too low.

Probable Cause

- The optical transmitter is not sending a signal.

Problem Resolution Procedure

- The card has failed. Replace the defective card. Refer to "Replacing OSIRIS Plug-in Units" on page 116.

MANSWCMPL (Manual Switch Complete)

The operator has initiated a manual switch to protection, and the switch has been successfully completed.

Probable Cause

- This is a status message.

Problem Resolution Procedure

- No action is required.

OCBLMISM (Output Cable Mismatch)

This condition is reported to indicate that the provisioned protection scheme is incompatible with the equipped output cable connected to the Alarm and Control Onterface Unit (ACIU) on a MICRO DS1 shelf. The cable arrangement depends on the protection scheme used for DS1 mappers.

Probable Cause

- Equipment redundancy is enabled and the shelf is equipped with an unprotected DS1 equipment cable configuration.
- Equipment redundancy is disabled and the shelf is equipped with a protected DS1 equipment cable configuration.

Problem Resolution Procedure

- Verify that the proper cable type is used. Depending if the redundancy has been enabled or disabled, the proper cable type must be used.
- Replace the Alarm and Control Interface Unit (ACIU) output cable with one that corresponds to the protection scheme. See the following table for product numbers.

Cable Type	Product Number
Protected	800791
Unprotected	800790

- Provision the appropriate protection scheme.

OOF (OAU Out of Frame)

Four consecutive incorrect framing patterns have been received in 3 consecutive seconds.

Probable Cause

- This alarm may be caused by an intermittent defect on an optical interface.
- Framing errors are being detected on the incoming signal.

Problem Resolution Procedure

- Verify the receive power on the OAU. This alarm can be reported if receive power is too high.
- Make sure that OAU types are correct. If this is an OC-3 system, make sure that no OC-12 OAUs are in use, and vice-versa.
- An OAU may be defective. Check the first OAU upstream for hardware failure and replace if necessary.
- The upstream network element may have lost clock synchronization. Re-establish upstream network element synchronization. This might require replacing a failed OAU. Refer to "Replacing OSIRIS Plug-in Units" on page 116.
- Verify that one of the network elements in the ring is provisioned as the master clock (local or external clock). An LOF can occur if no master clock is defined.

PFEATMISM (Protection Feature Mismatch)

This condition is reported to indicate that the protection equipment do not support all the features that at least one of the working equipment supports.

Probable Cause

- At least one protected T1 channel frame format is set to superframe (SF) or extended super frame (ESF), while the protection mapper do not supports monitoring of frame format.

Problem Resolution Procedure

- Replace the protection mapper with one that supports the monitoring of the frame format provisioned on the protected T1 channel, or set all the T1 frame format on all protected T1 channel to unframed.
- Regular DS1 mappers cannot monitor frame format, while DS1PM and DS1PM+ mappers can monitor super frame (SF) and extended super frame format (ESF). Refer to the table that follows to match mapper product codes with supported frame format.

	Product Code	Supported Frame Formats	Direction
DS1	800320/4	Unframed	none
	800320/4A	Unframed	none
	800320/4B	Unframed	none
	800320/7A	Unframed	none
	800320/7B	Unframed	none
DS1PM	800324	Unframed, SF, and ESF	Tx only
	800327	Unframed, SF, and ESF	Tx only
DS1PM+	800334	Unframed, SF, and ESF	Tx and Rx
	800337	Unframed, SF, and ESF	Tx and Rx

PRIEXT (OAU Primary External Clock Inactive)

This condition is reported to indicate that the OAU, configured for external timing, as lost its synchronization reference. Its synchronization reference is the interface configured as primary reference.

Probable Cause

- This alarm is reported if the primary clock is provisioned and has failed or a signal failure is detected incoming from the reference interface.

Problem Resolution Procedure

- Verify the primary clock input.
- Force traffic to protect on the mapper that is provisioned for the secondary clock.
- If the PRIEXT alarm clears on the protection mapper, then the working mapper is defective. Replace the defective mapper. Refer to "Replacing OSIRIS Plug-in Units" on page 116.
- Make sure that your shelf contains one of the following combinations of DS1 and OAU cards to support secondary external timing.
- The DS1 mapper that must be provisioned to carry the clock are:

DS1 product codes

800320/4B, 800320/7A, 800324, 800327, 800334, 800338

The OAU cards that support secondary external clock are:

OAU product codes

OC-3: 800310/2, 800310/3, 800310/4, 800311/2, 800311/3, 800311/4, 800314, 800315, 800317, 800317/2, 800317/4, 800318, 800318/2, 800318/4

OC-12: 800510/2, 800511/2, 800512/2, 800513/2, 800514/2, 800515/2

RDBER (Receive Data Bus Error)

This condition is reported by OAU equipment to indicate traffic corruption originating from the OAU towards the mapper.

Probable Cause

- Parity errors have been detected on the OAU receiver.

Problem Resolution Procedure

- Check for an OAU failure on this node or the upstream node. Replace a defective OAU. Refer to the equipment replacement procedure section.
- Verify that only one of the network elements in the ring is provisioned as the master clock (local or external clock). All other network elements must be provisioned as slaves (THRU line timing).
- A RDBER can occur if no master clock is defined, or if more than one master clock is defined.

RDCER (Receive Data Checksum Error)

This condition is reported by OAU equipment to indicate traffic corruption between the OAU towards the mapper.

Probable Cause

- Checksum errors have been detected on the OAU receiver.

Problem Resolution Procedure

- Check for an OAU failure on this node or the upstream node. Replace a defective OAU.
- Verify that only one of the network elements in the ring is provisioned as the master clock (local or external clock). All other network elements must be provisioned as slaves (THRU line timing).
- A RDCER can occur if no master clock is defined, or if more than one master clock is defined.

RESET (Software Reset)

This condition is reported when the MCU/NMCU, or a mapper software has reset.

Probable Cause

- This is a status message.

Problem Resolution Procedure

- No action is required.

REVMISM (Revision Mismatch)

This condition is reported to indicate an incompatibility between the MCU/NMCU software version and the equipment software version.

Probable Cause

- The DS1PM+ mapper software is not compatible with the MCU/NMCU software.
- The EC1TSA mapper software is not compatible with the MCU/NMCU software.
- Packet Path mapper software is not compatible with the MCU/NMCU software.
- MSE mapper software is not compatible with the MCU/NMCU software.

Problem Resolution Procedure

- Make sure that the software versions are compatible, or upgrade both software to the latest versions.
- Refer to *OSIRIS® Network User's Guide (206-002)* for software upgrade procedures.

SD (Line Signal Degrade)

An SD is declared when transmission degradations have reached the Signal Degrade Threshold of $1x10^{-9}$ on the OAU.

Probable Cause

- Degradation of the optical fibre
- Increasing coupling attenuation

- Failure on the far-end transmitter
- Internal equipment failure

Problem Resolution Procedure

- Investigate for a bent fibre.
- Clean the fibre patch cords with alcohol and lint-free tissue.
- The signal can degrade when pig tails are dirty.
- Use a light meter to measure incoming optic levels at OAU inputs.
- If input levels are below normal, then either the distance between nodes is too great for this type of OAU, or the OAU is slowly degrading.
- Check for an OAU failure. Replace a defective OAU. Refer to "Replacing OSIRIS Plug-in Units" on page 116.
- Check for loose connections at the fiber patch panel on the OAU, or on the mapper.

SECEXT (OAU Secondary External Clock Inactive)

This condition is reported to indicate that the OAU, configured for external timing, as lost its synchronization reference. Its synchronization reference is the interface configured as secondary reference.

Probable Cause

- This alarm is reported if the secondary clock is provisioned and has failed or a signal failure is detected incoming from the reference interface.

Problem Resolution Procedure

- Verify the secondary clock input.
- Force traffic to protect on the mapper that is provisioned for the secondary clock.
- If the SECEXT alarm clears on the protection mapper, then the working mapper is defective. Replace the defective mapper. Refer to "Replacing OSIRIS Plug-in Units" on page 116.
- Make sure that your shelf contains one of the following combinations of DS1 and OAU cards to support secondary external timing.

The DS1 mapper that must be provisioned to carry the clock are:

DS1 product codes

800320/4B, 800320/7A, 800324, 800327, 800334, 800338

The OAU cards that support secondary external clock are:

OAU product codes

OC-3: 800310/2, 800310/3, 800311/2, 800311/3, 800314, 800315, 800317, 800317/2, 800318, 800318/2

OC-12: 800510/2, 800511/2, 800512/2, 800513/2, 800514/2, 800515/2,

SL-MLINE (Select Mate Line)

The OAU has switched to an alternate clock reference. The OAU has selected the Mate Rx Line Clock

Probable Cause

- This is a status message.

Problem Resolution Procedure

- No action is required.

SL-LINE (Select Line)

The OAU has switched to an alternate clock reference. The OAU has selected the Rx Line Clock

Probable Cause

- This is a status message.

Problem Resolution Procedure

- No action is required.

SL-LOCAL (Select Local Oscillator)

The OAU has switched to an alternate clock reference. The OAU as Selected the Local Oscillator

Probable Cause

- This is a status message.

Problem Resolution Procedure

- No action is required.

SL-MLOCAL (Select Mate Local Oscillator)

The OAU has switched to an alternate clock reference. The OAU has selected the Mate Local Oscillator

Probable Cause

- This is a status message.

Problem Resolution Procedure

- No action is required.

SL-PRIEXT (Select Primary External Reference)

The OAU has switched to an alternate clock reference. The OAU as Selected the Primary External Clock.

Probable Cause

- This is a status message.

Problem Resolution Procedure

- No action is required.

SL-SECEXT (Select Secondary External Reference)

The OAU has switched to an alternate clock reference. The OAU as Selected the Secondary External Clock.

Probable Cause

- This is a status message.

Problem Resolution Procedure

No action is required.

STSnUNEQ (STS-n Path Unequipped - where n=1 to 48)

A received signal label is considered Unequipped if it is equal to an all-zeros value.

For Virtual Tributary path connections that are not equipped or equipped but not provisioned, the NE will generate all-zeros STS SPEs with "valid" Payload Pointers.

Probable Cause

- The OAU bandwidth for that STS is deleted or unassigned elsewhere in the ring.
- The STS cross-connection is not provisioned on a remote equipment.

Problem Resolution Procedure

- Check software settings for STS bandwidth assignments.
- The circuit is provisioned to receive a signal from an inactive STS. Locate the inactive STS.

SYCK (OAU System Clock Inactive)

This condition is reported by the OAU equipment to indicate a internal timing circuitry problem.

Probable Cause

- The system clock on the OAU has failed.

Problem Resolution Procedure

- Check for an OAU failure. Replace a defective OAU. Refer to "Replacing OSIRIS Plug-in Units" on page 116.

SYNCSTATCHNG (OAU Synchronization Status Change)

This condition is declared to indicate that the received synchronization status message value has changed.

Probable Cause

- This is a status message.

Problem Resolution Procedure

- No action is required.

TLOC (OAU Tx Clock Inactive)

This condition is reported by the OAU equipment to indicate that traffic is not being sent.

Probable Cause

- The transmitter clock unit part of the OAU equipment has failed.

Problem Resolution Procedure

- The OAU is defective, replace the equipment. Refer to "Replacing OSIRIS Plug-in Units" on page 116.

TLOS (OAU TX Loss of Signal)

This condition is reported by the OAU equipment to indicate that the laser output level is too low.

Probable Cause

- The optical transmitter is not sending a signal.

Problem Resolution Procedure

- The card has failed. Replace the defective card. Refer to "Replacing OSIRIS Plug-in Units" on page 116.

UPLOC (Microprocessor Loss of Clock)

The Microprocessor loss of clock condition is reported to indicate an impairment in the OAU internal circuitry.

Probable Cause

- The OAU is defective.

Problem Resolution Procedure

- Replace the OAU. Refer to "Replacing OSIRIS Plug-in Units" on page 116.

OC-n Condition Types

This section contains all OC3, OC12 and OC48 condition types.

ACLKFAIL (OC3 A Clock Fail)

This condition is reported to indicate that the clock source from the specified OAU, that is, A and/or B is inactive.

Probable Causes

- The OAU A is absent
- The OAU A is defective
- An OC3 mapper is defective

Problem Resolution Procedure

- Make sure that the OAU A is present. A removed OAU may cause the detection of a clock source to fail, but do not imply a defective equipment.
- Check for an OAU failure and replace it if necessary. Refer to "Replacing OSIRIS Plug-in Units" on page 116.
- Check for a mapper failure and replace it if necessary. Refer to "Replacing OSIRIS Plug-in Units" on page 116.

AIS-L (Alarm Indication Signal Detected – Line)

An AIS-L condition is reported when an AIS-L defect persists for a period of time.

An STE (and physical layer regenerators) sends an AIS-L to alert the downstream LTE that a defect has been detected on the incoming SONET section, or that the LTE supporting the provisioned line origination functions has failed.

Probable Causes

- Terminal loopback is active at the remote end. An NE is generating an AIS-L on an OC-n loopback.
- The NE is receiving an AIS-L from a remote equipment, such as a regenerator, due to a failure detected upstream from that equipment.
- The remote equipment is defective.

Problem Resolution Procedure

- Check if an OC-n Terminal loopback is active at the remote end. If the loopback is active, release the loopback.
- Check if an equipment alarm is active at the remote end. If an equipment alarm is active, follow the clearing procedure for the active alarm.
- If neither the loopback on OC-n line or the equipment alarm is active, replace the OC-n line card at the remote end.

APSB (APS Byte Failure)

An APSB is declared when a Protection Switching Byte defect persists for a period of time. The defect occurs when either an inconsistent APS byte or an invalid code is detected.

An inconsistent APS byte occurs when consecutive K1 bytes of successive frames are not identical, starting with the last frame containing a previously consistent byte. An invalid code occurs when the incoming K1 byte contains an unused code, or a code irrelevant for the specific switching operation consecutive frames. An invalid code also occurs when the incoming K1 byte contains an invalid channel number in consecutive frames.

Probable Causes

- An undefined, unused, or unsupported K1 code has been detected.
- A request for an invalid channel number has been received. For example, Channel 2 in a 1+1 architecture.

Problem Resolution Procedure

- Verify that both ends of the span are provisioned.
- Verify that the provisioning at both ends of the span is compatible.
- Verify the line signal integrity. Line level performance monitoring statistics will increment if an inconsistent APS byte is detected. Refer to “Chapter 6: Performance Monitoring” for the proper PM statistic. If the line signal is impaired proceed with the appropriate line signal measurement and replace any defective equipment. Refer to “Replacing OSIRIS Plug-in Units” on page 116.
- If the line signal level is within specification and the receiving equipment is operating within specification, either the transmitting or receiving equipment internal circuitry is malfunctioning. Proceed with the transmitting equipment replacement. Refer to “Replacing OSIRIS Plug-in Units” on page 116.

- If the problem remains, proceed with the receiving equipment replacement. Refer to "Replacing OSIRIS Plug-in Units" on page 116.

AUTOSWCMPL (Auto Switch Complete)

A signal failure or a signal degraded has been detected on the working. The protection line carries the traffic.

Probable Causes

This is a status message.

Problem Resolution Procedure

No action required.

AUTOSWPNDG (Auto Switch Pending)

A signal failure or a signal degraded has been detected on the working line and a signal failure was already detected on the protection line, or a signal degraded has been detected on the working line and a signal degraded was already detected on the protection line.

See the Protection switch section for signal failure and signal degrades detection criteria.

Probable Cause

This is a status message.

Problem Resolution Procedure

No action required.

BCLKFAIL (OC3 B Clock Fail)

The clock source from the specified OAU, that is, A and/or B is inactive.

Probable Causes

- The OAU B is absent
- The OAU B is defective
- An OC3 mapper is defective

Problem Resolution Procedure

- Make sure that the OAU B is present. A removed OAU may cause the detection of a clock source to fail, but does not imply defective equipment.
- Check for an OAU failure and replace it if necessary. Refer to "Replacing OSIRIS Plug-in Units" on page 116.
- Check for a mapper failure and replace it if necessary. Refer to "Replacing OSIRIS Plug-in Units" on page 116.

FRCDSWCMPL (Forced Switch Complete)

A forced switch request has been successfully operated.

The traffic has been forced onto the switch request targeted line. The targeted line is carrying the traffic.

Probable Cause
This is a status message.

Problem Resolution Procedure
No action is required.

FRCDSWREQ (Line Force Switch Active)
A line force switch request is active on the targeted line. The targeted line can either be the protection or the working line.

Probable Cause
This is a status message.

Problem Resolution Procedure
No action required.

HLDNA (Holdover Not Achieved Alarm)
A Holdover Not Achived Alarm a clocking difference between the Local OAU and the OAU from the preceding Node.

Probable Cause
- Bad Local OAU or from preceding Node.

Problem Resolution Procedure
- The card has failed. Replace the defective OAU card. Refer to "Replacing OSIRIS Plug-in Units" on page 116.

LCKOUTCMPL (Lockout Complete)
A lockout switch request has been successfully operated.

The traffic has been locked out of the protection line. The working line is carrying the traffic.

Probable Cause
This is a status message.

Problem Resolution Procedure
No action is required.

LCKOUTREQ (Line Lockout Active)
A line lockout switch request is active on the targeted line. The targeted line can either be the protection or the working line.

Probable Cause
This is a status message.

Problem Resolution Procedure
No action required.

LCLKFAIL (OC3 Local Clock Fail)

This condition is reported to indicate that the recovered clock, derived from the local line, unit part of the equipment has failed.

Probable Cause

- An OC3 card is defective.
- Some Ethernet equipment is defective.

Problem Resolution Procedure

- Ensure that no LOS is detected on the local line. A LOS may cause the detection of a local line clock failure, but does not imply defective equipment.
- If a LOS is not detected simultaneously, the working mapper is probably defective. Refer to "Replacing OSIRIS Plug-in Units" on page 116.

LINE (OAU RX Line Clock Inactive)

This condition is reported to indicate that the OAU, configured for through timing, as lost its synchronization reference. Its synchronization reference is the optical signal received on its interface.

Probable Cause

- A LOS, a LOF, or an AIS-L is detected on the line interface for that OAU. This condition is reported when the OAU's are configured for through timing.

Problem Resolution Procedure

- Look for a fiber cut on the spans adjacent to the network element that is reporting the alarm.
- Check for an OAU failure. Replace a defective OAU.
- Examine higher priority alarms.

LOF (Loss of Frame)

An LOF condition is reported when a Severely Error Frame (SEF) defect persists for a period of time.

A SEF defect is detected when the incoming signal has a minimum of four consecutive frames with framing error.

Probable Causes

- Incompatible signal type
- Excessive degradation of the optical fiber
- Coupling attenuation
- Failure on the far-end transmitter
- Internal equipment failure

Problem Resolution Procedure

1. Check the provisioning and make sure that the far end is transmitting the proper signal type expected by the near end.

2. Disconnect the Rx fiber. Measure the input power by optical power meter. Check if the input power is within the range between the minimum receiver sensitivity power and the overload power.
3. If the input power is within the range, clean the Rx connector on the OC-n line card, re-connect the Rx fiber. If the alarm remains active, replace the line card.
4. If the input power is too high, insert a proper attenuator in the fiber and connect the fiber back to the OC-n interface.
5. If the input power is too low, disconnect the Tx fiber at the remote end. Measure the output power by the optical power meter at the remote end. Check if the output power is not lower than the minimum transmitter power specified for the relevant OC-n interface.
6. If the output power is too low, replace the line card at the remote end.
7. If the output power is not too low. Repair or replace the fiber from the remote end to the near end.

LOS (Loss of Signal)

An LOS condition is reported when an "all-zeros pattern" persists for a period of time.

An "all-zeros pattern" corresponds to no light pulses for OC-n optical interfaces.

Probable Causes

- Fibre or cable cut
- Excessive degradation of the optical fibre
- Coupling attenuation
- Failure on the far-end transmitter
- Internal equipment failure
- A multi-mode transmitter is being used with a mono-mode fibre.

Problem Resolution Procedure

1. Disconnect the Rx fiber. Measure the input power by optical power meter. Check if the input power is within the range between the minimum receiver sensitivity power and the overload power.
2. If the input power is within the range, clean the Rx connector on the OC-n line card, re-connect the Rx fiber. If the alarm remains active, replace the line card.
3. If the input power is too low, disconnect the Tx fiber at the remote end. Measure the output power by the optical power meter at the remote end. Check if the output power is not lower than the minimum transmitter power specified for the relevant OC-n interface.
4. If the output power is too low, replace the line card at the remote end.
5. If the output power is not too low. Repair or replace the fiber from the remote end to the near end.

LOT (OC3 Loss of Transmitter)

This condition is reported by the OAU equipment to indicate that traffic is not being sent.

Probable Cause

- The optical transmitter is not sending a signal.

Problem Resolution Procedure

- The card has failed. Replace the defective card. Refer to "Replacing OSIRIS Plug-in Units" on page 116.

LPBKFAC (Facility Loopback)

A LPBKFAC condition is reported when a loop back operation has been initiated.

A loopback facility loops the signal back towards the SONET facility for that OC-n channel. A loopback is an out of service maintenance action.

Probable Cause

- This is a status message.

Problem Resolution Procedure

- No action is required.

LPBKTERM (Terminal Loopback)

A LPBKTERM condition is reported when a loop back operation has been initiated.

A loopback terminal loops the signal back towards the network for that OC-n channel. A loopback is an out of service maintenance action.

Probable Cause

- This is a status message

Problem Resolution Procedure

- No action is required.

MANSWCMPL (Manual Switch Complete)

A manual switch request has been successfully operated.

The traffic has been moved onto the switch request targeted line. The targeted line is carrying the traffic.

Probable Cause

This is a status message

Problem Resolution Procedure

No action is required.

MANSWREQ (Line Manual Switch Active)

A line manual switch request is active on the targeted line. The targeted line can either be the protection or the working line.

Probable Cause

This is a status message.

Problem Resolution Procedure

No action required.

OOF (OCn Out of Frame)

Four consecutive incorrect framing patterns have been received in 3 consecutive seconds.

Probable Cause

- This alarm may be caused by an intermittent defect on an optical interface.
- Framing errors are being detected on the incoming signal.

Problem Resolution Procedure

- Verify the receive power on the OAU. This alarm can be reported if receive power is too high.
- Make sure that OAU types are correct. If this is an OC-3 system, make sure that no OC-12 OAUs are in use, and vice-versa.
- An OAU may be defective. Check the first OAU upstream for hardware failure and replace if necessary.
- The upstream network element may have lost clock synchronization. Re-establish upstream network element synchronization. This might require replacing a failed OAU. Refer to "Replacing OSIRIS Plug-in Units" on page 116.
- Verify that one of the network elements in the ring is provisioned as the master clock (local or external clock). An LOF can occur if no master clock is defined.

PLM-P (STS Path Signal Label Mismatch)

A received payload label is considered mismatched if it does not equal either the label value corresponding to the locally provisioned PTE functionality or the label value corresponding to the equipped, non-specific code.

Probable Cause

- Local and destination equipment has been configured with a different STSMAP parameter.

Problem Resolution Procedure

- The circuit is provisioned to receive a signal from incompatible mapping type. Locate the incompatible mapped Path Terminating Equipment.

RFI-L (Remote Failure Indication – Line)

An RFI-L failure is reported when a Remote Defect Indication (RDI-L) condition persists for a period of time.

The RDI-L signal (formerly called Line FERF) indicates to the LTE that its peer LTE has detected an AIS-L (or a lower layer) defect on the signal that the first LTE originated.

Probable Cause

- The peer LTE has detected an AIS-L, LOS or LOF defect.

Problem Resolution Procedure

- Make sure that the BIU is seated in the shelf
- Ensure that the OAUs are seated in the shelf.
- Investigate for a fiber cut.

- The transmitter may be defective. Verify output power according to specifications.
- If the output power meets requirements, then a problem exists at the fibre-level.

RLOC (OC3 RX Loss of Clock)

This condition is reported by the mapper equipment to indicate that its recovered clock circuitry is not detecting a reference signal.

Probable Cause

- The recovered clock, derived from the local line, unit part of the equipment has failed.

Problem Resolution Procedure

- Ensure that no LOS is detected on the local line. A LOS may cause the detection of a Rx Loss of Clock failure, but do not imply defective equipment.
- If a LOS is not detected simultaneously, the working mapper is probably defective, replace it. Refer to "Replacing OSIRIS Plug-in Units" on page 116.

SD-L (OCn Line Signal Degrade)

An SD is declared when transmission degradations have reached the Signal Degrade Threshold of $1x10^{-6}$.

Probable Causes

- Degradation of the optical fibre
- Increasing coupling attenuation
- Failure on the far-end transmitter
- Internal equipment failure

Problem Resolution Procedure

- Investigate for a bent fibre.
- Clean the fibre patch cords with alcohol and lint-free tissue.
- The signal can degrade when pig tails are dirty.
- Use a light meter to measure incoming optic levels at inputs.
- If input levels are below normal, then either the distance between nodes is too great for this type of equipment, or the optical transmitter is slowly degrading.
- Check for an equipment failure. Replace a defective equipment. Refer to "Replacing OSIRIS Plug-in Units" on page 116.
- Check for loose connections at the fibre patch panel.

SYCKUNLCK (System Clock Not Locked Alarm)

A System Clock Not Locked Alarm is a clocking difference between the Local OAU and the OAU from the preceding Node.

Probable Cause

- Bad Local OAU or from preceding Node.

Problem Resolution Procedure

- The card has failed. Replace the defective OAU card. Refer to "Replacing OSIRIS Plug-in Units" on page 116.

SYCKFAIL (System Clock Fail Alarm)

A System Clock Fail Alarm is detected when the Oscillator on the Local OAU is defective.

Probable Cause

- Bad Local OAU.

Problem Resolution Procedure

- The card has failed. Replace the defective OAU card. Refer to "Replacing OSIRIS Plug-in Units" on page 116.

TLOS (OAU TX Loss of Signal)

This condition is reported by the OAU equipment to indicate that the laser output level is too low.

Probable Cause

- The optical transmitter is not sending a signal.

Problem Resolution Procedure

- The card has failed. Replace the defective card. Refer to "Replacing OSIRIS Plug-in Units" on page 116.

UNEQ-P (STS Path Unequipped)

A received signal label is considered Unequipped if it is equal to an all-zeros value.

For Virtual Tributary path connections that are not equipped or equipped but not provisioned, the NE will generate all-zeros STS SPEs with "valid" Payload Pointers.

Probable Cause

- The STS cross-connection is not provisioned on a remote equipment.

Problem Resolution Procedure

- The circuit is provisioned to receive a signal from an inactive STS. Locate the inactive STS.

EC-n Condition Types

This section contains all EC1 condition types.

ACLKFAIL (EC1 A Clock Fail)

The clock source from the specified OAU, that is, A and/or B is inactive.

Probable Causes

- The OAU A is absent
- The OAU A is defective
- An EC1 mapper is defective

Problem Resolution Procedure

- Make sure that the OAU A is present. A removed OAU may cause the detection of a clock source to fail, but do not imply a defective equipment.
- Check for an OAU failure and replace it if necessary. Refer to "Replacing OSIRIS Plug-in Units" on page 116.
- Check for a mapper failure and replace it if necessary. Refer to "Replacing OSIRIS Plug-in Units" on page 116.

AIS-L (Alarm Indication Signal Detected – Line)

An AIS-L condition is reported when an AIS-L defect persists for a period of time.

An STE (and physical layer regenerators) sends an AIS-L to alert the downstream LTE that a defect has been detected on the incoming SONET section, or that the LTE supporting the provisioned line origination functions has failed.

Probable Causes

- Terminal loopback is active at the remote end i.e. some NE is generating an AIS-L on an OC-n loopback.
- The NE is receiving an AIS-L from a remote equipment, such as a regenerator, due to a failure detected upstream from that equipment.
- The remote equipment is defective

Problem Resolution Procedure

- Check if EC-1 Terminal loopback is active at the remote end. If the loopback is active, release the loopback.
- Verify if the remote equipment is experiencing any line failures such as LOS or LOF. If it is the case, clear the failure.

BCLKFAIL (EC1 B Clock Fail)

The clock source from the specified OAU, that is, A and/or B is inactive.

Probable Causes

- The OAU B is absent
- The OAU B is defective
- An EC1 mapper is defective

Problem Resolution Procedure

- Make sure that the OAU B is present. A removed OAU may cause the detection of a clock source to fail, but do not imply a defective equipment.
- Check for an OAU failure and replace it if necessary. Refer to "Replacing OSIRIS Plug-in Units" on page 116.
- Check for a mapper failure and replace it if necessary. Refer to "Replacing OSIRIS Plug-in Units" on page 116.

FACLPBK (Facility Loopback)

A LPBKFACILITY condition is reported when a loop back operation has been initiated.

A loopback facility loops the signal back towards the SONET facility for that EC-n channel. A loopback is an out of service maintenance action.

Probable Cause

- This is a status message

Problem Resolution Procedure

- No action is required.

LCLKFAIL (EC1 Local Clock Fail)

This condition is reported to indicate that the recovered clock, derived from the local line, unit part of the equipment has failed.

Probable Cause

- The recovered clock, derived from the local line, unit part of the equipment has failed.

Problem Resolution Procedure

- Ensure that no LOS is detected on the local line. A LOS may cause the detection of a local line clock failure, but do not imply defective equipment.
- If a LOS is not detected simultaneously, the working mapper is probably defective, replace it if necessary. Refer to "Replacing OSIRIS Plug-in Units" on page 116.

LOF (Loss of Frame)

An LOF condition is reported when a Severely Error Frame (SEF) defect persists for a period of time.

A SEF defect is detected when the incoming signal has a minimum of four consecutive frames with framing error.

Probable Causes

- Incompatible signal type
- Failure on the far-end transmitter
- Internal equipment failure

Problem Resolution Procedure

- Verify that the received signal is an EC-1 signal and that its power level is within the specification.
- Verify that the cable length and the provisioned cable length are matching.
- Switch traffic to the protection EC-1 card. If this solves the problem, replace the working EC-1 card.

LOS (Loss of Signal)

An LOS condition is reported when an "all-zeros pattern" persists for a period of time.

An "all-zeros pattern" corresponds to no voltage transitions for EC-n electrical interfaces.

Probable Causes

- The cable or connector is excessively degraded

- Failure on the far-end transmitter
- Internal equipment failure
- Cable cut

Problem Resolution Procedure

- Make sure that the coax cables & connectors are good and properly connected.
- Make sure that the remote equipment is functioning properly (power on, card in, etc.).

  Note: The following procedure may affect traffic.
- If possible, switch EC-1 traffic to protection mapper. If problem clears, replace working EC1 mapper. You can do this for near-end and far-end equipment.

OOF (EC1 Out of Frame)

Four consecutive incorrect framing patterns have been received in 3 consecutive seconds.

Probable Cause

- This alarm may be caused by an intermittent defect on an electrical interface.
- Framing errors are being detected on the incoming signal.
- Failure on the far-end transmitter
- Internal equipment failure

Problem Resolution Procedure

- Verify that the received signal is an EC-1 signal and that its power level is within the specification.
- Verify that the cable length and the provisioned cable length are matching.
- Switch traffic to the protection EC-1 card. If this solves the problem, replace the working EC-1 card.

OUTDIS (Output Disabled)

This condition is reported to indicate that the OMODE parameter for that channel as been provisioned to generate AIS on its interface. The user has intentionally disabled the channel output. Channel interface output may be disabled when bandwidth reuse cross-connections are set up. This would prevent traffic miss-connections. Output should be set back to normal once bandwidth reuse cross-connects are complete.

Probable Cause

- This is a status message.

Problem Resolution Procedure

- No action is required.

PLM-P (STS Path Signal Label Mismatch)

A received payload label is considered mismatched if it does not equal either the label value corresponding to the locally provisioned PTE functionality or the label value corresponding to the equipped, non-specific code.

Probable Cause

- Local and destination equipment has been configured with a different STSMAP parameter.

Problem Resolution Procedure

- The circuit is provisioned to receive a signal from incompatible mapping type. Locate the incompatible mapped Path Terminating Equipment.

RFI-L (Remote Failure Indication – Line)

An RFI-L failure is reported when a Remote Defect Indication (RDI-L) condition persists for a period of time.

The RDI-L signal (formerly called Line FERF) indicates to the LTE that its peer LTE has detected an AIS-L (or a lower layer) defect on the signal that the first LTE originated.

Probable Cause

- The peer LTE has detected an AIS-L, LOS or LOF defect.

Problem Resolution Procedure

- Since the RDI-L is a maintenance signal generated to the upstream equipment when a failure such as AIS-L, LOS or LOF defect as been detected, correct the source of the problem at the far end.

RLOC (EC1 RX Loss of Clock)

This condition is reported by the mapper equipment to indicate that its recovered clock circuitry is not detecting a reference signal.

Probable Cause

The recovered clock, derived from the local line, unit part of the equipment has failed.

Problem Resolution Procedure

Ensure that no LOS is detected on the local line. A LOS may cause the detection of a Rx Loss of Clock failure, but do not imply defective equipment.

If a LOS is not detected simultaneously, the working mapper is probably defective, replace it if necessary. Refer to “Replacing OSIRIS Plug-in Units” on page 116.

SD-L (EC1 Line Signal Degrade)

An SD is declared when transmission degradations have reached the Signal Degrade Threshold of $1x10^{-6}$.

Probable Causes

- Distance between equipment do not meet specification.
- Degradation of the electrical medium.
- Failure on the far-end transmitter.
- Internal equipment failure.

Problem Resolution Procedure

- Increase the transmitter output level (often refer to line build out (LBO) or line length) at the far end equipment.

- Investigate for a bent cable.
- Check for loose connections at the fibre patch panel.
- Check for an equipment failure. Replace defective equipment. Refer to "Replacing OSIRIS Plug-in Units" on page 116.

TERMLPBK (Terminal Loopback)

A LPBKTERM condition is reported when a loop back operation has been initiated.

A loopback terminal loops the signal back towards the network for that EC-n channel. A loopback is an out of service maintenance action.

Probable Cause

- This is a status message

Problem Resolution Procedure

- No action is required.

UNEQ-P (STS Path Unequipped)

A received signal label is considered Unequipped if it is equal to an all-zeros value.

For Virtual Tributary path connections that are not equipped or equipped but not provisioned, the NE will generate all-zeros STS SPEs with "valid" Payload Pointers.

Probable Cause

- The STS cross-connection is not provisioned on a remote equipment.

Problem Resolution Procedure

- The circuit is provisioned to receive a signal from an inactive STS. Locate the inactive STS.

STSn Condition Types

This section contains all STS1 and STS3c condition types.

AIS-P (Alarm Indication Signal Detected – Path)

An LTE sends an AIS-P to alert the downstream STS PTE that it has detected a defect on its incoming line signal, or that STS PTE supporting provisioned path origination functions have failed.

Probable Causes

- The NE is receiving AIS-P from the remote NE or OC-n LOS, LOF, and AIS-L.
- An AIS-L defect (or a lower-layer, traffic related, near end defect i.e. LOS or LOF) is present.
- A remote STS not provisioned.

Problem Resolution Procedure

- Look for the presence of an LOS, LOF, AIS-L, LOP-P along the path and correct the situation.
- Verify that the remote end STS is provisioned and cross-connected.

AUTOSWCMPL (Auto Switch Complete)

A signal failure or a signal degraded detected on the working path has caused an automatic path protection switch. The protection path carries the traffic. This message is applicable to a revertive system.

Probable Causes

- This is a status message.

Problem Resolution Procedure

- No action required.

AUTOSWPNDG (Auto Switch Pending)

A signal failure or a signal degraded has been detected on the working path and a signal failure was already detected on the alternate path, or a signal degraded has been detected on the working path and a signal degraded was already detected on the alternate path.

See the Protection switch section for signal failure and signal degrades detection criteria.

Probable Cause

- This is a status message.

Problem Resolution Procedure

- No action required.

AUTOSWWTR (Auto Switch Wait to Restore)

A Wait-to-Restore period is defined for the Path Terminating Equipment (PTE) using revertive switching to prevent frequent automatically initiated switches that would occur as the result of an intermittent failure or degradation on the working path.

This request is issued when working channels meet the restoral threshold after a Signal Degrade or Signal Failure condition that caused the path switch.

Probable Cause

- This is a status message.

Problem Resolution Procedure

- No action required.

B2HE3 (Excessive Bit Error Rate $\geq 10^{-3}$)

An B2HE3 is declared when transmission degradations have reached 1 bit in error per 1000 bit received.

Probable Cause

- Excessive degradation of the optical fiber
- Coupling attenuation
- Failure on the far-end transmitter
- Equipment internal failure

Problem Resolution Procedure

- Locate the path that is raising the alarm. To do so:

    - Verify whether any alarms are present at the upstream node.
    - If no alarms are present, keep checking upstream until the node is located.
- Clean the fibre patch cords with alcohol and lint-free tissue.
- A high bit error rate can be caused by dirty pig tails.
- Use a light meter to measure incoming optic levels at OAU inputs. Refer to the *OSIRIS® XTD Shelf Installation Guide (203-003)* for input levels.
- If input levels are below normal, then either the distance between nodes is too great for this type of OAU, or the OAU transmitter has degraded.
- Check for loose connections at the fibre patch panel or on the OAU itself.
- Check for an OAU failure. Replace a defective OAU. Refer to "Replacing OSIRIS Plug-in Units" on page 116.
- Verify that one of the network elements in the ring is provisioned as the master clock (local or external clock).
- Check for a defective mapper at the far end node. Remove and replace a defective mapper. Refer to "Replacing OSIRIS Plug-in Units" on page 116.

B2HE4 (Excessive Bit Error Rate ≥ 10^{-4})

An B2HE4 is declared when transmission degradations have reached 1 bit in error per 10000 bit received.

Probable Cause

- Excessive degradation of the optical fiber
- Coupling attenuation
- Failure on the far-end transmitter
- Equipment internal failure

Problem Resolution Procedure

- Locate the path that is raising the alarm. To do so:
    - Verify whether any alarms are present at the upstream node.
    - If no alarms are present, keep checking upstream until the node is located.
- Clean the fibre patch cords with alcohol and lint-free tissue.
- A high bit error rate can be caused by dirty pig tails.
- Use a light meter to measure incoming optic levels at OAU inputs. Refer to the *OSIRIS® XTD Shelf Installation Guide (203-003)* for input levels.
- If input levels are below normal, then either the distance between nodes is too great for this type of OAU, or the OAU transmitter has degraded.
- Check for loose connections at the fibre patch panel or on the OAU itself.
- Check for an OAU failure. Replace a defective OAU. Refer to "Replacing OSIRIS Plug-in Units" on page 116.
- Verify that one of the network elements in the ring is provisioned as the master clock (local or external clock).
- Check for a defective mapper at the far end node. Remove and replace a defective mapper. Refer to "Replacing OSIRIS Plug-in Units" on page 116.

FRCDSWCMPL (Forced Switch Complete)

A forced switch operation has been initiated.

For non-revertive system, the traffic has been forced onto the switch request targeted entity. The targeted entity is carrying the traffic.

For revertive system, the traffic has been forced onto the protection entity. The protection entity is carrying the traffic.

Probable Cause

- This is a status message.

Problem Resolution Procedure

- No action is required.

FRCDSWREQ (Path Force Switch Active)

A STS path force switch request has been initiated.

Probable Cause

- This is a status message.

Problem Resolution Procedure

- No action required.

FRCDWKSWBK (Forced Working Switch Back)

A forced switch operation has been initiated.

For non-revertive systems, the traffic has been forced onto the switch request targeted entity. The targeted entity is carrying the traffic.

Probable Cause

- This is a status message.

Problem Resolution Procedure

- No action is required.

FRCDWKSWPR (Forced Working Switch to Protection)

A forced switch operation has been initiated.

For non-revertive systems, the traffic has been forced onto the switch request targeted entity. The targeted entity is carrying the traffic.

For revertive systems, the traffic has been forced onto the protection entity. The protection entity is carrying the traffic.

Probable Cause

- This is a status message.

Problem Resolution Procedure

- No action is required.

LCKOUTCMPL (Lockout Complete)

A lockout switch request has been initiated on the protection path.

Probable Cause

- This is a status message.

Problem Resolution Procedure

- No action is required.

LCKOUTREQ (Path Lockout Active)

A STS path lockout request has been initiated.

Probable Cause

- This is a status message.

Problem Resolution Procedure

- No action required.

LOCKOUTOFPR (Lockout of Protection)

A lockout switch request has been initiated on the protection path.

Probable Cause

- This is a status message.

Problem Resolution Procedure

- No action is required.

LOP (Loss of Pointer)

A LOP is a failure related to the pointer processing mechanism.

Several definitions of "valid pointer" are possible. An LOP is not expected to be a common defect in the network.

Probable Causes

The transmitter of the far-end equipment is configured for a different payload rate (STS-1 or STS-nc).

A consequence of a far-end equipment transmitter's failure or equipment internal failure.

Near-end equipment receiver failure or equipment internal failure.

Problem Resolution Procedure

1. Switch the traffic to the protection if possible.
2. Verify and make sure that the transmitter of the far-end equipment is configured to the same payload rate as expected for this node. (STS-1 or STS-nc).
3. If the condition is still active, replace the line card at the near end.
4. If the condition is still active, the original line card is not at fault at the near end, re-install the original line card.
5. Replace the line card at the remote end.

LOS (STS Path Loss of Signal)

The STS path Loss of signal condition is reported to indicate that the received signal level incoming from the backplane is too low..

Probable Causes

- The associated OAU is removed
- The associated OAU is defective

Problem Resolution Procedure

- If the condition is reported when the associated OAU card is absent or unseated, the condition will be masked and should be considered as a status message only.
- If the condition is reported when the associated OAU card is present, the OAU card may be defective. Replace the associated defective equipment. Refer to "Replacing OSIRIS Plug-in Units" on page 116.

MANSWREQ (Path Manual Switch Active)

A STS path manual switch request has been initiated.

Probable Cause

- This is a status message

Problem Resolution Procedure

- No action required.

MANSWCMPL (Manual Switch Complete)

The operator has initiated a manual switch to protection, and the switch has been successfully completed.

Probable Cause

- This is a status message.

Problem Resolution Procedure

- No action is required.

MANWKSWPR (Manual Working Switch to Protection)

The operator has initiated a manual switch to protection, and the switch has been successfully completed.

Probable Cause

- This is a status message.

Problem Resolution Procedure

- No action is required.

OUTDIS (Output Disabled)

This condition is reported to indicate that the OMODE parameter for that channel as been provisioned to generate AIS on its interface. The user has intentionally disabled the channel output. Channel interface output may be disabled when bandwidth reuse cross-connections are set up. This would prevent traffic miss-connections. Output should be set back to normal once bandwidth reuse cross-connects are complete.

Probable Cause

- This is a status message.

Problem Resolution Procedure

- No action is required.

PLM-P (STS Path Signal Label Mismatch)

A received payload label is considered mismatched if it does not equal either the label value corresponding to the locally provisioned PTE functionality or the label value corresponding to the equipped, non-specific code.

Probable Cause

- The STS bandwidth has different setting around the ring.
- Local and destination equipment has been configured with a different STSMAP parameter.

Problem Resolution Procedure

- Check software settings for STS bandwidth assignments.
- The circuit is provisioned to receive a signal from incompatible mapping type. Locate the incompatible mapped Path Terminating Equipment.

RFI-P (Remote Failure Indication – STS)

A RFI-P failure is derived from a persistent Remote Defect Indication (RDI) defect.

An RDI-P signal indicates to an STS PTE that its peer STS PTE has detected a defect on the signal that originated from the first STS PTE.

Probable Cause

- The far-end equipment has detected an AIS-P, LOP-P or an UNEQ-P.

Problem Resolution Procedure

- Since the RDI-P is a maintenance signal generated to the upstream equipment when a failure such as AIS-P, UNEQ-P, LOP-P, PLM-P defect as been detected, correct the source of the problem at the far end.

SD-P (STS Path Signal Degrade)

An SD is declared when transmission degradations have reached the provisioned Signal Degrade Threshold.

Probable Causes

- Degradation of the optical fibre upstream
- Increasing coupling attenuation of the optical fibre upstream
- Failure on the far-end transmitter
- Internal equipment failure

Problem Resolution Procedure

- Check for an equipment failure. Replace defective equipment. Refer to “Replacing OSIRIS Plug-in Units” on page 116.
- Investigate for a bent fibre upstream. Clean the fibre patch cords with alcohol and lint-free tissue. The signal can degrade when pig tails are dirty.
- Use a light meter to measure incoming optic levels at inputs.

- If input levels are below normal, then either the distance between nodes is too great for this type of equipment, or the optical transmitter is slowly degrading.
- Check for loose connections at the fibre patch panel.

STSINTFLT (STS Path Internal Fault)

The STS Path Internal Fault condition is reported to indicate that the received signal level incoming from the backplane is too low..

Probable Causes

- The associated OAU is removed
- The associated OAU is defective

Problem Resolution Procedure

- If the condition is reported when the associated OAU card is absent or unseated, the condition will be masked and should be considered as a status message only.
- If the condition is reported when the associated OAU card is present, the OAU card may be defective. Replace the associated defective equipment. Refer to "Replacing OSIRIS Plug-in Units" on page 116.

STSnUNEQ (STS-n Path Unequipped - where n=1 to 48)

A received signal label is considered unequipped if it is equal to an all-zeros value.

For Virtual Tributary path connections that are not equipped or equipped but not provisioned, the NE will generate all-zeros STS SPEs with "valid" Payload Pointers.

Probable Cause

- The OAU bandwidth for that STS is deleted or unassigned elsewhere in the ring.
- The STS cross-connection is not provisioned on a remote equipment.

Problem Resolution Procedure

- Check software settings for STS bandwidth assignments.
- The circuit is provisioned to receive a signal from an inactive STS. Locate the inactive STS.

UNEQ-P (STS Path Unequipped)

A received signal label is considered Unequipped if it is equal to an all-zeros value.

For Virtual Tributary path connections that are not equipped or equipped but not provisioned, the NE will generate all-zeros STS SPEs with "valid" Payload Pointers.

Probable Cause

- The OAU bandwidth for that STS is deleted or unassigned elsewhere in the ring.
- The STS cross-connection is not provisioned on a remote equipment.

Problem Resolution Procedure

- Check software settings for STS bandwidth assignments.
- The circuit is provisioned to receive a signal from an inactive STS. Locate the inactive STS.

WKSWPR (Working Switch to Protection)

A signal failure or a signal degraded detected on the working path has caused an automatic path protection switch. The protection path carries the traffic. This message is applicable to a revertive system.

Probable Causes

- This is a status message.

Problem Resolution Procedure

- No action required.

WTR (Wait to Restore)

A Wait-to-Restore period is defined for the Path Terminating Equipment (PTE) using revertive switching to prevent frequent automatically initiated switches that would occur as the result of an intermittent failure or degradation on the working path.

This request is issued when working channels meet the restoral threshold after a Signal Degrade or Signal Failure condition that caused the path switch.

Probable Cause

- This is a status message.

Problem Resolution Procedure

- No action required.

VT Condition Types

This section contains all VT condition types.

AIS-V (Alarm Indication Signal - Virtual Tributary)

An AIS-V is a maintenance signal used in the digital network to alert downstream equipment that a defect or equipment failure has been detected.

Probable Causes

- One of these is present:
- An AIS-P, UNEQ-P, PLM-P, or LOP-P defect
- A lower-layer traffic related defect
- A near-end defect

Problem Resolution Procedure

- Look for the presence of a LOS, LOF, AIS-L, LOP-P, UNEQ-P, PLM-P along the path and correct the situation
- Verify that the remote end VT is provisioned.

AUTOSWCMPL (Auto Switch Complete)

A signal failure or a degraded signal detected on the working path has caused an automatic path protection switch. The protection path carries the traffic. This message is applicable to revertive systems.

Probable Causes

- This is a status message.

Problem Resolution Procedure

- No action required.

AUTOSWPNDG (Auto Switch Pending)

A signal failure or a signal degraded has been detected on the working path and a signal failure was already detected on the alternate path, or

A signal degraded has been detected on the working path and a signal degraded was already detected on the alternate path.

See the Protection switch section for signal failure and signal degrades detection criteria.

Probable Cause

- This is a status message.

Problem Resolution Procedure

- No action required.

AUTOSWWTR (Auto Wait to Restore)

An Automatic Wait-to-Restore (AUTOSWWTR) period is defined for the Path Terminating Equipment (PTE) using revertive switching to prevent frequent automatically initiated switches that would occur as the result of an intermittent failure or degradation on the working path.

This request is issued when working channels meet the restoral threshold after a Signal Degrade or Signal Failure condition that caused the path switch.

Probable Cause

This is a status message.

Problem Resolution Procedure

No action required.

B2HE3 (Excessive Bit Error Rate $\geq 10^{-3}$)

An B2HE3 is declared when transmission degradations have reached 1 bit in error per 1000 bits received.

Probable Cause

- Excessive degradation of the optical fiber
- Coupling attenuation
- Failure on the far-end transmitter
- Equipment internal failure

Problem Resolution Procedure

- Locate the path that is raising the alarm. To do so:
- Verify whether any alarms are present at the upstream node.
- If no alarms are present, keep checking upstream until the node is located.

- Clean the fibre patch cords with alcohol and lint-free tissue.
- A high bit error rate can be caused by dirty pig tails.
- Use a light meter to measure incoming optic levels at OAU inputs. Refer to the *OSIRIS® XTD Shelf Installation Guide (203-003)* for input levels.
- If input levels are below normal, then either the distance between nodes is too great for this type of OAU, or the OAU transmitter has degraded.
- Check for loose connections at the fibre patch panel or on the OAU itself.
- Check for an OAU failure. Replace a defective OAU. Refer to "Replacing OSIRIS Plug-in Units" on page 116.
- Verify that one of the network elements in the ring is provisioned as the master clock (local or external clock).
- Check for a defective mapper at the far end node. Remove and replace a defective mapper. Refer to "Replacing OSIRIS Plug-in Units" on page 116.

B2HE4 (Excessive Bit Error Rate ≥ 10^{-4})

An B2HE4 is declared when transmission degradations have reached 1 bit in error per 10000 bit received.

Probable Cause

- Excessive degradation of the optical fiber
- Coupling attenuation
- Failure on the far-end transmitter
- Equipment internal failure

Problem Resolution Procedure

- Locate the path that is raising the alarm. To do so:
- Verify whether any alarms are present at the upstream node.
- If no alarms are present, keep checking upstream until the node is located.
- Clean the fibre patch cords with alcohol and lint-free tissue.
- A high bit error rate can be caused by dirty pig tails.
- Use a light meter to measure incoming optic levels at OAU inputs. Refer to the *OSIRIS® XTD Shelf Installation Guide (203-003)* for input levels.
- If input levels are below normal, then either the distance between nodes is too great for this type of OAU, or the OAU transmitter has degraded.
- Check for loose connections at the fibre patch panel or on the OAU itself.
- Check for an OAU failure. Replace a defective OAU. Refer to the Equipment Replacement Procedure section.
- Verify that one of the network elements in the ring is provisioned as the master clock (local or external clock).
- Check for a defective mapper at the far end node. Remove and replace a defective mapper. Refer to "Replacing OSIRIS Plug-in Units" on page 116.

FRCDSWCMPL (Forced Switch Complete)

A forced switch operation has been initiated.

For non-revertive systems, the traffic has been forced onto the switch request targeted entity. The targeted entity is carrying the traffic.

For revertive systems, the traffic has been forced onto the protection entity. The protection entity is carrying the traffic.

Probable Cause

- This is a status message.

Problem Resolution Procedure

- No action is required.

FRCDSWREQ (Path Force Switch Active)

A VT path force switch request has been initiated.

Probable Cause

This is a status message.

Problem Resolution Procedure

No action required.

FRCDWKSWBK (Forced Working Switch Back)

A forced switch operation has been initiated.

For non-revertive systems, the traffic has been forced onto the switch request targeted entity. The targeted entity is carrying the traffic.

Probable Cause

- This is a status message.

Problem Resolution Procedure

- No action is required.

FRCDWKSWPR (Forced Working Switch to Protection)

A forced switch operation has been initiated.

For non-revertive systems, the traffic has been forced onto the switch request targeted entity. The targeted entity is carrying the traffic.

For revertive systems, the traffic has been forced onto the protection entity. The protection entity is carrying the traffic.

Probable Cause

- This is a status message.

Problem Resolution Procedure

- No action is required.

LCKOUTCMPL (Lockout Complete)

A lockout switch request has been initiated on the protection path.

Probable Cause

- This is a status message.

Problem Resolution Procedure

- No action is required.

LCKOUTREQ (Path Lockout Active)

A VT path lockout request has been initiated.

Probable Cause

- This is a status message

Problem Resolution Procedure

- No action required

LOCKOUTOFPR (Lockout of Protection)

A lockout switch request has been initiated on the protection path.

Probable Cause

- This is a status message.

Problem Resolution Procedure

- No action is required.

LOS (VT Path Loss of Signal)

The VT path Loss of signal condition is reported to indicate that the received signal level incoming from the backplane is too low.

Probable Causes

- The associated OAU is removed
- The associated OAU is defective

Problem Resolution Procedure

- If the condition is reported when the associated OAU card is absent or unseated, the condition will be masked and should be considered as a status message only.
- If the condition is reported when the associated OAU card is present, the OAU card may be defective. Replace the associated defective equipment. Refer to "Replacing OSIRIS Plug-in Units" on page 116.

MANSWCMPL (Manual Switch Complete)

The operator has initiated a manual switch to protection, and the switch has been successfully completed.

Probable Cause

- This is a status message.

Problem Resolution Procedure

- No action is required.

MANWKSWPR (Manual Working Switch to Protection)

The operator has initiated a manual switch to protection, and the switch has been successfully completed.

Probable Cause

- This is a status message.

Problem Resolution Procedure

- No action is required.

PLM-V (VT Path Signal Label Mismatch)

A received payload label is considered mismatched if it does not equal either the label value corresponding to the locally provisioned PTE functionality or the label value corresponding to the equipped, non-specific code.

Probable Cause

- Local and destination equipment has been configured with a different STSMAP parameter.

Problem Resolution Procedure

The circuit is provisioned to receive a signal from incompatible mapping type. Locate the incompatible mapped Path Terminating Equipment.

RFI-V (Remote Failure Indication – VT)

An RFI-V failure is derived from a persistent Remote Defect Indication (RDI) defect.

An RDI-V signal is used in all VT-based applications to indicate to a VT PTE that its peer VT PTE has detected a defect on the signal that first VT PTE originated.

Probable Cause

- The far end equipment has detected an AIS-V, a LOP-V or an UNEQ-V defect.

Problem Resolution Procedure

- Since the RDI-V is a maintenance signal generated to the upstream equipment when a failure such as AIS-V, UNEQ-V, LOP-V, PLM-V defect as been detected, correct the source of the problem at the far end.

SD-V (VT Path Signal Degrade)

An SD is declared when transmission degradations have reached the provisioned Signal Degrade Threshold.

Probable Causes

- Degradation of the optical fibre upstream
- Increasing coupling attenuation of the optical fibre upstream
- Failure on the far-end transmitter
- Internal equipment failure

Problem Resolution Procedure

- Check for an equipment failure. Replace defective equipment. Refer to the Equipment Replacement Procedure section.

- Investigate for a bent fibre upstream. Clean the fibre patch cords with alcohol and lint-free tissue. The signal can degrade when pig tails are dirty.
- Use a light meter to measure incoming optic levels at inputs.
- If input levels are below normal, then either the distance between nodes is too great for this type of equipment, or the optical transmitter is slowly degrading.
- Check for loose connections at the fibre patch panel.

UNEQ-V (VT Path Unequipped)

A received signal label is considered Unequipped if it is equal to an all-zeros value.

For Virtual Tributary path connections that are not equipped or equipped but not provisioned, the NE will generate all-zeros VT SPEs with "valid" Payload Pointers.

Probable Cause

- The VT cross-connection is not provisioned on a remote equipment.

Problem Resolution Procedure

- The cross-connection is provisioned to receive a signal from an inactive STS. Locate the inactive STS.

VTINTFLT (VT Path Internal Fault)

The VT Path Internal Fault condition is reported to indicate that the received signal level incoming from the backplane is too low.

Probable Causes

- The associated OAU is removed
- The associated OAU is defective

Problem Resolution Procedure

- If the condition is reported when the associated OAU card is absent or unseated, the condition will be masked and should be considered as a status message only.
- If the condition is reported when the associated OAU card is present, the OAU card may be defective. Replace the associated defective equipment. Refer to "Replacing OSIRIS Plug-in Units" on page 116.

WKSWPR (Working Switch to Protection)

A signal failure or a degraded signal detected on the working path has caused an automatic path protection switch. The protection path carries the traffic. This message is applicable to revertive system.

Probable Causes

- This is a status message.

Problem Resolution Procedure

- No action required.

WTR (Wait to Restore)

A Wait-to-Restore (WTR) period is defined for the Path Terminating Equipment (PTE) using revertive switching to prevent frequent automatically initiated switches that would occur as the result of an intermittent failure or degradation on the working path.

This request is issued when working channels meet the restoral threshold after a Signal Degrade or Signal Failure condition that caused the path switch.

Probable Cause

This is a status message.

Problem Resolution Procedure

No action required.

DS3 Condition Types

This section contains all T3 condition types.

AIS (Alarm Indication Signal)

An AIS is a maintenance signal used in the digital network to alert downstream equipment that a defect or equipment failure has been detected.

Probable Causes

- The NE is receiving an AIS from the remote DS3 equipment.

Problem Resolution Procedure

- Verify DS3 path from end to end including all higher-layer traffic (STS path, line, or section layer) in order to locate the higher order problem and correct the situation.
- Verify that the cross-connection as been established from source to destination.

BPV (Bipolar Violation)

This condition is reported to indicate that an excessive bipolar violation rate has been detected on the channel interface. A BPV occurs when the alternate polarity rule for binary "ones" is violated.

Probable Cause

- Persistent errors have been detected within the electrical signal.
- The electrical encoding scheme might not match the signal.

Problem Resolution Procedure

- Check cabling and connections between the termination panel and the equipment. The tip or ring on the input cable may be open
- Ensure that the distance between the nodes does not exceed the supported line length.
- Verify the line length channel parameter.
- Use a test set to verify incoming signal parameters on the channel that is displaying the alarm.
- Check the line coding. The only supported line code is B3ZS.

FACLPBK (Facility loopback)

A LPBKFACILITY condition is reported when a loop back operation has been initiated.

A loopback facility loops the signal back towards the DS3 physical interface. A loopback is an out of service maintenance action.

Probable Cause

- This is a status message.

Problem Resolution Procedure

- No action is required.

LOO (Loss of Output)

This condition is reported by mapper equipment to indicate that the electrical signal output level is below normal operation.

Probable Cause

- The DS3 channel is not transmitting a signal on its interfaces.

Problem Resolution Procedure

- Check cables. The output cable must be attached to the output connector.
- Verify patch cord or cross-connections. Make sure that *in* and *out* signals are connected correctly.
- The mapper is defective. Replace the mapper.

LOS (Loss of Physical-layer Signal)

An LOS is detected when no pulse of either positive or negative polarity is detected on the incoming signal for a specified number of bit periods that persist for a period of time.

Probable Causes

- Cable cut
- DS3 cable or connector degrade
- DS3 Tributary Interface Unit internal failure
- Failure on the remote DS3 transmitter

Problem Resolution Procedure

- Verify that the remote end transmitter is operational. In order to do that, monitor the transmitted signal if possible and if not, switch traffic to the protection mapper.
- Verify that the cable is connected properly and not damaged by monitoring the signal at the very end of the cable.
- Switch local mapper to the protection unit and verify if the problem is solved. If this solves the problem, replace the working unit.

OUTDIS (Output Disabled)

This condition is reported to indicate that the OMODE parameter for that channel as been provisioned to generate AIS on its interface. The user has intentionally disabled the channel output. Channel interface output may be disabled when bandwidth reuse cross-connections are set up. This would prevent traffic miss-connections. Output should be set back to normal once bandwidth reuse cross-connects are complete.

Probable Cause

- This is a status message.

Problem Resolution Procedure

- No action is required.

RAI (T3 Remote Alarm Indication)

LOF or AIS failures result in the transmission of a continuous RAI signal in the reverse direction.

Detecting an RAI indicates that an LOF or AIS failure has been declared at the remote DS3 Path Termination Equipment (PTE).

Probable Cause

- The remote equipment has detected an LOF or AIS failure.

Problem Resolution Procedure

- Verify that the far-end terminal is receiving a valid signal.
- Verify all external devices for functionality and connectivity.

SD (T3 Line Signal Degrade)

An SD is declared when transmission degradations have reached the Signal Degrade Threshold of $1x10^{-6}$.

Probable Causes

- Distance between equipment do not meet specification
- Degradation of the electrical medium.
- Failure on the far-end transmitter
- Internal equipment failure

Problem Resolution Procedure

- Increase the transmitter output level (often refer to line build out (LBO) or line length) at the far end equipment
- Check for a defective cable.
- Check for loose connections at the fibre patch panel.
- Check for an equipment failure. Replace defective equipment. Refer to the “Replacing OSIRIS Plug-in Units” on page 116.

TERMLPBK (Terminal Loopback)

A LPBKTERM condition is reported when a loop back operation has been initiated.

A loopback terminal loops the signal back towards the network for that DS3 channel. A loopback is an out of service maintenance action.

Probable Cause

- This is a status message.

Problem Resolution Procedure

- No action is required.

DS1 Condition Types

This section contains all T1 condition types.

AIS (Alarm Indication Signal)

An AIS is a maintenance signal used in the digital network to alert downstream equipment that a defect or equipment failure has been detected.

Probable Causes

- The NE is receiving an AIS from the remote DS1 equipment.

Problem Resolution Procedure

- Verify DS1 path from end to end including all higher-layer traffic (STS path, line, or section layer) in order to locate the higher order problem and correct the situation.
- Verify that the cross-connection as been established from source to destination.

BPV (Bipolar Violation)

This condition is reported to indicate that an excessive bipolar violation rate has been detected on the channel interface. A BPV occurs when the alternate polarity rule for binary "ones" is violated.

Probable Cause

- Persistent errors have been detected within the electrical signal.
- The electrical encoding scheme might not match the signal.

Problem Resolution Procedure

- Check cabling and connections between the termination panel and the equipment. The tip or ring on the input cable may be open
- Check the line coding software configuration on the mapper that is reporting the alarm. For example, an AMI/B8ZS mismatch may exist between the software configuration and the physical line.
- Ensure that the distance between the nodes does not exceed the supported line length.
- Verify the line length channel parameter.
- Use a test set to verify incoming signal parameters on the channel that is displaying the alarm.

FACLPBK (Facility Loopback)

A LPBKFACILITY condition is reported when a loop back operation has been initiated.

A loopback facility loops the signal back towards the DS1 physical interface. A loopback is an out of service maintenance action.

Probable Cause

- This is a status message.

Problem Resolution Procedure

- No action is required.

FACAULPBK (Facility Automatic Loopback)

A facility loopback has been automatically initiated in response to a loop code being detected incoming from the channel interface. This feature is available on DS1PMP mapper.

Probable Cause

- This is a status message.

Problem Resolution Procedure

- No action is required.

FMTMISMAT (Format Mismatch)

This condition is reported to indicate that the slot equipage does not match the provisioned equipment type. DS1 frame format monitoring is not supported on that equipment. This condition has been replaced by the FEATMISM condition.

Probable Cause

- The DS1 card is not provisioned correctly.
- The wrong type of equipment is physically present in the shelf

Problem Resolution Procedure

- Make sure that a DS1 mapper is not provisioned as a DS1PM.
- Regular DS1 mappers cannot monitor DS1 frames.
- DS1PM mappers can monitor unframed, super frame (SF) and extended super frame (ESF) format. Refer to the table below to match mapper product codes with supported frame formats.

	Product Code	Supported Frame Formats monitoring
DS1	800320/4	Unframed
	800320/4A	Unframed
	800320/4B	Unframed
	800320/7	Unframed
	800320/7A	Unframed
DS1PM	800324	Unframed, SF, and ESF
	800327	Unframed, SF, and ESF

LCRCD (Loop Code Received)

The DS1PM+ mapper is receiving a Loop Up or a Loop Down code. A Loop Up Code Received may trigger a loopback to be automatically activated. A Loop Down code may terminate an automatically activated loopback. See also FACAULPBK and TERMAULPBK.

Probable Cause

- This is a status message.

Problem Resolution Procedure

- No action is required.

LOF (Loss of Frame)

An LOF is declared when an Out Of Frame (OOF) defect persists for a pre-determined period of time. An OOF defect is the occurrence of a particular density of a framing error.

Probable Causes

- Local and destination equipment has been configured with a different frame format.
- DS1 cable or connector degraded.
- DS1 Tributary Interface Unit internal failure.
- Failure on the remote DS1 transmitter has occurred.

Problem Resolution Procedure

- Verify that the incoming signal's frame format is matching the provisioned frame format.
- Verify that the remote end transmitter is operational. In order to do that, monitor the transmitted signal if possible and if not, switch traffic to the protection mapper.
- Verify that the cable is connected properly and not damaged by monitoring the signal at the very end of the cable.
- Switch the local mapper to the protection unit and verify if the problem is solved. If this solves the problem, replace the working unit.

LOO (Loss of Output)

This condition is reported by mapper equipment to indicate that the electrical signal output level of at least one channel interface is below normal operation.

Probable Cause

- The DS1 channel is not transmitting a signal on its interfaces.

Problem Resolution Procedure

- Check cables. The output cable must be attached to the output connector.
- Verify patch cord or cross-connections. Make sure that *in* and *out* signals are connected correctly.
- The mapper is defective. Replace the mapper.

LOS (Loss of Physical-layer Signal)

An LOS is detected when no pulse of either positive or negative polarity is detected on the incoming signal for a specified number of bit periods that persists for a period of time.

Probable Causes

- Cable cut.
- DS1 cable or connector degrade.
- DS1 Tributary Interface Unit internal failure.
- Failure on the remote DS1 transmitter has occurred.

Problem Resolution Procedure

- Verify that the remote end transmitter is operational. In order to do that, monitor the transmitted signal if possible and if not, switch traffic to the protection mapper
- Verify that the cable is connected properly and not damaged by monitoring the signal at the very end of the cable.
- Switch local mapper to the protection unit and verify if the problem is solved. If this solves the problem, replace the working unit.

OUTDIS (Output Disabled)

This condition is reported to indicate that the OMODE parameter for that channel as been provisioned to generate AIS on its interface. The user has intentionally disabled the channel output. Channel interface output may be disabled when bandwidth reuse cross-connections are set up. This would prevent traffic miss-connections. Output should be set back to normal once bandwidth reuse cross-connects are complete.

Probable Cause

- This is a status message.

Problem Resolution Procedure

- No action is required.

RAI (T1 Remote Alarm Indication)

LOF or AIS failures result in the transmission of a continuous RAI signal in the reverse direction.

Detecting an RAI indicates that an LOF or AIS failure has been declared at the remote DS1 Path Termination Equipment (PTE).

Probable Cause

- The remote equipment has detected an LOF or AIS failure.

Problem Resolution Procedure

- Verify that the far-end terminal is receiving a valid signal.
- Verify all external devices for functionality and connectivity.

SD (T1 Line Signal Degrade)

An SD is declared when transmission degradations have reached the Signal Degrade Threshold of $1x10^{-6}$.

Probable Causes

- Distance between equipment do not meet specification
- Degradation of the electrical medium
- Failure on the far-end transmitter
- Internal equipment failure

Problem Resolution Procedure

- Increase the transmitter output level (often refer to line build out (LBO) or line length) at the far end equipment

- Investigate for a bent cable.
- Check for loose connections at the fibre patch panel.
- Check for an equipment failure. Replace defective equipment. Refer to the Equipment Replacement Procedure section.

TERMAULPBK (Terminal Automatic Loopback)

A terminal loopback has been automatically initiated in response to a loop code being detected incoming from the network. This feature is available on DS1PMP mapper.

Probable Cause

- This is a status message.

Problem Resolution Procedure

- No action is required.

TERMLPBK (Terminal Loopback)

A LPBKTERM condition is reported when a loop back operation has been initiated.

A loopback terminal loops the signal back towards the network for that DS1 channel. A loopback is an out of service maintenance action.

Probable Cause

- This is a status message.

Problem Resolution Procedure

- No action is required.

TOW (T1 Traffic Overwritten)

The DS1PM+ mapper has the ability to send test signal. This condition is reported to indicate that the test signal is overwriting regular traffic.

Probable Cause

- This is a status message

Problem Resolution Procedure

- No action is required.

Security Condition Types

This section contains all security condition types.

INTRUSION (Illegal Login Attempt)

This condition is reported to indicate that a user has attempted to log on multiple times unsuccessfully.

Probable Cause

- Four unsuccessful attempts have been made to log on to the network from one of the nodes. This message is visible to all open sessions except the one from which the invalid login attempt occurred.

Problem Resolution Procedure

- Wait at least 2 minutes then perform the correct log on sequence. Use the same connection type that was used in your previous attempt.

Ethernet Condition Types

This section contains all ethernet condition types.

LNKDWN (Link Down)

The Ethernet Link Down condition is reported when the Ethernet Physical layer (Physical Coding Sublayer or PCS) has loss its Synchronization and/or there is an auto-negotiation failure.

Probable Cause

- Ethernet cable has been removed or damaged/cut.
- The Line rate parameter provisioned on the Ethernet port does not match with the one configured on the remote equipment
- Ethernet-far-end equipment fault (card removed, power failure, etc.…)
- Failure of the auto-negotiation process:
  - Ethernet-far-end port has its auto-negotiation process disabled;
  - Incompatible fixed and advertised parameters between both Ethernet ports;
  - Both Ethernet ports cannot agree on a common set of parameters;
  - Incompatible auto-negotiation protocol between the near-end Ethernet PHY and the far-end Ethernet PHY.

Problem Resolution Procedure

- Use a test set to check the signal input at the patch panel monitor jack. If a signal is present, go to the next step.
- If a signal is not present, the outside link is down.
- Check cabling and connections between the external device and the equipment.
- Make sure that the external device is connected to the right jack on the Fast Ethernet mapper. The top jack is MDI, and the bottom jack is MDI-X. Refer to the *OSIRIS® XTD Shelf Installation Guide (203-003)*.

PROVMISMAT (Provisioning Mismatch)

The Provisioning Mismatch condition is reported when provisioning parameters between two Fast Ethernet facilities are different. This condition applies to Fast Ethernet mapper card.

Probable Cause

- There is a misconnection. The two STS-1s assigned to the ethernet ports are cross-connected to the 2 STS-1s assigned to the same ethernet port.
- There is a mismatch in the configuration. One end is provisioned with a single STS and the remote port is configured with a pair of STS-1s.
- The Duplex setting is different between both ends of the circuit.
- The turbo mode has been activated at only one end of the circuit.

Problem Resolution Procedure

Reprovision the circuit so that both ends are using the same mode. Also make sure that Turbo mode is either enabled or disabled for both ends.

PYLDLPD (Ethernet Payload Looped)

The Payload Loopback condition is reported when the Ethernet payload being sent on the transport Network is "looped back" to its source. This condition is applicable to Fast Ethernet mapper card.

Probable Cause

- There is a provisioning misconnection. The first STS-1 is cross-connected to the second one.

Problem Resolution Procedure

- Only one end of the cross-connect is provisioned. You must provision the far-end of the connection.

REVMISM (Software Revision Mismatch)

This condition applies to the Ethernet 10Base-T mapper. The software revision mismatch condition is reported when traffic is carried between different mapper revisions.

Probable Cause

- Incompatibility between different revisions of Ethernet 10Base-T mapper.

Problem Resolution Procedure

- User should not mix 800340/3 with older 800340 or 800340/2.

VCG Condition Types

These conditions applies to the Multi-Service Ethernet mapper.

MBRFAIL (Member Fail)

The Member Fail condition is reported when traffic while using LCAS (Link Capacity Adjustment Scheme) is not being carried on one or more of the provisioned VT/STS1 path between two end points.This condition notifies the operator that the circuit is not carrying the full capacity of the cross-connection.

Probable Cause

- Traffic is not being carried on one or more VT/STS1 path across the Network.

Problem Resolution Procedure

- Verify VT/STS1 path status.
- Verify Member sequence numbering.

MBRUNPROT (Member Unprotect)

The Member Unprotected condition is reported when traffic is not being carried on one or more of the provisioned VT/STS1 on the Protection Path. This condition is not service affecting.

Probable Cause

- Traffic is being carried unprotected on one or more VT/STS1 across the Network.

Problem Resolution Procedure

- Check for an OAU failure at a remote site. Replace a defective OAU. Refer to "Replacing OSIRIS Plug-in Units" on page 116.
- Make sure that correct OAU types are in use.
- If the distance between nodes does not correspond to the receive sensitivity of the OAU, this alarm can be reported.
- Verify that one of the network elements in the ring is provisioned as the master clock (local or external clock). All other network elements must be provisioned as slaves (THRU timing). .

VCGFAIL

The VCG Fail condition is reported when traffic, if LCAS (Link Capacity Adjustment Scheme) not activated, is not being carried end-to-end.This condition is service affecting.

Probable Cause

- Traffic is not being carried on one or more VCAT members across the Network.

Problem Resolution Procedure

- Verify VT/STS1 path status.
- Verify Member sequence numbering.

OSI Association Condition Types

This section contains all OSI Association condition types.

ABRTD (OSI Association Aborted <abort reason>)

An OSI association to a remote network element has terminated unexpectedly. OSI associations are used to route TL1 commands to remote network elements and for software download using FTAM.

Probable Cause

- Problems in the wide-area OSI network. This can include link-downs and network congestion.

Problem Resolution Procedure

- Verify that both the originator and the responder are operational.
- Verify that the OSI stack is provisioned at both ends of the association.
- Verify that the communication link is still operational and not damaged by a higher order problem such as a SONET defect.

File Transfer Access and Management Condition Types

This section contains all FTAM condition types.

FTAMCANCEL (<size>-FTAM Software Download Aborted <filename>)

A user has cancelled an FTAM software download (started with the ACT-SWDL-FTAM TL1 command). <size> is the number of bytes downloaded prior to the download being cancelled. <filename> is the name of the file being downloaded.

Probable Cause

- The CANC-SWDL-FTAM TL1 command was used to cancel an active software download over FTAM. This condition is generated due to a user action. This is a status message.

Problem Resolution Procedure

- No action is required.

FTAMENDERR (FTAM Software Download Terminated Unexpectedly)

A software download from an FTAM server terminated unexpectedly.

Probable Cause

- Problems in the wide-area OSI network, such as link failure and congestion.
- Problems in the FTAM server, such as disk failure or server overload.

Problem Resolution Procedure

- The software download should be repeated once the root cause of the problem has been resolved.
- Contact your Wide Area Network (WAN) Administrator.

FTAMPRGRS (FTAM Software Download Progress: <count> bytes received, <percentage>% done)

This condition reports on the progress of a software download from an FTAM server. When the ACT-SWDL-FTAM TL1 command is used to initiate the activity, a progress reporting interval is specified with the PROGPRD= parameter. Periodically, this condition reports the <count> of byte downloaded, and the <percentage> complete.

Probable Cause

- The TL1 command ACT-FTAM-SWDL was used. This condition is generated due to a user action. This is a status message.

Problem Resolution Procedure

- No action is required.

FTAMSTART (FTAM Software Download Started with File <filename> of Size <filesize>)

This condition reports that a software download from an FTAM server was started. The filename and total file size are given.

Probable Cause

- The TL1 command ACT-FTAM-SWDL was used.

Problem Resolution Procedure

- No action is required.

FTAMSUCCESS (FTAM Software Download Completed Successfully)

This condition reports that a software download from an FTAM server completed successfully.

Probable Cause

- The TL1 command ACT-FTAM-SWDL was used. This condition is generated due to a user action. This is a status message.

Problem Resolution Procedure

- No action is required.

Trivial File Transfer Protocol Condition Types

This section contains all TFTP condition types.

TFTPCANCEL (TFTP Software Download Aborted with File <filename>: <size>)

A user has cancelled an TFTP software download (started with the ACT-SWDL-TFTP TL1 command). <size> is the number of bytes downloaded prior to the download being cancelled. <filename> is the name of the file being downloaded.

Probable Cause

- The CANC-SWDL-TFTP TL1 command was used to cancel an active software download over FTAM. This condition is generated due to a user action. This is a status message.

Problem Resolution Procedure

- No action is required.

TFTPENDERR (TFTP Software Download Terminated Unexpectedly on Node <node ID> Slot <AID>)

A software download from a TFTP server terminated abnormally.

Probable Cause

- Problems in the TCP/IP wide area network, such as link failures or congestion.
- Problems on the TFTP server, such as disk failure or server over-load.

Problem Resolution Procedure

- Contact your Wide Area Network (WAN) Administrator.
- Repeat the software download once the root cause has been resolved.

TFTPPRGRS (TFTP Software Download Progress: <count>

bytes with file <filename>)

This condition reports on the progress of a software download from a TFTP server. When the ACT-SWDL-TFTP TL1 command is used to initiate the activity, a progress reporting interval is specified with the PROGPRD= parameter. Periodically, this condition reports the <count> of bytes downloaded, and the <filename>.

Probable Cause

- The TL1 command ACT-FTAM-SWDL was used. This condition is generated due to a user action. This is a status message.

Problem Resolution Procedure

- No action is required.

TFTPPRGRS (TFTP Software Download Progress for File <filename>: <count> bytes of <size> bytes)

This condition reports on the progress of a software download from a TFTP server. When the ACT-SWDL-TFTP TL1 command is used to initiate the activity, a progress reporting interval is specified with the PROGPRD= parameter. Periodically, this condition reports the <count> of bytes downloaded, and the <filename>.

Probable Cause

- The TL1 command ACT-FTAM-SWDL was used. This condition is generated due to a user action. This is a status message.

Problem Resolution Procedure

- No action is required.

TFTPSTART (TFTP Software Download Started with File <filename>)

This condition reports that a software download from a TFTP server was started. The filename is given.

Probable Cause

- The TL1 command ACT-FTAM-SWDL was used. This condition is generated due to a user action. This is a status message.

Problem Resolution Procedure

- No action is required.

TFTPSTART (TFTP Software Download Started with File <filename> of size <size>)

This condition reports that a software download from a TFTP server was started. The filename and size are given.

Probable Cause

- The TL1 command ACT-FTAM-SWDL was used. This condition is generated due to a user action. This is a status message.

Problem Resolution Procedure

- No action is required.

TFTPSUCCESS (TFTP Software Download Completed Successfully on Node <node ID>)

This condition reports that a software download from an TFTP server completed successfully.

Probable Cause

- The TL1 command ACT-FTAM-SWDL was used. This condition is generated due to a user action. This is a status message.

Problem Resolution Procedure

- No action is required.

System Condition Types

This section contains all system condition types.

POWER (Power Failure Alarm)

A PWR condition is reported when one of the two power inputs to that equipment falls below the acceptable level of operation (The acceptable DC power level for OSIRIS equipment is -19.6 volt).

Probable Causes

- One of the two power inputs to that equipment has fallen below -19.6 volt.

Problem Resolution Procedure

- Verify that both power input feeds are connected properly and that voltage levels are between -20.6 and -60 VDC.
- Check for any blown fuses or a tripped breaker at the power plant.

SHLFALM (Shelf Alarm)

A critical Shelf Alarm is an additional indication that service is affected, and in effect, escalates the alarm level.

Probable Cause

- At least five or more T1s are defective (LOS, AIS, etc.) or at least 1 DS3/STS is affected.

Problem Resolution Procedure

- Clear equipment and line alarms.

Network Element Condition Types

This section contains all network element condition types.

REMOTE (Remote Alarm Report)

This condition is reported to indicate that an alarm, either minor, major or critical, is declared at a remote Network Element.

Probable Cause

- An alarm is active at a remote NE

Problem Resolution Procedure

- Log into the remote NE and follow the appropriate problem resolution procedure in this document.

Data Communication Channel Condition Types

This section contains all DCC condition types.

DCC (SDCC-X Link Failure)

This condition is reported to indicate that the communication between adjacent Network Element is impaired.

Probable Cause

- The line carrying the DCC (Data Communications Channel) has failed.
- The network element cannot communicate through the DCC (Data Communications Channel). DCC-X is transmitted out OAU-A and received in OAU-B.

Problem Resolution Procedure

- If this is a new node, verify that the fibers are terminated correctly. Refer to the *OSIRIS® XTD Shelf Installation Guide (203-003)*.
- Verify that DCC software settings are enabled for all network elements.
- Check whether MCUs are present in all nodes. A DCC failure can be caused by a removed MCU.
- An MCU reset can also trigger this alarm. If this is the case, the alarm will clear within three minutes.
- Check for an OAU failure at a remote site. Replace a defective OAU. Refer to "Replacing OSIRIS Plug-in Units" on page 116.
- Make sure that correct OAU types are in use.
- If the distance between nodes does not correspond to the receive sensitivity of the OAU, this alarm can be reported.
- Verify that one of the network elements in the ring is provisioned as the master clock (local or external clock). All other network elements must be provisioned as slaves (THRU timing).

DCC (SDCC-Y Link Failure)

This condition is reported to indicate that the communication between adjacent Network Element is impaired.

Probable Cause

- The line carrying the DCC (Data Communications Channel) has failed.
- The network element cannot communicate through the DCC (Data Communications Channel). DCC-Y is transmitted out OAU-B and received in OAU-A.

Problem Resolution Procedure

- If this is a new node, verify that the fibers are terminated correctly. Refer to the *OSIRIS® XTD Shelf Installation Guide (203-003)*.
- Verify that DCC software settings are enabled for all network elements.
- Check whether MCUs are present in all nodes. A DCC failure can be caused by a removed MCU.
- An MCU reset can also trigger this alarm. If this is the case, the alarm will clear within three minutes.
- Check for an OAU failure at a remote site. Replace a defective OAU. Refer to "Replacing OSIRIS Plug-in Units" on page 116.
- Make sure that correct OAU types are in use.
- If the distance between nodes does not correspond to the receive sensitivity of the OAU, this alarm can be reported.
- Verify that one of the network elements in the ring is provisioned as the master clock (local or external clock). All other network elements must be provisioned as slaves (THRU timing).

OSILINKERR (W-OAU Link Failure)

This condition is reported to indicate that the communication between adjacent Network Element is impaired.

Probable Cause

- The line carrying the DCC (Data Communications Channel) has failed.
- The network element cannot communicate through the DCC (Data Communications Channel). W-OAU is transmitted out OAU-A and received in OAU-B.

Problem Resolution Procedure

- If this is a new node, verify that the fibers are terminated correctly. Refer to the *OSIRIS® XTD Shelf Installation Guide (203-003)*.
- Verify that DCC software settings are enabled for all network elements.
- Check whether MCUs are present in all nodes. A DCC failure can be caused by a removed MCU.
- An MCU reset can also trigger this alarm. If this is the case, the alarm will clear within three minutes.

- Check for an OAU failure at a remote site. Replace a defective OAU. Refer to "Replacing OSIRIS Plug-in Units" on page 116.
- Make sure that correct OAU types are in use.
- If the distance between nodes does not correspond to the receive sensitivity of the OAU, this alarm can be reported.
- Verify that one of the network elements in the ring is provisioned as the master clock (local or external clock). All other network elements must be provisioned as slaves (THRU timing).

OSILINKERR (E-OAU Link Failure)

This condition is reported to indicate that the communication between adjacent Network Element is impaired.

Probable Cause

- The line carrying the DCC (Data Communications Channel) has failed.
- The network element cannot communicate through the DCC (Data Communications Channel). E-OAU is transmitted out OAU-B and received in OAU-A.

Problem Resolution Procedure

- If this is a new node, verify that the fibers are terminated correctly. Refer to the *OSIRIS® XTD Shelf Installation Guide (203-003)*.
- Verify that DCC software settings are enabled for all network elements.
- Check whether MCUs are present in all nodes. A DCC failure can be caused by a removed MCU.
- An MCU reset can also trigger this alarm. If this is the case, the alarm will clear within three minutes.
- Check for an OAU failure at a remote site. Replace a defective OAU. Refer to "Replacing OSIRIS Plug-in Units" on page 116.
- Make sure that correct OAU types are in use.
- If the distance between nodes does not correspond to the receive sensitivity of the OAU, this alarm can be reported.
- Verify that one of the network elements in the ring is provisioned as the master clock (local or external clock). All other network elements must be provisioned as slaves (THRU timing).

Session Condition Types

This section contains all session condition types.

LOGON (Private System)

This condition is reported to indicate that a user has logged on successfully.

Probable Cause

- This is a status message.

Problem Resolution Procedure

- No action required.

Chapter 4
Network Element Hardware Notification

This chapter describes the problem notification that may be provided by the network elements and how to clear them.

OSIRIS Hardware Notification

The OSIRIS network element provides a variety of indicators to interface with central and remote offices. These indicators are defined below.

The Alarm and Craft Interface Unit (ACIU) provides relay contacts for audible and visual alarms at the central office, and for environmental monitoring and control at remote offices. The front panel contains visual alarm indicators for Critical, Major and Minor alarms, craft ports (Ethernet and serial), and Alarm Cut Off button. Each card on the network element (NE) also has LEDs which provide a visual indication of the card's current state.

To identify the source of any alarm(s), log on to the NE and query the NE alarm database. If you have problems logging on to the NE, refer to "Chapter 2: Communication Problems". All office alarm indicators are triggered by alarms detected by the local NE, except for the **Remote Alarm**, which is only available when the Positron proprietary data communication channel (DCC) is used.

For OSIRIS-VUE user, access the "Active Alarms" application. This application is automatically launched when starting OSIRIS-VUE and can be accessed using the main menu. This application allows filtering on a per Network Element basis.

Refer to "OSIRIS Alarms and Conditions" on page 30 for a definition, probable cause and a problem resolution procedure for each alarm.

LED Interpretation

This section provides a definition for the OSIRIS LEDs located on the faceplate of the Alarm and Craft Interface Unit (ACIU), the Network Management and Control Unit (NMCU), and the traffic carrying equipment.

Alarm and Craft Interface Unit (ACIU)

LED	Color	Attribute	Shelf Behavior
CRITICAL	RED	SOLID	This alarm LED turns on to indicate a critical alarm condition on the shelf. It is controlled by the NMCU.
MAJOR	RED	SOLID	This alarm LED turns on to indicate a major alarm condition on the shelf. It is controlled by the NMCU.
MINOR	AMBER	SOLID	This alarm LED turns on to indicate a minor alarm condition on the shelf. It is controlled by the NMCU.
REMOTE	AMBER	SOLID	This alarm LED turns on to indicate that at least one alarm is declared at a remote Network Element. Available with MARCONI proprietary DCC only.
PWR A	RED	SOLID	This alarm LED turns on to indicate that the power feed A is below 19.5V ± 0.5V. When the voltage reaches 20.5V ± 0.5V, the alarm clears.
PWR B	RED	SOLID	This alarm LED turns on to indicate that the power feed B is below 19.5V ± 0.5V. When the voltage reaches 20.5V ± 0.5V, the alarm clears.
ACTI	AMBER	SOLID	This LED turns on to indicate that the office audible alarm was turned OFF with the Alarm Cut Off (ACO) button. The active alarm condition has not been cleared. This LED will turn OFF once the alarm condition is cleared.
FA ALM	GREEN	SOLID	This LED color indicates that the fuse for the power input A is present and operating normally.
	RED	SOLID	This LED color indicates that the fuse for the power input A is present but is blown and should be replaced.
FB ALM	GREEN	SOLID	This LED color indicates that the fuse for the power input B is present and operating normally.
	RED	SOLID	This LED color indicates that the fuse for the power input B is present but is blown and should be replaced.

Network Management and Control Unit (NMCU)

Color	Attribute	Description
OFF	OFF	No power to equipment
GREEN	SOLID	Normal
	FLASHING	Software download in progress
AMBER	BLINKING	Saving configuration into non-volatile memory
RED	BLINKING	Saving software into non-volatile memory

Service Equipment

Upper LED

Color	Attribute	Description
OFF	OFF	No power to equipment
GREEN	SOLID	Normal/ Ready for provisioning
	FLASHING	Facility alarm condition present on card
RED	SOLID	- Waiting for initialization (at installation only) - Equipment failure

Lower LED (Mappers equipped with CPU only)

Color	Attribute	Description
OFF	OFF	No power to equipment
GREEN	SOLID	Normal
	FLASHING	Software download in progress
RED	BLINKING	Saving software into non-volatile memory

Auxiliary 2 Card

Color	Attribute	Description
OFF	OFF	No power
Red(2 sec.)	SOLID	Initialization
Green	SOLID	Normal
Green	FLASHING	Alarm condition
Red	SOLID	Failure

Alarm Port

The Alarm port is a connector that provides access to the alarm relay contacts of the shelf. These relay contacts are used to activate the alarm reporting system of the office. Both normally open and normally closed alarm systems are supported. Two types of office alarm indications are provided: visual and audible. Each group has three levels of alarm indications: critical, major, and minor.

A power loss alarm indication is also available on the Alarm port. Office alarm indicators are triggered by alarms detected by the local Network Element.

Note: An OSIRIS network operating with the Positron proprietary data communication channel (DCC) protocol can report remote alarms via the audible minor relay contact.

Alarm Cut Off

The ACO push button lets you terminate an audible office alarm indication as an acknowledgement of the reported alarm. When this button is pushed, the relay contacts for the audible office alarm are disabled and the ACO LED is turned ON. The ACO LED remains ON and the relay contacts for the office audible alarm remain disabled until a new alarm is detected.

If a new alarm is detected, the relay contacts for the office audible alarm are re-enabled as an indication of a new event, and the ACO LED turns OFF to indicate that the ACO has become inactive. The ACO can be pressed again as an acknowledgement for the new alarm(s). If the alarm condition is cleared, the ACO LED turns OFF and the relay contacts for the audible office alarm remain disabled.

Environmental I/O

Environmental monitoring and control of the remote office is available via a connector which provides four relay outputs for auxiliary controls and eleven inputs for dry-contact sensing interfaces. These sensors collect external equipment alarm and status information.

All eleven inputs are monitored individually and autonomously report changes in their status. Automatic messages may be sent autonomously. The environmental input condition can be queried in the NE alarm database and will operate the appropriate office alarm relay contacts.

Chapter 5
Protection Switching

This chapter describes the different Protection Schemes supported by OSIRIS.

OSIRIS Protection Schemes

This section describes the following protection schemes which are used for OSIRIS.

- Unidirectional Protection Switched Ring (UPSR)
- Equipment 1:N Protection Switching
- Synchronization Reference Protection Switching

Unidirectional Protection Switched Ring (UPSR)

Path protection is provided through a selector function implemented in the receive direction. This selector operates at the appropriate payload rate supported by the mapper, namely, VT1.5, STS1 and STS3c. A bridge of the signal can be achieved through cross-connect type in order to provide a copy of the signal onto the alternate path in the transmit direction. The mapper card is responsible for the path protection functions.

The path protection scheme can operate in one of two modes, revertive or non-revertive. A wait to restore period can be set in revertive mode to prevent frequent oscillation of the path selector. Also, a holdoff timer, present on DS1 mapper card, can be set when the path protection scheme operates behind a line protection scheme.

Path selector operation can be initiated automatically or manually. Signal failure or degradation may cause the path selector to operate automatically while three basic operations can be initiated manually by the user. These operations are “manual” and “force” switching, and path “lockout”.

Refer to “Hierarchy of STS Path Protection Switching Requests” and “Hierarchy of VT Path Protection Switching Requests” on page 101, for the hierarchy of automatic and manual switch requests. Refer to “UPSR Standing Conditions” on page 101 for a definition. See below for the list of automatically and manually initiated switch requests as well as state requests relevant to Path protection modes of operation.

Manually Initiated Switch Requests (revertive mode)

- Lockout of protection
- Force switch out of working
- Manual switch out of working

Manually Initiated Switch Requests (non-revertive mode)

- Force switch onto working or protection
- Manual switch onto working or protection

Automatically Initiated Switch Requests

- Automatic switch out of working or protection due to signal failure
- Automatic switch out of working or protection due to signal degraded

State Requests

- Wait to restore state (revertive mode only)

Most manually initiated switch requests can be operated on either the protected or the protecting path, but cannot be initiated on both the protected and the protecting path simultaneously.

The user is provided with full control of the selector via the "force" and the "lockout" switch requests. Initiating a "lockout" can increase a "forced" switch request priority, or force the selector to switch paths even when a forced switch request is active. These types of switches may be used for traffic restoration and upgrades. A "manual" switch request may be used for trouble isolation. "Manual" switch requests are preempted by automatic switch request due to signal failure or degradation.

Hierarchy of STS Path Protection Switching Requests

Protection Switching Request	Priority	Standing Condition	Request Type
Release Protection Switch	Highest	---	User Request
Operate Lockout of Protection	|	LCKOUTREQ	User Request
Operate Forced Switch to Working / Operate Forced Switch to Protection	|	FRCDSWREQ	User Request
Signal Fail Switch to Working / Signal Fail Switch to Protection (AIS-P, LOP-P, or UNEQ-P)	|	---	Automatic Request
Signal Fail Switch to Working / Signal Fail Switch to Protection (1.0E-3/4 Excessive STS Path BER)	|	---	Automatic Request
Signal Degrade Switch to Working / Signal Degrade Switch to Protection (1.0E-5/6/7/8/9 Excessive STS Path BER)	|	---	Automatic Request
Operate Manual Switch to Working / Operate Manual Switch to Protection	|	MANSWREQ	User Request
Wait-To-Restore	|	WTR	State Request
No Request	Lowest	---	State Request

Hierarchy of VT Path Protection Switching Requests

Protection Switching Request	Priority	Standing Condition	Request Type
Release Protection Switch	Highest	---	User Request
Operate Lockout of Protection	|	LCKOUTREQ	User Request
Operate Forced Switch to Working / Operate Forced Switch to Protection	|	FRCDSWREQ	User Request
Signal Fail Switch to Working / Signal Fail Switch to Protection (AIS-V, LOP-V, or UNEQ-V)	|	---	Automatic Request
Signal Fail Switch to Working / Signal Fail Switch to Protection (1.0E-3/4 Excessive VT Path BER)	|	---	Automatic Request
Signal Degrade Switch to Working / Signal Degrade Switch to Protection (1.0E-5/6/7/8/9 Excessive VT Path BER)	|	---	Automatic Request
Operate Manual Switch to Working / Operate Manual Switch to Protection	|	MANSWREQ	User Request
Wait-To-Restore	|	WTR	State Request
No Request	Lowest	---	State Request

UPSR Standing Conditions

The following standing conditions apply to the UPSR protection scheme on OSIRIS.

- **AUTOSWCMPL** (Auto Switch Complete): This condition is reported to indicate that an automatic switch request has been performed.
- **AUTOSWPNDG** (Auto Switch Pending): This condition is reported to indicate that an automatic switch request has been prevented.

- **AUTOSWWTR** (Auto Wait To Restore): The traffic of the working mapper that was automatically switched to the protection mapper has now been restored. The system waits five minutes before switching back. This message is displayed during the waiting period.
- **FRCDSWCMPL** (Forced Switch Complete): This condition is reported to indicate that a force switch request has been performed.
- **FRCDSWREQ** (EQPT Force Switch Request): An equipment force switch request has been initiated.
- **LCKOUTCMPL** (Lockout Complete): A lockout switch request has been initiated on the protection equipment.
- **LCKOUTREQ** (EQPT Lockout Protection Request): An equipment lockout request has been initiated on the protection equipment.
- **LCKOUTREQ** (EQPT Lockout Working Request): An equipment lockout request has been initiated on the working equipment.
- **MANSWCMPL** (Manual Switch Complete): The operator has initiated a manual switch to protection, and the switch has been successfully completed.
- **MANSWREQ** (EQPT Manual Switch Request): An equipment manual switch request has been initiated

Equipment 1:N Protection Switching

Equipment providing electrical interface ports may operate in a 1:n protection scheme. Each DS1 equipment protection group requires a Protection Switch Control Unit (PSCU) or an Alarm and Craft Interface Unit (ACIU) for Micro-shelves for proper operation. The PSCU or ACIU switches all the T1 electrical interfaces from the working to the protection equipment and vice versa. Other types of interface cards such as DS3 and EC1 do not require a PSCU or ACIU for protection switching.

Equipment protection is performed for the entire equipment functionality, particularly, interface port setting and channel monitoring. Equipment protection switch events may cause a traffic hit.

Equipment protection operation can be initiated either automatically or manually. Equipment failure or card removal are criteria for automatic switch request while three basic operations can be initiated manually by the user. These operations are “manual” and “force” switching for working equipment, and “lockout” for the protection equipment.

Refer to “Hierarchy of Equipment 1:n Protection Switching Requests” on page 103 for the hierarchy of automatic and manual switch requests and to “Equipment 1:n Standing Conditions” on page 103 for a definition. See below for the list of automatically and manually initiated switch requests as well as state requests relevant to equipment protection operation.

Manually Initiated Switch Requests

- Lockout of protection
- Force switch out of working
- Manual switch out of working

Automatically Initiated Switch Requests

- Automatic switch out of working

- Automatic switch out of protection

State Requests

- Wait to restore state

Manually initiated equipment protection switch operations are persistent, that is, the switch requests, once performed, cause a standing condition. Equipment protection switch requests of higher priority prevents equipment protection switch requests of equal or lower priority. Equipment protection switch requests of higher priority preempt equipment protection switch requests of lower priority.

The user is provided with full control of the traffic carrying equipment via the "force" and "lockout" switch requests. These types of switches may be used for equipment replacement and upgrades. Note that a "force" switch request to absent protection equipment will remain pending until protection equipment is in position. A "manual" switch request may be used for trouble isolation. "Manual" switch requests are preempted by automatic switch requests due to equipment failure or card removal.

Hierarchy of Equipment 1:n Protection Switching Requests

Protection Switching Request	Priority	Standing Condition	Request Type
Release user switch request	Highest	---	User Request
Operate Lockout of Protection (Working and Protection mappers)	|	LCKOUTREQ	User Request
Automatic Switch out of Protection (Protection Card Remove)	|	---	Automatic Request
Operate Forced Switch to Protection mapper 1	|	FRCDSWREQ	User Request
Operate Forced Switch to Protection mappers 2 to 13	|	FRCDSWREQ	User Request
Operate Forced Switch to Protection mapper 14	|	FRCDSWREQ	User Request
Automatic Switch to Protection mapper 1 (Card Failure, Card Remove)	|	AUTOSWCOMPL	Automatic Request
Automatic Switch to Protection mappers 2 to 13 (Card Failure, Card Remove)	|	AUTOSWCOMPL	Automatic Request
Automatic Switch to Protection mapper 14 (Card Failure, Card Remove)	|	AUTOSWCOMPL	Automatic Request
Manual Switch to Protection	|	MANSWREQ	User Request
No Request	Lowest		State Request

Equipment 1:n Standing Conditions

The following standing conditions apply to the Equipment 1:n Protection Switching protection scheme on OSIRIS.

- **AUTOSWCMPL** (Auto Switch Complete): This condition is reported to indicate that an automatic switch request has been performed.
- **AUTOSWPNDG** (Auto Switch Pending): This condition is reported to indicate that an automatic switch request has been prevented.

- **AUTOSWWTR** (Auto Wait To Restore): The traffic of the working mapper that was automatically switched to the protection mapper has now been restored. The system waits five minutes before switching back. This message is displayed during the waiting period.
- **FRCDSWCMPL** (Forced Switch Complete): This condition is reported to indicate that a force switch request has been performed.
- **FRSWPNDG** (Forced Switch Pending): This condition is reported to indicate that an automatic switch request has been prevented.
- **FRCDSWREQ** (EQPT Force Switch Request): An equipment force switch request has been initiated.
- **LCKOUTCMPL** (Lockout Complete): A lockout switch request has been initiated on the protection equipment.
- **LCKOUTREQ** (EQPT Lockout Protection Request): An equipment lockout request has been initiated on the protection equipment.
- **LCKOUTREQ** (EQPT Lockout Working Request): An equipment lockout request has been initiated on the working equipment.
- **MANSWCMPL** (Manual Switch Complete): The operator has initiated a manual switch to protection, and the switch has been successfully completed.
- **MANSWREQ** (EQPT Manual Switch Request): An equipment manual switch request has been initiated

Synchronization Reference Protection Switching

Two synchronization references are available for externally timed and line timed network element. These synchronization references are referred to the primary and secondary references. The OSIRIS network element can derive synchronization from most mapper interface cards as well as from the OAU interfaces.

When deriving synchronization from the OAU interfaces, OSIRIS acts as a line-timed network element and detects and acts upon received synchronization status messages (SSM). When deriving synchronization from the mapper interface cards, OSIRIS act as an externally-timed network element. SSM messaging is not supported on mapper interface cards.

The OSIRIS network element does not provide manually initiated operations for selecting the synchronization reference (that is primary and secondary) for protection switching. Synchronization reference protection switching operates in non-revertive mode only.

Hierarchy of Synchronization Protection Switching Requests

Protection Switching Request	Priority	Transient Condition	Request Type
Automatic Synchronization Reference Switch to primary / secondary (LOS, LOF, AIS)	Highest	LINE / PRIEXT / SECEXT	Automatic Request
Automatic Synchronization Reference Switch (Do NOT use for Synchronization quality level) (OAU line interface only)	|	LINE	Automatic Request
Automatic Synchronization Reference Switch (Stratum 4 Traceable quality level) (OAU line interface only)	|	LINE	Automatic Request
Automatic Synchronization Reference Switch (SONET Minimum Clock Traceable quality level) (OAU line interface only)	|	LINE	Automatic Request

Protection Switching Request	Priority	Transient Condition	Request Type
Automatic Synchronization Reference Switch (Stratum 3 Traceable quality level) (OAU line interface only)	|	LINE	Automatic Request
Automatic Synchronization Reference Switch (Stratum 3E Traceable quality level) (OAU line interface only)	|	LINE	Automatic Request
Automatic Synchronization Reference Switch (Transit Node Clock Traceable quality level) (OAU line interface only)	|	LINE	Automatic Request
Automatic Synchronization Reference Switch (Stratum 2 Traceable quality level) (OAU line interface only)	|	LINE	Automatic Request
Automatic Synchronization Reference Switch (Synchronized - Traceability Unknown quality level) (OAU line interface only)	|	LINE	Automatic Request
Automatic Synchronization Reference Switch (Stratum 1 Traceable quality level) (OAU line interface only)	Lowest	LINE	Automatic Request

Synchronization Reference Standing Conditions

The following standing conditions apply to the Synchronization Reference Protection Switching protection scheme on OSIRIS.

- **LINE** (OAU RX Line Clock Inactive): This condition is reported to indicate that the OAU, configured for through timing, has lost its synchronization reference. Its synchronization reference is the optical signal received on its interface.
- **PRIEXT** (OAU Primary External Clock Inactive): This condition is reported to indicate that the OAU, configured for external timing, has lost its synchronization reference. Its synchronization reference is the interface configured as primary reference.
- **SECEXT** (OAU Secondary External Clock Inactive): This condition is reported to indicate that the OAU, configured for external timing, has lost its synchronization reference. Its synchronization reference is the interface configured as secondary reference.
- **SL-MLINE** (Select Mate Line): The OAU has switched to an alternate clock reference. The OAU has Selected the Mate Rx Line Clock.
- **SL-MLOCAL** (Select Mate Local Oscillator) The OAU has switched to an alternate clock reference. The OAU has Selected the Mate Local Oscillator.
- **SL-LINE** (Select Line): The OAU has switched to an alternate clock reference. The OAU has Selected the Rx Line Clock.
- **SL-LOCAL** (Select Local Oscillator): The OAU has switched to an alternate clock reference. The OAU has Selected the Local Oscillator.
- **SL-PRIEXT** (Select Primary External Reference): The OAU has switched to an alternate clock reference. The OAU has Selected the Primary External Clock.
- **SL-SECEXT** (Select Secondary External Reference): The OAU has switched to an alternate clock reference. The OAU has Selected the Secondary External Clock.
- **SYNCSTATCHNG** (Synchronization Status Change): Indicates a change in the incoming synchronization status message that is part of the Extended Superframe Format (ESF). Synchronization status messages are bit-oriented message in the ESF data link of DS1 signals. These messages contain clock quality labels that allow a SONET network element to select the most suitable synchronization reference from the set of available references.

Chapter 6
Performance Monitoring

This chapter describes the different statistics that are used to monitor the performance of the network. Monitoring these statistics can help you detect potential problems before alarm conditions occur.

About Performance Monitoring

Performance monitoring (PM) statistics allow you to monitor the performance of your network. Check PM statistics regularly to diagnose problem areas before alarm conditions occur. If any of the PM statistics start to increase quickly, it is likely that an equipment problem will soon occur.

Performance Monitoring Statistics

There are PM statistics available for the SONET and DSn layers, protection switch event and equipment failure on any node in the network. This section lists and describes the PM statistics that are available.

Equipment PM

Near End Equipment PM

PM Statistic	Definition
PSC	For a working line, the PSC (protection switch count) parameter is a count of the number of times that service has been switched from the monitored equipment to the protection equipment, plus the number of times it has been switched back to the working line. For a protection line, it is a count of the number of times that service has been switched from any working equipment to the protection equipment, plus the number of times service has been switched back to a working equipment. The PSC parameter is only applicable if line level protection switching is used.
PSD	For a working line, the PSD (protection switch duration) parameter is a count of the seconds that service was being carried on the protection equipment. For the protection equipment, it is a count of the seconds that the line was being used to carry service. The PSD parameter is only applicable if revertive line level protection switching is used.
FC	The near end FC (failure count) counts the number of times the equipment failed

T3 Line PM

Near End T3 Line Layer PM

PM Statistic	Definition
CV-L	The near end CV-L (code violation line) parameter is a count of both BPVs and EXZs occurring over the accumulation period. An EXZ will increment the CV Line count by one regardless of the length of the zero string. BPVs that are part of the zero substitution code are excluded.
ES-L	The ES-L (errored seconds line) parameter is a count of seconds containing one or more BPVs, one or more EXZs or one or more LOS defects. BPVs that are part of the zero substitution are excluded.
SES-L	The near end SES-L parameter is a count of seconds during which BPVs plus EXZs exceed 44, or one or more LOS defects occur. BPVs that are a part of the zero substitution code are excluded.
LOSS-L	The near end LOSS-L is a count of one-second intervals containing one or more LOS defects.

T3 Path PM

Near End T3 Path Layer PM

PM Statistic	Definition
CVP-P	The near end CVP-P parameter is a count of P-bit parity errors occurring in the accumulation period.
CVCP-P	The near end CVCP-P parameter is a count of CP-bit parity errors occurring in the accumulation period.
ESP-P	The near end ESP-P parameter is a count of seconds containing one or more P-bit parity errors, one or more SEF defects, or one or more AIS defects.
ESCP-P	The ESCP-P parameter is a count of seconds containing one or more CP-bit parity errors, one or more SEF defects, or one or more AIS defects. ESCP-P is defined for the C-bit parity application.
SESP-P	The near end SESP-P parameter is a count of seconds containing more than 44 P-bit parity violations, one or more SEF defects, or one or more AIS defects.
SESCP-P	The near end SESCP-P parameter is a count of seconds containing more than 44 CP-bit parity errors, one or more SEF defects, or one or more AIS defects.
SAS-P	The near end SASP-P parameter is a count of one-second intervals containing one or more SEFs, or one or more AIS defects on the path.
AISS-P	The near end AISS-P parameter is a count of one-second intervals containing one or more AIS defects.
UASP-P	The near end UASP-P parameter is a count of one-second intervals when the T3 path is unavailable. A T3 path becomes unavailable when 10 consecutive SESP-Ps occur. The ten SESP-Ps are included in unavailable time. Once unavailable, the T3 path becomes available when ten consecutive seconds with no SESP-Ps occur. The ten seconds with no SESP-Ps are excluded from unavailable time.
UASCP-P	The near end UASCP-P parameter is a count of one-second intervals when the T3 path is unavailable. A T3 path becomes unavailable when 10 consecutive SESCP-Ps occur. The ten SESCP-Ps are included in unavailable time. Once unavailable, the T3 path becomes available when ten consecutive seconds with no SESCP-Ps occur. The ten seconds with no SESCP-Ps are excluded from unavailable time.
FC-P	The near end FC-P parameter is a count of the number of occurrences of near end path failure events. The failure event begins when either an LOF or an AIS failure is declared. The failure event ends when the LOS or AIS are clear.

OC / EC Section PM

Near End OC/EC Section Layer PM

PM Statistic	Definition
SEFS	The SEFS-S parameter is a count of the seconds when a SEF defect was present. A SEF defect is expected during most seconds where a LOS or loss of frame (LOF) defect is present. However, there may be situations when that is not the case, and the SEFS-S parameter is only incremented based on the presence of the SEF defect.

OC / EC Line PM

Near End Line Layer PM

PM Statistic	Definition
CV-L	The near end CV-L parameter is a count of BIP errors detected at the Line layer (i.e., using the B2 bytes in the incoming SONET signal). Up to 8XN BIP errors can be detected per STS-N frame, with each error incrementing the CV-L current second register.
ES-L	The ES-L parameter is a count of the seconds during which (at any point during the second) at least one Line layer BIP error was detected or an AIS-L defect (or a lower-layer, traffic-related, near end defect) was present.
SES-L	The near end SES-L parameter is a count of the seconds during which K or more Line layer BIP errors were detected or an AIS-L (see GR-253 for values) was present.
UAS-L	The near end UAS-L parameter is a count of the seconds during which the Line was considered unavailable. A Line becomes unavailable at the onset of 10 consecutive seconds that qualify as SES-Ls, and continues to be unavailable until the onset of 10 consecutive seconds that do not qualify as SES-Ls.
FC-L	The near end FC-L parameter is a count of the number of near end line failure events. A failure event begins when the AIS-L failure is declared, and ends when the failure is cleared. A failure event that begins in one period and ends in another period is counted only in the period in which it begins. Note that functionally, an AIS-L failure will be declared either by receiving (and timing) an AIS-L signal from another NE, or by receiving (and timing) an internally generated AIS-L signal from STE in the same NE where the LTE resides.

T1 Line PM

Near End T1 Line Layer PM

PM Statistic	Definition
CV-L	The near end CV-L (code violation line) parameter is a count of both BPVs (bipolar violation) and EXZs (excessive zeros) occurring over the accumulation period. An EXZ shall increment the CV-L by 1 regardless of the length of zero string. For a B8Zs-coded signal, BVPs that are part of the zero substitution code are excluded
ES-L	The near end ES-L (errored second line) parameter is a count of 1 second interval containing one or more BPVs (bipolar violation), or one or more EXZs (excessive zeros), or one or more LOS (Loss of signal) defects. For a B8Zs-coded signal, BVPs that are part of the zero substitution code are excluded
SES-L	The near end SES-L (Severely errored seconds line) parameter is a count of 1 second interval with 1544 or more BPVs (bipolar violation) plus EXZ (excessive zeros), or one or more LOS (Loss of signal) defects. For a B8Zs-coded signal, BVPs that are part of the zero substitution code are excluded
LOSS-L	The near end Loss of Signal Seconds Line (LOSS-L) is a count of one-second intervals containing one or more LOS defects.

T1 Path PM

Near End T1 Path Layer PM

PM Statistic	Definition
CV-P	The near end CV-P (code violation path) parameter for a DS1-ESF is a count of CRC-6 errors. For a DS1-SF, it is a count of detected frame bit errors.
ES-P	The near end ES-P (errored second path) parameter is a count of the seconds containing one or more anomalies and/or defects for paths on the receive end of the signal. For DS1-ESF paths, this parameter is a count of one-second intervals containing one or more CRC-6 errors, or one or more CS (controlled slip) events, or one or more SEF or AIS defects. For DS1-SF paths, this parameter is a count of one-second intervals containing one or more FE events, or one or more CS (controlled slip) events, or one or more SEF (severely errored frame) or AIS defects.
SES-P	The near end SES-P (Severely errored seconds path) parameter is a count of the seconds containing more than a particular quantity of anomalies and/or defects for paths of the signal. For the DS1-ESF paths, this parameter is a count of seconds when 320 or more CRC-6 errors or one or more SEF (severely errored frame) or AIS defects occurred. For DS1-SF paths, a SES (severely errored second) is a second containing either the occurrence of four FEs, or one or more SEF or AIS defects.
SAS-P	The near end SAS-P (Severely errored frame path) parameter is a count of one-second intervals containing one or more SEFs or one or more AIS defects on the signal.
AISS-P	The near end AISS-P (alarm indication signal second) parameter is a count of seconds containing one or more AIS defects.
UAS-P	The near end UAS-P (unavailable second path) parameter is a count of one-second intervals when the DS1 path is unavailable. The DS1 path becomes available when ten consecutive seconds occur with no SESs (severely errored second). The ten seconds with no SESs are excluded from unavailable time.
FC-P	The near end FC-P (failure count path) parameter is a count of the number of occurrences of the near end path failure events. A near path failure events begins when either and LOF or AIS failure is declared and ends when both LOF and AIS are clear.

Chapter 7
Replacing Hardware

This chapter describes how to replace your OSIRIS-XTD Shelf hardware. The chapter is divided into sections covering each of the shelves.

The major topics covered are:

- Equipment Handling Precautions
- Replacing OSIRIS Plug-in Units

Equipment Handling Precautions

Before following any directions in this chapter, read the following safety precautions. These safety precautions must be adhered to in the maintenance and use of the OSIRIS-XTD Shelf equipment, and single-fiber cables. These precautions ensure the safety of all personnel and the protection of the equipment.

Handling Equipment

Observe the following safety precautions when handling OSIRIS equipment.

CAUTION

The OSIRIS equipment are sensitive to electrostatic discharge.

Wear a grounded wriststrap or heel grounder at all times during handling. You may use additional personal grounding methods, for example, stand on a conductive carpet or wear conductive shoes.

When unpacking the equipment, place the antistatic bag containing the unit on an electrostatic discharge (ESD) safe surface. (An ESD safe surface is a conductive surface connected directly to an earth ground.)

When moving the equipment, carry the unit in an ESD safe container or in the antistatic bag provided.

Handle plug-in units by the card ejector. Do not touch the solder side of the card, its pin connectors, or any metallic components. Do not stack plug-in units on, or against each other. Store uninstalled plug-in units in their original antistatic bags.

Incorrect handling of the equipment may void the warranty.

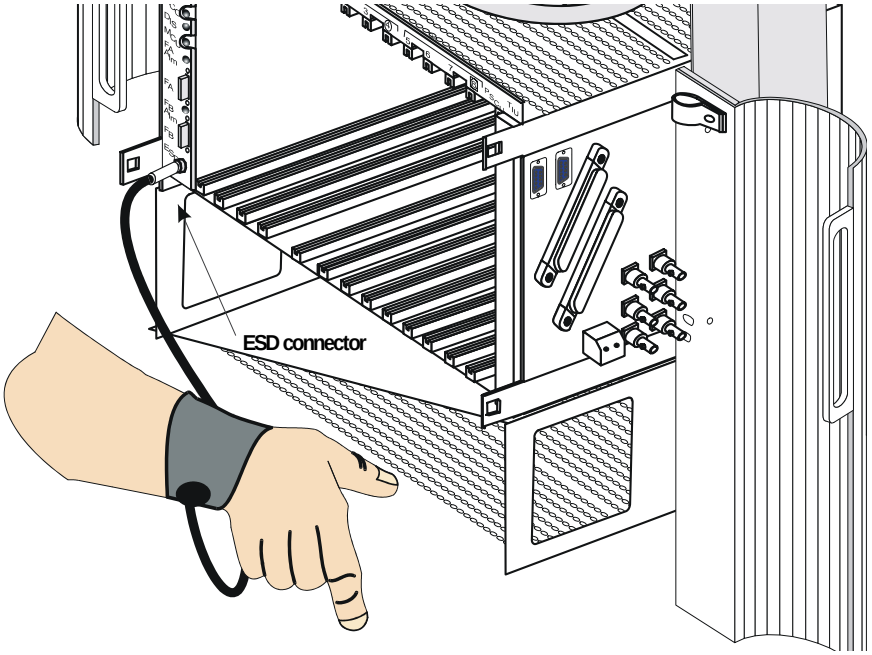
Using the ESD Connector

To protect against electrostatic discharge damage, an electrostatic discharge (ESD) connector that properly grounds a wriststrap is included with the equipment.

1. Do one of the following:
   - On the OSIRIS-XTD Shelf, locate the electrostatic discharge connector, labelled ESD, on the Alarm and Craftperson Interface Unit (ACIU). See Figure 5.

2. Connect a wriststrap to your wrist and then to the electrostatic discharge (ESD) connector. (If you wear a heel grounder, do not connect it to the ESD connector.)

Figure 5 Connecting a wriststrap to the ESD connector on the OSIRIS XTD Shelf



Store Plug-in Units Carefully

To prevent damage to plug-in units during storage, observe these precautions:

- Keep spare plug-in units in their original shipping containers.
- Store boards away from high humidity and temperature, otherwise, board warpage may occur.
- Prevent the accumulation of dirt or dust on the pin connectors as it may cause damage to the board or its components.

Handling Single-Fiber Cables

Observe the following safety precautions when working with single-fiber cables:

- Ensure that the optical connectors of the optical mappers transmit and receive units and the optical connectors of the fiber cables are protected by dust caps at all times.
- Keep all optical connectors capped when disconnecting fiber cables. Invisible laser radiation may be present in a fiber optic cable, which may cause severe eye damage, or even blindness.
- Wear safety glasses when installing optical fibers.
- Clean your hands after handling single-fiber cables to make certain that your hands are free of fiber particles.
- Handle optical fibers carefully and always position them in a safe and secure location during installation.
- Do not handle pieces of cut fiber with bare fingers. Use tweezers, or the sticky side of a piece of vinyl tape, to pick up and discard any loose fiber ends. All fiber cuttings should be placed in a plastic bottle provided for that purpose.

Replacing OSIRIS Plug-in Units

This section describes the procedures for replacing plug-in units in an operational OSIRIS XTD Shelf. In all cases the replacement unit must be identical to the unit removed. If the new unit is not identical to the original unit, follow the directions in this chapter to remove the plug-in unit, then follow the instructions included with the new unit to replace the unit.

Avoiding Traffic Interruption

In-service traffic is not interrupted by the removal of any one DS1/E1, DS3/E3 or EC-1 mapper, if there are protection mappers in slots 4, 8, 12, 22, and 23. Systems provisioned with equipment protection allow traffic to be switched to protection.

The protection mapper allows traffic to be switched to protection. This is acceptable as a short term solution, if you are just replacing the working mapper, but you cannot remove a working mapper on a permanent basis; the protection mapper does not act as a substitute mapper.

Removing an Ethernet, PacketPath (PEC 4) or MSE mapper **disrupts** the traffic moving through that mapper.

Removing an OC3c, OC3 Tributary, STM-1 or PAC 155 mapper does not disrupt traffic because they work with the APS (Automatic Protection Switching) feature, which allows a protection mapper to ensure traffic if the working mapper is removed.

Removing a PSCU if the traffic is on protection mapper (DS1/E1) disrupts in-service traffic.

Removing an Optical Access Unit automatically transfers traffic to the alternate OAU. If there is only one OAU, traffic is disrupted if it is removed.

Removing a coupled OAU/BIU automatically transfers traffic to the alternate OAU/BIU. If there is only one OAU/BIU, traffic is disrupted if it is removed.

Other plug-in units such as the ACIU and MCU may also be removed without affecting in-service traffic.

Removing the TIU **affects** service that passes through it.

Provisioned Information

Automatic configuration uploads allow the replacement unit to assume the configuration of the unit which was removed. The replacement unit automatically provisions itself with the attributes of the original unit.

WARNING

While removing plug-in units, avoid unintentional contact with DC input feeds and emergency power input feed parts. Contact presents a risk of electric shock and energy hazards.

Replacing Plug-In Units

The basic procedure to replace plug-in units is as follows:

1. Remove the shelf cover before starting the procedure.

2. Identify the plug-in unit by either the CLEI code on the face of the unit's top extractor lever or by the product code on the face of the unit's bottom extractor lever.
3. Identify the software that resides on the plug-in unit.
4. Remove the plug-in unit from the OSIRIS XTD Shelf.

Make sure that the new plug-in unit and the software that resides on it, are of the same type as the unit and software that you are replacing.

5. Insert the new plug-in unit. It is automatically provisioned with the settings of the original mapper.
6. Verify that there are no alarms associated to the new plug-in unit.
7. Replace the shelf cover. The newly installed plug-in unit is automatically provisioned with the settings of the original plug-in unit.

This table lists plug-in units and the tasks required to replace them on an OSIRIS XTD Shelf. For example, to replace an E1, perform the tasks in the sequence indicated by the numbers in the DS1/E1 column.

Plug-in Units to Replace											Replacement Tasks
Fast Ethernet (optical)[1]	OAU/ OC-3c/ STM-1[1]	MCU/ NMCU	DS1/E1 & DS3/E3/ EC-1	DS1PM+	Ethernet/ Fast Ethernet (electric) & V.35	PEC 4	PAC 155	MSE	AUX2	Protection Mappers & PSCU	
1	1	1	1	1	1	1	1	1	1	1	Remove shelf cover.
			2	2							Force a protection switch. LED is amber.
	2						2				Manually switch traffic to protection. If successful then force traffic switch to protection.
										2	Lock out protection mapper.
		2		3		2	3	2		3	Identify software version. See step 3 in the Replacing Plug-in-Units procedure.
2	3	3	3	4	2	3	4	3	2	4	Unseat plug-in unit.
3	4				3	4	5	4			Remove cables from plug-in unit.
4	5						6				Install protective caps on fiber patch cords.
5	6	4	4	5	4	5	7	5	3	5	Remove plug-in unit.
6	7	5	5	6	5	6	8	6	4	6	Insert new plug-in unit and lock in latches.
7	8	6	6	7	6	7	9	7	5	7	Check the LED status.
		7		8		8	10	8		8	Check software version of new card
8	9						11				Check power output.
9	10				7	9	12	9			Connect cables/fiber to plug-in unit.
	11										Perform continuity test.
10	12	8	7	9	8	10	13	10	6	9	Verify that there are no alarms related to the new plug-in unit.
										10	Release lock out protection mapper.
	13						14				Release the forced switch to protection
			8	10							Release the protection switch.
	14	9	9	11	9	11	15	11	7	11	Replace the shelf cover.

1. Observe all cautions when working with OAUs, OC-3c, OC3 Trib, STM-1, PacketPath and Ethernet (optical).

Replacing the ACIU

Before replacing the ACIU, it is necessary to disconnect from the Regular Power Source and connect to the Emergency Power Input Connector.

Switching Power from the Primary Power Source

The OSIRIS XTD Shelf is equipped with an emergency power input connector. This connector enables you to avoid traffic interruptions when your regular power source requires maintenance or it is necessary to replace the Alarm and Craftperson Interface Unit (ACIU).

The OSIRIS XTD Shelf accepts auxiliary power from the Emergency Power Inputs on the three TIUs (right and left sides of the shelf).

ALWAYS use the Emergency Power Input on the left TIU. TIUs on the right are fused at 5 AMPs only; the current may be higher than this rating. The left TIU has a 10 AMP fuse soldered on the PCB.

Input voltage is rated at -60V DC to -20V DC, except for the OC-48, which has an input voltage of between -40V and -60V DC. Power fuses are rated as 60V DC GMT 7.5 AMP.

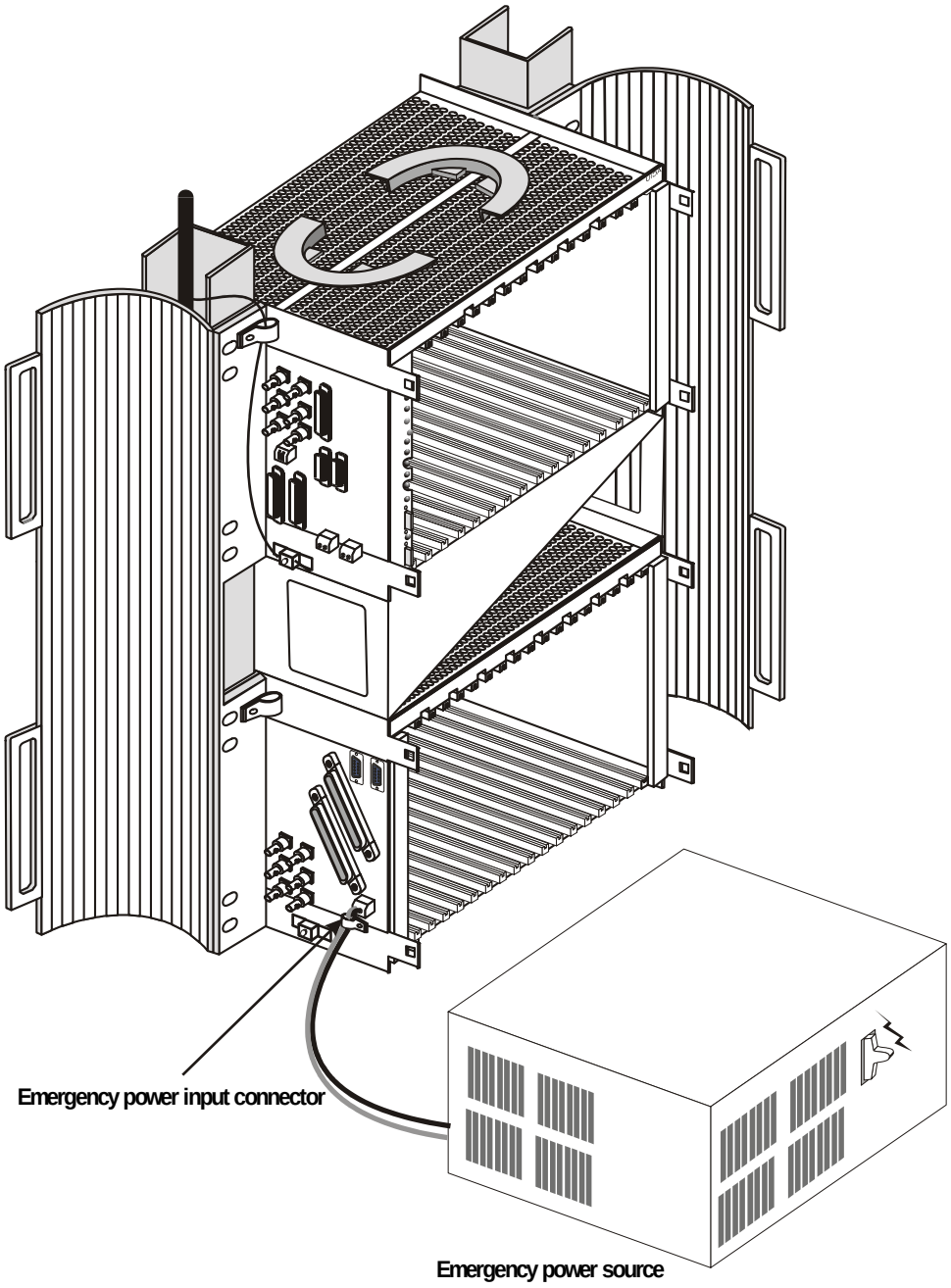
The Emergency Power Input is reserved for emergency maintenance procedures and must NOT be used to permanently power the system.

To switch power from the primary power source.

1. Ensure that the disconnect devices on the emergency power source are in the OFF position.
2. Turn the disconnect device of the A feed on the power distribution frame to the OFF position.
3. Remove the power cable from the A feed on the power distribution frame.
4. Remove the power cable from the V_A power input connector on the OSIRIS XTD Shelf.
5. Connect the power cable from the positive (+) lead on the emergency power source to the positive terminal of the emergency power input connector on the OSIRIS XTD Shelf.
6. Connect the power cable from the negative (-) lead on the emergency power source to the negative terminal of the emergency power input connector on the OSIRIS XTD Shelf.
7. Turn the disconnect devices on the emergency power source to the ON position.
8. Turn OFF the power distribution frame.
9. Remove the power cable from the B feed on the power distribution frame.
10. Remove the power cable from the V_B power input connector on the OSIRIS XTD Shelf.

The OSIRIS XTD Shelf is now powered by the emergency power source.

Figure 6 Connecting to the Emergency Power Input Connector from an Emergency Power Source



Replacing the ACIU

This section describes the procedure for replacing the ACIU and then reconnecting to the Regular Power Source, once ACIU replacement has been completed.

WARNING

There is a danger of electrical shock if the following instructions are not followed.

Removing the ACIU disrupts traffic unless power is provided through the emergency power input connector.

CAUTION

When handling any plug-in units, it is necessary to use the ESD Connector, refer to "Using the ESD Connector" on page 114.

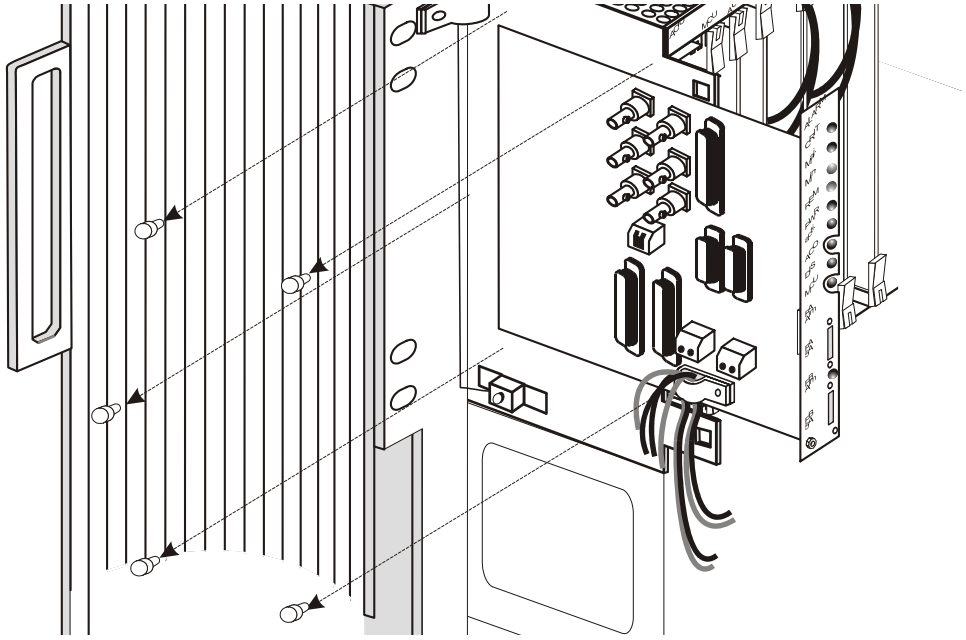
Note: ACIU replacement always temporarily interrupts DS3/EC-1/E-3 traffic.

To Replace the ACIU:

1. Remove the OSIRIS XTD Shelf cover.
2. Before continuing make sure that you have already switched the power from the primary power source. Refer to "Switching Power from the Primary Power Source" on page 119.
3. Disconnect all other cables which may be connected to the ACIU of the OSIRIS XTD Shelf.
4. Remove the five screws holding the ACIU to the shelf. Retain these screws since you must use these same five screws to anchor the new ACIU. You may damage the ACIU if you use any other screws.
5. Remove the ACIU.
6. Identify the ACIU by either the CLEI code or the product code.
7. Install a new ACIU of the same type.
8. Insert and tighten the same five screws you removed during Step 9 to hold the ACIU to the OSIRIS XTD Shelf.
9. Connect all the cables you disconnected, except for the power cables.
10. Connect the power cable to the V_B power input connector on the OSIRIS XTD Shelf.
11. Turn the disconnect device of the B feed on the power distribution frame to the ON position.
12. Make sure that the disconnect device of the A feed on the power distribution frame is in the OFF position.
13. Remove the power cable from the emergency power input connector on the OSIRIS XTD Shelf.
14. Connect this power cable to the V_A power input connector on the OSIRIS XTD Shelf.
15. Turn the disconnect device of the A feed on the power distribution frame to the ON position.
16. Verify that there are no alarms associated with the new ACIU.

17. Put back the OSIRIS XTD Shelf cover that was removed.

Figure 7 Removing the ACIU



Replacing the TIU

The TIU provides a physical interface for incoming and outgoing signals for electrical mappers. It is installed on the back of the OSIRIS-XTD Shelf.

The following procedure is for replacing TIU 1, TIU 2, and TIU 3 on the OSIRIS XTD Shelf. To remove the combined ACIU/TIU you must use the procedure to remove the ACIU. Refer to "Replacing the ACIU" on page 119.

Note: TIU replacement always temporarily interrupts traffic.

CAUTION

When handling any plug-in units, it is necessary to use the ESD Connector, refer to "Using the ESD Connector" on page 114.

To replace the TIU:

1. Remove the OSIRIS XTD Shelf cover.
2. Identify the TIU by either the CLEI code or the product code.
3. Disconnect cables from the DS1/E1 and DS3/E3 connectors on the TIU. Label all cables before removing them.
4. Remove the five screws holding the TIU to the shelf. Retain these screws since you must use these same five screws on the new TIU. You may damage the TIU if you use any other screws.
5. Remove the TIU.
6. Install the new TIU.
7. Insert and tighten the same five screws you removed to hold the TIU to the shelf.
8. Reconnect cables.

9. Verify that there are no alarms associated with the new TIU.
10. Replace the OSIRIS XTD Shelf cover.

Changing Fuses

There are two user-changeable fuses in the OSIRIS XTD Shelf. These fuses are located in the ACIU. Although there are other fuses in the OSIRIS XTD Shelf, these fuses are not user-changeable.

CAUTION

You may void the warranty on the OSIRIS XTD Shelf if the fuses, other than the two in the ACIU, are changed.

For continued protection against risk of fire, replace a fuse with one of the same type and rating.

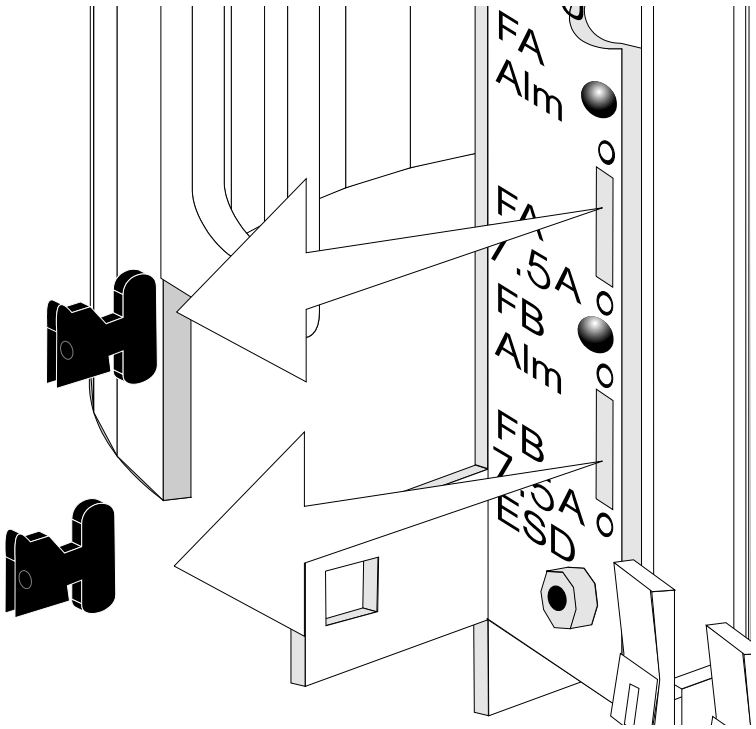
The fuses used in the OSIRIS XTD Shelf ACIU are as follows:

Designation	Rating	Manufacturer	Model #
FA, FB	7.5A, 60V DC, 125V AC	Bussmann Littelfuse	GMT-7.5 48107.5

Change the fuse as follows:

1. Remove the blown fuse from the ACIU. Refer to Figure 8.
2. Insert the new fuse into the ACIU.

Figure 8 Removing the fuse from the ACIU



Appendix

This appendix contains a list of acronyms used in this document and their meanings.

Acronyms

ACI Application Context Identifier

ACSE Association Control Service Element

ADM Add-Drop Multiplex

AFI Authority and Format Identifier

AID Access Identifier

AIS Alarm Indication Signal

AITS Acknowledged Information Transfer Service

ANSI American National Standards Institute

APD Avalanche Photodiode

APS Automatic Protection Switching

ASE Application Service Element

ASN.1 Abstract Syntax Notation 1

ATM Asynchronous Transfer Mode

B3ZS Bipolar with Three-Zero Substitution

B8ZS Bipolar with Eight-Zero Substitution

BA Booster Amplifier

BER Bit Error Ratio

BIP Bit Interleaved Parity

B-ISDN Broadband Integrated Services Digital Network

BITS Building Integrated Timing Supply

CC Composite Clock

CCITT International Telegraph & Telephone Consultative Committee

(replaced by ITU-T)

CEV Controlled Environmental Vault

CID Calling Address Identification

CLNP Connectionless-mode Network Layer Protocol

CLNS Connectionless-mode Network Service

CMI Coded Mark Inversion

CMISE Common Management Information Service Element

CNM Customer Network Management

CO Central Office

CONP Connection-mode Network Layer Protocol

CORBA Common Object Request Broker Architecture

CR Critical alarm

CSMA/CD Carrier Sense Multiple Access with Collision Detection

CV Coding Violation

CV-L Line Coding Violation

CV-LFE Far End Line Coding Violation

CV-P STS Path Coding Violation

CV-PFE Far End STS Path Coding Violation

CV-S Section Coding Violation

CV-V VT Path Coding Violation

CV-VFE Far End VT Path Coding Violation

DCC Data Communications Channel

DCF Dispersion Compensating Fiber

DCN Data Communications Network

DCS Digital Cross-Connect System

DFB Distributed Feedback

DM Degraded Minute

dpANS Draft Proposed American National Standard

DQDB Distributed Queue Dual Bus

DSF Dispersion Shifted Fiber

DSP Domain Specific Part

DS Digital Signal

DSAP Destination Service Access Point

DSn Digital Signal at level n

DSNE Directory Server NE

DUS DON'T USE for Synchronization

EIA Electronic Industries Association

EMC Electromagnetic Compatibility

EML Element Management Layer

EMS Element Management System

ENE End NE

EOC Embedded Operations Channel

EOW Express Orderwire

ES End System

ES Errored Second

ES-L Line Errored Second

ES-LFE Far End Line Errored Second

ES-P STS Path Errored Second

ES-PFE Far End STS Path Errored Second

ES-S Section Errored Second

ES-V VT Path Errored Second

ES-VFE Far End VT Path Errored Second

ESF Extended Superframe Format

FA Framework Technical Advisory

FC Failure Count

FC-L Line Failure Count

FC-LFE Far End Line Failure Count

FC-P STS Path Failure Count

FC-PFE Far End STS Path Failure Count

FC-V VT Path Failure Count

FC-VFE Far End VT Path Failure Count

FDDI Fiber Distributed Data Interface

FEBE Far End Block Error (replaced with REI)

FERF Far End Receive Failure (replaced with RDI)

FR Family of Requirements

FT File Transfer

FTAM File Transfer Access and Management

GNE Gateway NE

GR Generic Requirement

IAO Intraoffice

ICI Inter-Carrier Interface

ID Identifier

IDI Initial Domain Identifier

IDLC Integrated Digital Loop Carrier

IDP Initial Domain Part

IDRP Inter Domain Routing Protocol

IEEE Institute of Electrical and Electronics Engineers

INE Intermediate NE

IR Intermediate Reach

IS Intermediate System

ISI Intersymbol Interference

ISO International Organization for Standardization

ISP International Standardized Profile

ITU-T International Telecommunication Union - Telecommunication Standardization Sector (formerly CCITT)

LAN Local Area Network

LAPD Link Access Protocol on the D-Channel

LBC Laser Bias Current

LBO Line Build Out

LCN Local Communications Network

LDB Loop Detection Buffer

LEC Local Exchange Carrier

LED Light-Emitting Diode

LLC Logical Link Control

LOF Loss Of Frame

LOH Line Overhead

LOP Loss Of Pointer

LOS Loss Of Signal

LOW Local Orderwire

LR Long Reach

LSS Link Status Signal

LTE Line Terminating Equipment

MAC Media Access Control

MAN Metropolitan Area Network

MD Mediation Device

MF Mediation Function

MJ Major alarm

MLM Multi-Longitudinal Mode

MN Minor alarm

MPN Mode Partition Noise

MSE Multi-Service Ethernet

MTBF Mean Time Between Failure

MTIE Maximum Time Interval Error

MTTR Mean Time To Repair

NA Not Alarmed

NDF New Data Flag

NE Network Element

NET Network Entity Title

NPDU Network Protocol Data Unit

NRZ Non-Return to Zero

NSA Non-Service Affecting

NSAP Network Service Access Point

NSIF Network and Services Integration Forum

NSPDU Network Service Protocol Data Unit

OAM&P Operations, Administration, Maintenance, & Provisioning

OC-N Optical Carrier at level N

OFA Optical Fiber Amplifier

OIW OSI Implementors Workshop

OOF Out Of Frame

OPR Optical Power Received

OPT Optical Power Transmitted

ORL Optical Return Loss

OS Operations System

OSE Open Systems Environment

OSI Open Systems Interconnection

OTGR Operations Technology Generic Requirements

OW Orderwire

PA Pre-Amplifier

PBX Private Branch Exchange

PCH Pre-Chirp

PDC Passive Dispersion Compensation

PDL Polarization Dependent Loss

PDU Protocol Data Unit

PID Protocol Identification

PIN Positive-Intrinsic-Negative (photodiode)

PJ Pointer Justification

PKI Public Key Infrastructure

PLCP Physical Layer Convergence Procedure

PLL Phase Lock Loop

PLM-P STS Path Payload Label Mismatch

PLM-V VT Path Payload Label Mismatch

PM Performance Monitoring

PMF Polarization Maintaining Fiber

PNO Provisionable by the Network Operator

POH Path Overhead

PPDU Presentation Protocol Data Unit

PRS Primary Reference Source or Stratum 1 Traceable

PSAP Presentation Service Access Point

PSC Protection Switching Count

PSD Protection Switching Duration

PSN Packet Switched Network

PTE Path Terminating Equipment

PVC Permanent Virtual Circuit

QoS Quality of Service

RAI Remote Alarm Indication

RDI Remote Defect Indication

REI Remote Error Indication

RES Reserved for Network Synchronization Use

RFI Remote Failure Indication

RGTR Regenerator

RPDU Route Protocol Data Unit

RPP Reliability Prediction Procedure

RZ Return to Zero

SA Service Affecting

SAPI Service Access Point Identifier

SAW Surface Acoustic Wave

SD Signal Degrade

SDH Synchronous Digital Hierarchy

SEF Severely Errored Framing

SEFS Severely Errored Framing Second

SEFS-S Section Severely Errored Framing Second

SES Severely Errored Second

SES-L Line Severely Errored Second

SES-LFE Far End Line Severely Errored Second

SES-P STS Path Severely Errored Second

SES-PFE Far End STS Path Severely Errored Second

SES-S Section Severely Errored Second

SES-V VT Path Severely Errored Second

SES-VFE Far End VT Path Severely Errored Second

SF Signal Fail

SIA Stable Implementation Agreements

SIF SONET Interoperability Forum

SLM Single Longitudinal Mode

SLM-P STS Signal Label Mismatch (replaced by PLM-P and UNEQ-P)

SLM-V VT Signal Label Mismatch (replaced by PLM-V and UNEQ-V)

SMC SONET Minimum Clock (traceable)

SMF Single Mode Fiber

SNDCF Subnetwork Dependent Convergence Function

SNR Signal to Noise Ratio

SOH Section Overhead

SONET Synchronous Optical Network

SPE Synchronous Payload Envelope

SPM Self Phase Modulation

SR Short Reach

SR Special Report

SSAP Source Service Access Point

SSR Side Mode Suppression Ratio

STE Section Terminating Equipment

ST2 Stratum 2 (traceable)

ST3E Stratum 3E (traceable)

ST3 Stratum 3 (traceable)

ST4 Stratum 4 (traceable)

STS Synchronous Transport Signal

STS-N Synchronous Transport Signal level N

STU Synchronized - Traceability Unknown

SYNTRAN Synchronous (DS3) Transmission

TA Technical Advisory

TARP TID Address Resolution Protocol

TBD To Be Determined

TCA Threshold Crossing Alert

TCP/IP Transport Control Protocol/ Internet Protocol

TDEV Time Deviation

TDC TARP Data Cache

TEF TARP Echo Function

TEI Terminal Endpoint Identifier

TIA Telecommunications Industries Association

TID Target Identification

TIE Time Interval Error

TL1 Transaction Language 1

TM Terminal Multiplex

TMN Telecommunications Management Network

TNC Transit Node Clock (traceable)

TP Transport Protocol

TP4 Transport Protocol Class 4

TR Technical Reference

TSAP Transport Service Access Point

TSG Timing Signal Generator

UAS Unavailable Second

UAS-L Line Unavailable Second

UAS-LFE Far End Line Unavailable Second

UAS-P STS Path Unavailable Second

UAS-PFE Far End STS Path Unavailable Second

UAS-V VT Path Unavailable Second

UAS-VFE Far End VT Path Unavailable Second

UI Unit Interval

UID User Identification

UITS Unacknowledged Information Transfer Service

UNEQ-P STS Path Unequipped

UNEQ-V VT Path Unequipped

UNI User Network Interface

UPSR Unidirectional Path Switched Ring

URC Update Remote Cache

USL User System Language

VC Virtual Circuit

VT Virtual Tributary

WS Workstation

WTR Wait To Restore

ZCS Zero Code Suppression

Index

M

N

O

P

R

S

T

U

V

W