Cisco ONS SONET TL1 Reference Guide

Cisco ONS 15310-MA, Cisco ONS 15454, Cisco ONS 15454 M2, and Cisco ONS 15454 M6
Product and Documentation Release 9.2
May 2010

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: 78-19405-01

Cisco ONS SONET TL1 Reference Guide, Release 9.2

CONTENTS

FIGURES

TABLES

Preface

Note The terms "Unidirectional Path Switched Ring" and "UPSR" may appear in Cisco literature. These terms do not refer to using Cisco ONS 15xxx products in a unidirectional path switched ring configuration. Rather, these terms, as well as "Path Protected Mesh Network" and "PPMN," refer generally to Cisco's path protection feature, which may be used in any topological network configuration. Cisco does not recommend using its path protection feature in any particular topological network configuration.

This section explains the objectives, intended audience, and organization of this publication and describes the conventions that convey instructions and other information.

Revision History

This is the first release of this publication.

Document Objectives

This guide explains the use of Transaction Language 1 (TL1) for the Cisco ONS 15310-MA, Cisco ONS 15454, Cisco ONS 15454 M2, and Cisco ONS 15454 M6 systems. Use this guide in conjunction with the appropriate publications listed in the Related Documentation section.

Audience

To use this publication, you should be familiar with Cisco or equivalent optical transmission hardware and cabling, telecommunications hardware and cabling, electronic circuitry and wiring practices, and preferably have experience as a telecommunications technician.

Document Organization

The *Cisco ONS SONET TL1 Reference Guide, R9.2* is organized into the following chapters:

- Chapter 1, "General Information," explains command syntax, autonomous messages, Cisco Transport Controller (CTC) interoperability, security level privileges associated with each command, command completion behavior, and other general information.
- Chapter 2, "Procedures and Provisioning," provides procedures and provisioning for setting up TL1 communication, test access, gateway, software download, and other procedures and provisioning using TL1.
- Chapter 3, "TL1 Errors" provides TL1 error information supported by the Cisco ONS 15310-MA, Cisco ONS 15454, Cisco ONS 15454 M2, and Cisco ONS 15454 M6.

Related Documentation

Use the *Cisco ONS SONET TL1 Reference Guide, R9.2* in conjunction with the following referenced Release 9.2 publications:

- *Cisco ONS SONET TL1 Command Guide*
  Provides a full TL1 command and autonomous message set including parameters, access identifiers (AIDs), conditions, and modifiers.
- *Cisco ONS SONET TL1 Command Quick Reference Guide*
  Provides input formats and output formats (where applicable) for all Release 9.2 TL1 commands and autonomous messages.
- *Cisco ONS SONET TL1 for Beginners*
  Provides basic beginning instruction for using TL1.
- *Cisco ONS 15454 Procedure Guide*
  Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide
  Provides procedures and tasks for the corresponding Cisco ONS node and network.
- *Cisco ONS 15454 Reference Manual*
  Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual
  Provides reference material for the corresponding Cisco ONS node and network.
- *Cisco ONS 15454 Troubleshooting Guide*
  Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide
  Provides general troubleshooting procedures, alarm descriptions and troubleshooting procedures, and performance monitoring and SNMP parameters.
- *Cisco ONS 15454 DWDM Procedure Guide*
  Explains installation, turn up, provisioning, and maintenance for Cisco ONS 15454 dense wavelength division (DWDM) systems.

- *Cisco ONS 15454 DWDM Reference Manual*
  Explains installation, turn up, provisioning, and maintenance for Cisco ONS 15454 dense wavelength division (DWDM) systems.
- *Cisco ONS 15454 DWDM Troubleshooting Guide*
  Provides troubleshooting information and troubleshooting-related parameters for the Cisco ONS 15454 (ANSI) and Cisco ONS 15454 SDH (ETSI) platforms, specifically the DWDM application that can operate on either platform.
- *Cisco ONS 15454 and Cisco ONS 15454 SDH Ethernet Card Software Feature and Configuration Guide*
  Provides software features for all Ethernet cards and configuration information for Cisco IOS on ML-Series cards.
- *Cisco ONS 15310-CL and Cisco ONS 15310-MA Ethernet Card Software Feature and Configuration Guide*
  Provides software features and operations of the ML-100T-8 and the CE-100T-8 Ethernet cards for the Cisco ONS 15310-MA.
- Release Notes for Cisco ONS 15454, ONS 15454 M2, and ONS 15454 M6 DWDM, Release 9.2
  Release Notes for Cisco ONS 15454 SONET and SDH, Release 9.2
  Release Notes for Cisco ONS 15310-MA, Release 9.2
  Provides caveats, closed issues, and new feature and functionality information.

For an update on End-of-Life and End-of-Sale notices, refer to http://cisco.com/en/US/products/hw/optical/ps2001/prod_eol_notices_list.html

Document Conventions

This publication uses the following conventions:

Convention	Application
boldface	Commands and keywords in body text.
[ ]	Keywords or arguments that appear within square brackets are optional.
Ctrl	The control key. For example, where Ctrl + D is written, hold down the Control key while pressing the D key.
< >	Command parameters that must be replaced by module-specific codes.

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the document.

Caution Means *reader be careful*. In this situation, the user might do something that could result in equipment damage or loss of data.

Warning **IMPORTANT SAFETY INSTRUCTIONS**

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS

Waarschuwing **BELANGRIJKE VEILIGHEIDSINSTRUCTIES**

Dit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van de standaard praktijken om ongelukken te voorkomen. Gebruik het nummer van de verklaring onderaan de waarschuwing als u een vertaling van de waarschuwing die bij het apparaat wordt geleverd, wilt raadplegen.

BEWAAR DEZE INSTRUCTIES

Varoitus **TÄRKEITÄ TURVALLISUUSOHJEITA**

Tämä varoitusmerkki merkitsee vaaraa. Tilanne voi aiheuttaa ruumiillisia vammoja. Ennen kuin käsittelet laitteistoa, huomioi sähköpiirien käsittelemiseen liittyvät riskit ja tutustu onnettomuuksien yleisiin ehkäisytapoihin. Turvallisuusvaroitusten käännökset löytyvät laitteen mukana toimitettujen käännettyjen turvallisuusvaroitusten joukosta varoitusten lopussa näkyvien lausuntonumeroiden avulla.

SÄILYTÄ NÄMÄ OHJEET

Attention **IMPORTANTES INFORMATIONS DE SÉCURITÉ**

Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant entraîner des blessures ou des dommages corporels. Avant de travailler sur un équipement, soyez conscient des dangers liés aux circuits électriques et familiarisez-vous avec les procédures couramment utilisées pour éviter les accidents. Pour prendre connaissance des traductions des avertissements figurant dans les consignes de sécurité traduites qui accompagnent cet appareil, référez-vous au numéro de l'instruction situé à la fin de chaque avertissement.

CONSERVEZ CES INFORMATIONS

Warnung **WICHTIGE SICHERHEITSHINWEISE**

Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu Verletzungen führen kann. Machen Sie sich vor der Arbeit mit Geräten mit den Gefahren elektrischer Schaltungen und den üblichen Verfahren zur Vorbeugung vor Unfällen vertraut. Suchen Sie mit der am Ende jeder Warnung angegebenen Anweisungsnummer nach der jeweiligen Übersetzung in den übersetzten Sicherheitshinweisen, die zusammen mit diesem Gerät ausgeliefert wurden.

BEWAHREN SIE DIESE HINWEISE GUT AUF.

Avvertenza **IMPORTANTI ISTRUZIONI SULLA SICUREZZA**

Questo simbolo di avvertenza indica un pericolo. La situazione potrebbe causare infortuni alle persone. Prima di intervenire su qualsiasi apparecchiatura, occorre essere al corrente dei pericoli relativi ai circuiti elettrici e conoscere le procedure standard per la prevenzione di incidenti. Utilizzare il numero di istruzione presente alla fine di ciascuna avvertenza per individuare le traduzioni delle avvertenze riportate in questo documento.

CONSERVARE QUESTE ISTRUZIONI

Advarsel **VIKTIGE SIKKERHETSINSTRUKSJONER**

Dette advarselssymbolet betyr fare. Du er i en situasjon som kan føre til skade på person. Før du begynner å arbeide med noe av utstyret, må du være oppmerksom på farene forbundet med elektriske kretser, og kjenne til standardprosedyrer for å forhindre ulykker. Bruk nummeret i slutten av hver advarsel for å finne oversettelsen i de oversatte sikkerhetsadvarslene som fulgte med denne enheten.

TA VARE PÅ DISSE INSTRUKSJONENE

Aviso **INSTRUÇÕES IMPORTANTES DE SEGURANÇA**

Este símbolo de aviso significa perigo. Você está em uma situação que poderá ser causadora de lesões corporais. Antes de iniciar a utilização de qualquer equipamento, tenha conhecimento dos perigos envolvidos no manuseio de circuitos elétricos e familiarize-se com as práticas habituais de prevenção de acidentes. Utilize o número da instrução fornecido ao final de cada aviso para localizar sua tradução nos avisos de segurança traduzidos que acompanham este dispositivo.

GUARDE ESTAS INSTRUÇÕES

¡Advertencia! **INSTRUCCIONES IMPORTANTES DE SEGURIDAD**

Este símbolo de aviso indica peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considere los riesgos de la corriente eléctrica y familiarícese con los procedimientos estándar de prevención de accidentes. Al final de cada advertencia encontrará el número que le ayudará a encontrar el texto traducido en el apartado de traducciones que acompaña a este dispositivo.

GUARDE ESTAS INSTRUCCIONES

Varning! **VIKTIGA SÄKERHETSANVISNINGAR**

Denna varningssignal signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanliga förfaranden för att förebygga olyckor. Använd det nummer som finns i slutet av varje varning för att hitta dess översättning i de översatta säkerhetsvarningar som medföljer denna anordning.

SPARA DESSA ANVISNINGAR

FONTOS BIZTONSÁGI ELOÍRÁSOK

Ez a figyelmezeto jel veszélyre utal. Sérülésveszélyt rejto helyzetben van. Mielott bármely berendezésen munkát végezte, legyen figyelemmel az elektromos áramkörök okozta kockázatokra, és ismerkedjen meg a szokásos balesetvédelmi eljárásokkal. A kiadványban szereplo figyelmeztetések fordítása a készülékhez mellékelt biztonsági figyelmeztetések között található; a fordítás az egyes figyelmeztetések végén látható szám alapján keresheto meg.

ORIZZE MEG EZEKET AZ UTASÍTÁSOKAT!

Предупреждение **ВАЖНЫЕ ИНСТРУКЦИИ ПО СОБЛЮДЕНИЮ ТЕХНИКИ БЕЗОПАСНОСТИ**

Этот символ предупреждения обозначает опасность. То есть имеет место ситуация, в которой следует опасаться телесных повреждений. Перед эксплуатацией оборудования выясните, каким опасностям может подвергаться пользователь при использовании электрических цепей, и ознакомьтесь с правилами техники безопасности для предотвращения возможных несчастных случаев. Воспользуйтесь номером заявления, приведенным в конце каждого предупреждения, чтобы найти его переведенный вариант в переводе предупреждений по безопасности, прилагаемом к данному устройству.

СОХРАНИТЕ ЭТИ ИНСТРУКЦИИ

警告 重要的安全性说明

此警告符号代表危险。您正处于可能受到严重伤害的工作环境中。在您使用设备开始工作之前，必须充分意识到触电的危险，并熟练掌握防止事故发生的标准工作程序。请根据每项警告结尾提供的声明号码来找到此设备的安全性警告说明的翻译文本。

请保存这些安全性说明

警告 安全上の重要な注意事項

「危険」の意味です。人身事故を予防するための注意事項が記述されています。装置の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止策に留意してください。警告の各国語版は、各注意事項の番号を基に、装置に付属の「Translated Safety Warnings」を参照してください。

これらの注意事項を保管しておいてください。

주의 중요 안전 지침

이 경고 기호는 위험을 나타냅니다. 작업자가 신체 부상을 일으킬 수 있는 위험한 환경에 있습니다. 장비에 작업을 수행하기 전에 전기 회로와 관련된 위험을 숙지하고 표준 작업 관례를 숙지하여 사고를 방지하십시오. 각 경고의 마지막 부분에 있는 경고문 번호를 참조하여 이 장치와 함께 제공되는 번역된 안전 경고문에서 해당 번역문을 찾으십시오.

이 지시 사항을 보관하십시오.

Aviso **INSTRUÇÕES IMPORTANTES DE SEGURANÇA**

Este símbolo de aviso significa perigo. Você se encontra em uma situação em que há risco de lesões corporais. Antes de trabalhar com qualquer equipamento, esteja ciente dos riscos que envolvem os circuitos elétricos e familiarize-se com as práticas padrão de prevenção de acidentes. Use o número da declaração fornecido ao final de cada aviso para localizar sua tradução nos avisos de segurança traduzidos que acompanham o dispositivo.

GUARDE ESTAS INSTRUÇÕES

Advarsel **VIGTIGE SIKKERHEDSANVISNINGER**

Dette advarselssymbol betyder fare. Du befinder dig i en situation med risiko for legemesbeskadigelse. Før du begynder arbejde på udstyr, skal du være opmærksom på de involverede risici, der er ved elektriske kredsløb, og du skal sætte dig ind i standardprocedurer til undgåelse af ulykker. Brug erklæringsnummeret efter hver advarsel for at finde oversættelsen i de oversatte advarsler, der fulgte med denne enhed.

GEM DISSE ANVISNINGER

تحذير **إرشادات الأمان الهامة**

يوضح رمز التحذير هذا وجود خطر. وهذا يعني أنك متواجد في مكان قد ينتج عنه التعرض لإصابات. قبل بدء العمل، احذر مخاطر التعرض للصدمات الكهربائية وكن على علم بالإجراءات القياسية للحيلولة دون وقوع أي حوادث. استخدم رقم البيان الموجود في أخر كل تحذير لتحديد مكان ترجمته داخل تحذيرات الأمان المترجمة التي تأتي مع الجهاز.

قم بحفظ هذه الإرشادات

Upozorenje **VAŽNE SIGURNOSNE NAPOMENE**

Ovaj simbol upozorenja predstavlja opasnost. Nalazite se u situaciji koja može prouzročiti tjelesne ozljede. Prije rada s bilo kojim uređajem, morate razumjeti opasnosti vezane uz električne sklopove, te biti upoznati sa standardnim načinima izbjegavanja nesreća. U prevedenim sigurnosnim upozorenjima, priloženima uz uređaj, možete prema broju koji se nalazi uz pojedino upozorenje pronaći i njegov prijevod.

SAČUVAJTE OVE UPUTE

Upozornění **DŮLEŽITÉ BEZPEČNOSTNÍ POKYNY**

Tento upozorňující symbol označuje nebezpečí. Jste v situaci, která by mohla způsobit nebezpečí úrazu. Před prací na jakémkoliv vybavení si uvědomte nebezpečí související s elektrickými obvody a seznamte se se standardními opatřeními pro předcházení úrazům. Podle čísla na konci každého upozornění vyhledejte jeho překlad v přeložených bezpečnostních upozorněních, která jsou přiložena k zařízení.

USCHOVEJTE TYTO POKYNY

Προειδοποίηση

ΣΗΜΑΝΤΙΚΕΣ ΟΔΗΓΙΕΣ ΑΣΦΑΛΕΙΑΣ

Αυτό το προειδοποιητικό σύμβολο σημαίνει κίνδυνο. Βρίσκεστε σε κατάσταση που μπορεί να προκαλέσει τραυματισμό. Πριν εργαστείτε σε οποιοδήποτε εξοπλισμό, να έχετε υπόψη σας τους κινδύνους που σχετίζονται με τα ηλεκτρικά κυκλώματα και να έχετε εξοικειωθεί με τις συνήθεις πρακτικές για την αποφυγή ατυχημάτων. Χρησιμοποιήστε τον αριθμό δήλωσης που παρέχεται στο τέλος κάθε προειδοποίησης, για να εντοπίσετε τη μετάφρασή της στις μεταφρασμένες προειδοποιήσεις ασφαλείας που συνοδεύουν τη συσκευή.

ΦΥΛΑΞΤΕ ΑΥΤΕΣ ΤΙΣ ΟΔΗΓΙΕΣ

אזהרה

הוראות בטיחות חשובות

סימן אזהרה זה מסמל סכנה. אתה נמצא במצב העלול לגרום לפציעה. לפני שתעבוד עם ציוד כלשהו, עליך להיות מודע לסכנות הכרוכות במעגלים חשמליים ולהכיר את הנהלים המקובלים למניעת תאונות. השתמש במספר ההוראה המסופק בסופה של כל אזהרה כד לאתר את התרגום באזהרות הבטיחות המתורגמות שמצורפות להתקן.

שמור הוראות אלה

Opomena

ВАЖНИ БЕЗБЕДНОСНИ НАПАТСТВИЈА

Симболот за предупредување значи опасност. Се наоѓате во ситуација што може да предизвика телесни повреди. Пред да работите со опремата, бидете свесни за ризикот што постои кај електричните кола и треба да ги познавате стандардните постапки за спречување на несреќни случаи. Искористете го бројот на изјавата што се наоѓа на крајот на секое предупредување за да го најдете неговиот период во преведените безбедносни предупредувања што се испорачани со уредот.

ЧУВАЈТЕ ГИ ОВИЕ НАПАТСТВИЈА

Ostrzeżenie

WAŻNE INSTRUKCJE DOTYCZĄCE BEZPIECZEŃSTWA

Ten symbol ostrzeżenia oznacza niebezpieczeństwo. Zachodzi sytuacja, która może powodować obrażenia ciała. Przed przystąpieniem do prac przy urządzeniach należy zapoznać się z zagrożeniami związanymi z układami elektrycznymi oraz ze standardowymi środkami zapobiegania wypadkom. Na końcu każdego ostrzeżenia podano numer, na podstawie którego można odszukać tłumaczenie tego ostrzeżenia w dołączonym do urządzenia dokumencie z tłumaczeniami ostrzeżeń.

NINIEJSZE INSTRUKCJE NALEŻY ZACHOWAĆ

Upozornenie

DÔLEŽITÉ BEZPEČNOSTNÉ POKYNY

Tento varovný symbol označuje nebezpečenstvo. Nachádzate sa v situácii s nebezpečenstvom úrazu. Pred prácou na akomkoľvek vybavení si uvedomte nebezpečenstvo súvisiace s elektrickými obvodmi a oboznámte sa so štandardnými opatreniami na predchádzanie úrazom. Podľa čísla na konci každého upozornenia vyhľadajte jeho preklad v preložených bezpečnostných upozorneniach, ktoré sú priložené k zariadeniu.

USCHOVAJTE SI TENTO NÁVOD

Obtaining Optical Networking Information

This section contains information that is specific to optical networking products. For information that pertains to all of Cisco, refer to the Obtaining Documentation, Obtaining Support, and Security Guidelines section.

Where to Find Safety and Warning Information

For safety and warning information, refer to the *Cisco Optical Transport Products Safety and Compliance Information* document that accompanied the product. This publication describes the international agency compliance and safety information for the Cisco ONS 15454 system. It also includes translations of the safety warnings that appear in the ONS 15454 system documentation.

Cisco Optical Networking Product Documentation CD-ROM

Optical networking-related documentation, including Cisco ONS 15xxx product documentation, is available in a CD-ROM package that ships with your product. The Optical Networking Product Documentation CD-ROM is updated periodically and may be more current than printed documentation.

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation*, as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

CHAPTER 1

General Information

Note The terms "Unidirectional Path Switched Ring" and "UPSR" may appear in Cisco literature. These terms do not refer to using Cisco ONS 15xxx products in a unidirectional path switched ring configuration. Rather, these terms, as well as "Path Protected Mesh Network" and "PPMN," refer generally to Cisco's path protection feature, which may be used in any topological network configuration. Cisco does not recommend using its path protection feature in any particular topological network configuration.

Transaction Language 1 (TL1) is a subset of the input and output messages contained in the International Telecommunications Union (ITU) Man-Machine Language (MML). TL1 provides a standard set of messages that can be used for communicating between operating systems and network elements (NEs), and personnel and network elements. For more information about TL1, refer to Telcordia document GR-833-CORE, *Network Maintenance: Network Element and Transport Surveillance Messages*.

This chapter provides information and procedures for getting started with TL1:

1.1 Command Syntax

TL1 commands conform to the following syntax:

a:b:c:d:e: ... z;

where:

“a” is the command code

“b” is the target identifier (TID)

“c” is the access identifier (AID) or the user identifier (UID)

“d” is the correlation tag (CTAG)

“e: ... z;” are other positions required for various commands

The TID, AID, and CTAG route and control the TL1 command. Other parameters provide additional information required to complete the action requested by the command. TL1 command codes, parameter names, and parameter values can be either uppercase or lowercase exclusively or any combination of the two, unless specifically noted in the command description.

The TID is a unique name given to each system when it is installed. The name identifies the particular NE (in this case, the ONS 15310-MA, Cisco ONS 15454, Cisco ONS 15454 M2, or Cisco ONS 15454 M6) to which each command is directed. The value of TID can be any TL1 identifier or text string, but it is limited to 20 characters. An identifier contains any number of letters or digits, but must start with a letter. A text string is any alphanumeric or punctuation character or characters enclosed in double quotation marks. The presence of the TID is required in all input commands, but its value can be null (represented by two successive colons). The TID can be null when the operating system directly communicates with the target NE. The recommended value for the TID, when it is used, is the target’s common language location identifier (CLLI) code. To establish the TID for a node, use the Provisioning > General tab in CTC.

The AID is an access code used to identify and address specific objects within the NE. These objects include individual pieces of equipment, transport spans, access tributaries, and other objects.

The CTAG is a unique identifier given to each input command by the user. When the NE responds to a specific command, it includes the command’s CTAG in the reply. Including the CTAG eliminates confusion about which response corresponds to which command. Valid CTAG values include strings of up to six characters composed of identifiers (alphanumeric, beginning with a letter) or decimal numerals (a string of decimal digits with an optional nontrailing period).

The following specification characters are used throughout this document as vehicles for defining the syntax:

- Angle brackets (< >) enclose a symbol specifier, for example, <CTAG>.
- Square brackets ([ ]) enclose an optional symbol, for example, [<TID>].
- Quotation marks (“ ”) enclose a literal character, as shown in the following output example:

  SLOT-7:PLUGIN,TC,,,,,,,:\“EQUIPMENT PLUG-IN\”,TCC

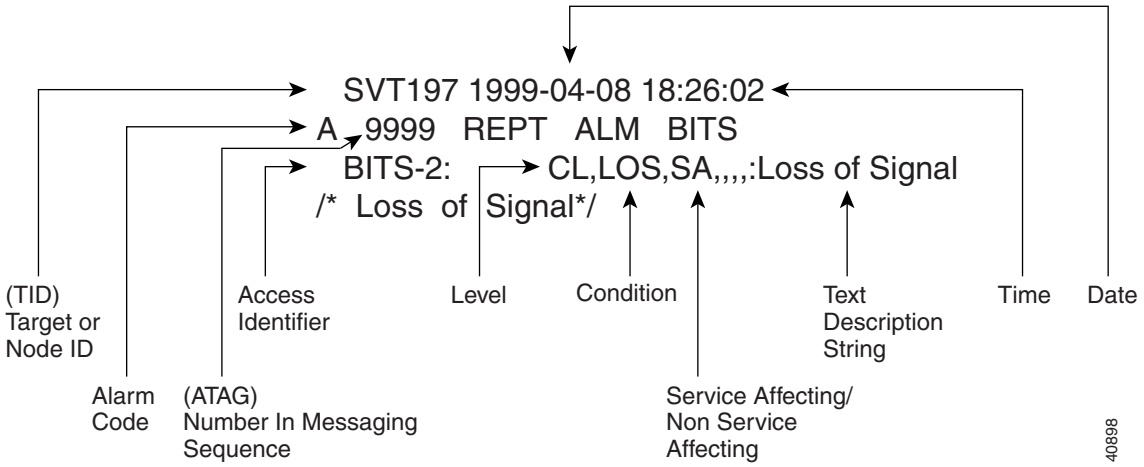
1.2 Autonomous Message Syntax

Autonomous messages are used to report alarms, configuration changes, and condition changes. Many of these messages, such as those relating to alarm conditions, are spontaneously triggered by the NE itself without intervention. Other messages, such as those relating to the reporting of periodic condition states or performance data values, are scheduled by the NE user through other commands. Because you do not issue autonomous messages to the NE, they do not include input formats or input examples.

The autonomous TL1 messages are included in the *Cisco ONS SONET TL1 Command Guide*. Figure 1-1 shows the autonomous message format. The autonomous message tag (ATAG) is used for message sequencing. The number is incremented by one for each autonomous message sent by the NE. Cisco NEs use the whole numbers 0000 to 9999 as ATAGs.

Note Some autonomous messages (REPT DBCHG and REPT EVT SESSION, for example) differ slightly from the format shown in the third line of Figure 1-1.

Figure 1-1 Autonomous Message Format



The alarm code indicates the severity of the autonomous message. Valid values for alarm codes in decreasing order of severity are as follows:

- *C—Critical alarm
- **—Major alarm
- *^—Minor alarm
- A^—Nonalarmed message

Critical, Major, and Minor correspond to the reporting of alarmed events. The Nonalarmed message designation is used when the NE is reporting nonalarmed events, periodic measurements, or the results of previously scheduled diagnostics or audits. If multiple alarms are reported in the same message, the alarm code represents the highest severity of those being reported.

The following is an example of an output message that includes the Critical alarm code:

```
  AB7-56 1970-01-01 16:02:10
*C 100.100 REPT ALM EQPT
  "SYSTEM:CR,HITEMP,NSA,,,,:\"High Temperature\",TCC"
```

1.3 Command Completion Behavior

When you enter a TL1 command, one of three completion codes is returned. The completion codes are: completed (COMPLD), partial (PRTL), and deny (DENY). You can specify an explicit, implicit, or explicit with implicit list as explained in the following sections.

1.3.1 General Rules

The following sections contain general rules for AID lists and AID grouped lists.

1.3.1.1 Explicit List of AIDs—No Wildcards

If a set of AIDs is explicitly listed, including a set of just one AID, then each AID that is listed must complete successfully to return a COMPLD message. If more than one AID is in the set and at least one AID succeeds but all do not, then a PRTL with errors for each failed AID is returned. If all AIDs in the set fail, a DENY with errors for each failed AID is returned.

1.3.1.2 Implicit List of AIDs—Single AID With Wildcard

If a set of AIDs is implied by the use of the ALL modifier on a single AID, then follow the same rules as in Section 1.3.1.1 Explicit List of AIDs—No Wildcards. The caveat is that the implicit list only includes AIDs that apply to the command. For example, assume SLOT-3 contains an OC-12 card and only STS-3-4 and STS-3-7 are of path-width STS3c while the rest are STS1. An ED-STS1 command with STS-3-ALL AID applies only on the STS1 implicit AID set STS-3-{1,2,3,10,11,12} (with the ED-STS1 command).

No errors will be reported against any member of STS-3-{4,5,6,7,8,9} as they belong to the STS3c AID set.

Apply the following rules to the set:

1. If all valid AIDs match, COMPLD is returned with a matching list of cross-connections.
2. If some valid AIDs match but not all, COMPLD is returned with a matching list of cross-connections.
3. If all valid AIDs fail to match, DENY is returned.

1.3.1.3 Explicit List Grouped With Implicit List

If the set of AIDs is composed of two subsets, one set including explicitly stated AIDs and the other set implied by one or more AID(s) with the ALL modifier, then follow the rules of Section 1.3.1.1 Explicit List of AIDs—No Wildcards and Section 1.3.1.2 Implicit List of AIDs—Single AID With Wildcard, respectively. Apply the logic in Table 1-1 to the results from the two subsets:

Table 1-1 Explicit List, Implicit List, and Combined List Logic

Explicit List Returns	Implicit List Returns	Combined List Returns
COMPLD	COMPLD	COMPLD plus matching list
COMPLD	DENY	PRTL with errors plus matching list
PRTL	COMPLD	PRTL with errors plus matching list

Table 1-1 Explicit List, Implicit List, and Combined List Logic

Explicit List Returns	Implicit List Returns	Combined List Returns
PRTL	DENY	PRTL with errors plus matching list
COMPLD	PRTL	PRTL with errors plus matching list
DENY	PRTL	PRTL with errors plus matching list
DENY	COMPLD	PRTL with errors plus matching list
PRTL	PRTL	PRTL with errors plus matching list
DENY	DENY	DENY with errors

Example of explicit AID list grouped with implicit AID list:

FAC-1-1&FAC-2-ALL
FAC-3-ALL&FAC-7-ALL
STS-2-ALL&STS-12-1&STS-13-2&STS-14-ALL

1.3.2 Command Completion Behavior for Retrieval of Cross-Connections

When you enter a RTRV-CRS command, one of three completion codes will be returned. The completion codes are: COMPLD, PRTL, and DENY. You can specify an explicit, implicit, or explicit with implicit list as explained in the following sections.

1.3.2.1 Explicit List of AIDs—No Wildcards

For an explicit list of AIDs on a RTRV-CRS command, an error code will be returned for each AID that fails validation (for example, the user specifies STS-N-13 when SLOT-N only contains an OC-12) or for each AID where no matching cross-connection is found. To determine the completion code, follow the rules from the "1.3.1.1 Explicit List of AIDs—No Wildcards" section on page 1-4. If the result is either PRTL or COMPLD, then a list of matching cross-connections will accompany the response.

1.3.2.2 Implicit List of AIDs—Single AID With Wildcard

If a set of AIDs is implied by the use of the ALL modifier on a single AID, then follow the same AID expansion rule as defined in the example from the "1.3.1.2 Implicit List of AIDs—Single AID With Wildcard" section on page 1-4. Apply the following rules to the set:

1. If all valid AIDs match, COMPLD is returned with a matching list of cross-connections.
2. If some valid AIDs match but not all, COMPLD is returned with a matching list of cross-connections.
3. If all valid AIDs fail to match, DENY is returned.

In the following command example, STS-9-ALL maps to STS-9-{1,2,3,10,11,12}: RTRV-CRS-STS1:<TID>}:STS-9-ALL:<CTAG>. This is because there is a single-port OC-12 card in Slot 3 with STS-3C defined for STS-9-4 and STS-9-7. The set is traversed and returns only the STS1 cross-connections that exist using endpoints in that set. If no cross-connections are retrieved, COMPLD is returned.

1.3.2.3 Explicit List Grouped With Implicit List

When you have determined the implicit list, apply the rules from Section 1.3.2.2 Implicit List of AIDs—Single AID With Wildcard to the implicit list and the rules from Section 1.3.2.1 Explicit List of AIDs—No Wildcards to the explicit list. Apply the logic in Table 1-1 on page 1-4 to the results from the two subsets.

1.4 User Security Levels

User security levels limit the amount of time a user can leave the system idle before the TL1 session is locked to prevent unauthorized users from making changes. Higher security levels have shorter timeouts. Starting with Release 4.0, timeouts can be provisioned (by a Superuser) from CTC. If provisioned, it only affects users who are not currently logged in. A user that is logged in has to log out and log back in before the new timeouts will take affect. A Superuser can provision security levels through TL1 with the SET-ATTR-SECUDFLT command. Security levels are listed with each command and message in the *Cisco ONS SONET TL1 Command Guide*.

Table 1-2 shows security levels and their default timeouts.

Table 1-2 Security Default Timeouts

Security Level	Default Timeout
Retrieve	Unlimited
Maintenance	60 minutes
Provisioning	30 minutes
Superuser	15 minutes

1.5 Keyboard Shortcuts

TL1 has the ability to store previously issued commands so that they can be recalled for future use. A maximum of 20 commands are stored. All types of commands are stored, including invalid commands. If the session is a GNE session, it will store commands sent to both the gateway network element (GNE) and the end network element (ENE).

- Pressing **Ctrl-R** recalls the last command issued. Each time Ctrl-R is pressed, a previously issued command is displayed.
- Pressing **Ctrl-F** recalls commands in the forward direction.

After a command has been recalled, you can use the Backspace key to edit the command as necessary. Cursor keys (for example, left and right arrows) are not permitted for editing.

Note Command recall keys are only available when using a serial port session or an interactive Telnet session (for example, telnet <hostname> 3083).

The CTC TL1 session has its own means for recalling previously issued commands, described in the "Open a TL1 Session Through CTC" section on page 2-2.

1.6 Mixed Mode Timing Support

Although TL1 supports mixed mode timing, Cisco strongly advises against its implementation. Mixed mode timing is not a recommended timing mode because of the inherent risk of creating timing loops. Refer to Telcordia document GR-436-CORE, *Digital Network Synchronization Plan* for recommended synchronization planning. Refer to the platform-specific Cisco ONS Procedure Guide for information about setting up timing. For further assistance, contact the Cisco Technical Assistance Center (TAC) at www.cisco.com or call (800) 553-2447 for unresolved problems.

1.7 Starting Positions for an STS-Nc SPE

Table 1-3, Table 1-4, and Table 1-5 list possible starting positions for the ONS 15310-MA, ONS 15454, ONS 15454 M2, and ONS 15454 M6 STS-Nc synchronous payload envelope (SPE). In each of table, a "Y" indicates that the position is supported, and an "N" indicates that the position is not supported. More information about the generic NE support requirement can be found in Telcordia GR-253-CORE, *Synchronous Optical Network (SONET) Transport Systems: Common Generic Criteria*.

Table 1-3 Starting Positions for an STS-Nc SPE in an OC-12 Signal

STS-1 Number	STS-3c SPE	STS-6c SPE	STS-9c SPE	STS-12c SPE
1	Y	Y	Y	Y
4	Y	Y	Y	N
7	Y	Y	N	N
10	Y	N	N	N

Table 1-4 Starting Positions for an STS-Nc SPE in an OC-48 Signal

STS-1 Number	STS-3c SPE	STS-6c SPE	STS-9c SPE	STS-12c SPE	STS-24c SPE	STS-48c SPE
1	Y	Y	Y	Y	Y	Y
4	Y	Y	Y	N	Y	N
7	Y	Y	N	N	Y	N
10	Y	N	Y	N	Y	N
13	Y	Y	Y	Y	Y	N
16	Y	Y	Y	N	Y	N
19	Y	Y	Y	N	Y	N
22	Y	N	N	N	Y	N
25	Y	Y	Y	Y	Y	N
28	Y	Y	Y	N	N	N
31	Y	Y	N	N	N	N
34	Y	N	N	N	N	N
37	Y	Y	Y	Y	N	N
40	Y	Y	Y	N	N	N

Table 1-4 Starting Positions for an STS-Nc SPE in an OC-48 Signal (continued)

STS-1 Number	STS-3c SPE	STS-6c SPE	STS-9c SPE	STS-12c SPE	STS-24c SPE	STS-48c SPE
43	Y	Y	N	N	N	N
46	Y	N	N	N	N	N

Table 1-5 Starting Positions for an STS-Nc SPE in an OC-192 Signal

STS-1 Number	STS-3c SPE	STS-6c SPE	STS-9c SPE	STS-12c SPE	STS-24c SPE	STS-48c SPE	STS-192c SPE
1	Y	Y	Y	Y	Y	Y	Y
4	Y	Y	Y	N	Y	N	N
7	Y	Y	N	N	Y	N	N
10	Y	N	Y	N	Y	N	N
13	Y	Y	Y	Y	Y	N	N
16	Y	Y	Y	N	Y	N	N
19	Y	Y	Y	N	Y	N	N
22	Y	N	N	N	Y	N	N
25	Y	Y	Y	Y	Y	N	N
28	Y	Y	Y	N	N	N	N
31	Y	Y	N	N	N	N	N
34	Y	N	N	N	N	N	N
37	Y	Y	Y	Y	N	N	N
40	Y	Y	Y	N	N	N	N
43	Y	Y	N	N	N	N	N
46	Y	N	Y	N	N	N	N
49	Y	Y	Y	Y	Y	Y	N
52	Y	Y	Y	N	Y	N	N
55	Y	Y	Y	N	Y	N	N
58	Y	N	N	N	Y	N	N
61	Y	Y	Y	Y	Y	N	N
64	Y	Y	Y	N	Y	N	N
67	Y	Y	N	N	Y	N	N
70	Y	N	N	N	Y	N	N
73	Y	Y	Y	Y	Y	N	N
76	Y	Y	Y	N	N	N	N
79	Y	Y	N	N	N	N	N
82	Y	N	Y	N	N	N	N
85	Y	Y	Y	Y	N	N	N
88	Y	Y	Y	N	N	N	N

Table 1-5 Starting Positions for an STS-Nc SPE in an OC-192 Signal (continued)

STS-1 Number	STS-3c SPE	STS-6c SPE	STS-9c SPE	STS-12c SPE	STS-24c SPE	STS-48c SPE	STS-192c SPE
91	Y	Y	Y	N	N	N	N
94	Y	N	N	N	N	N	N
97	Y	Y	Y	Y	Y	Y	N
100	Y	Y	Y	N	Y	N	N
103	Y	Y	N	N	Y	N	N
106	Y	N	N	N	Y	N	N
109	Y	Y	Y	Y	Y	N	N
112	Y	Y	Y	N	Y	N	N
115	Y	Y	N	N	Y	N	N
118	Y	N	Y	N	Y	N	N
121	Y	Y	Y	Y	Y	N	N
124	Y	Y	Y	N	N	N	N
127	Y	Y	Y	N	N	N	N
130	Y	N	N	N	N	N	N
133	Y	Y	Y	Y	N	N	N
136	Y	Y	Y	N	N	N	N
139	Y	Y	N	N	N	N	N
142	Y	N	N	N	N	Y	N
145	Y	Y	Y	Y	Y	N	N
148	Y	Y	Y	N	Y	N	N
151	Y	Y	N	N	Y	N	N
154	Y	N	Y	N	Y	N	N
157	Y	Y	Y	Y	Y	N	N
160	Y	Y	Y	N	Y	N	N
163	Y	Y	Y	N	Y	N	N
166	Y	N	N	N	Y	N	N
169	Y	Y	Y	Y	Y	N	N
172	Y	Y	Y	N	N	N	N
175	Y	Y	N	N	N	N	N
178	Y	N	N	N	N	N	N
181	Y	Y	Y	Y	N	N	N
184	Y	Y	Y	N	N	N	N
187	Y	Y	N	N	N	N	N
190	Y	N	N	N	N	N	N

1.8 Default Values

This section lists the default values applied by the system when they are not explicitly specified during provisioning.

1.8.1 BLSR

Table 1-6 lists the default BLSR values that are applied by the system when they are not explicitly specified during BLSR provisioning (ENT-BLSR).

Table 1-6 BLSR Default Values

BLSR Parameter	Default
RVRTV	Y
RVTM	5.0 minutes
SRVRTV	Y
SRVTM	5.0 minutes

1.8.2 Cross-Connections

Table 1-7 lists the default cross-connection values that are applied by the system when they are not explicitly specified during circuit creation (ENT-CRS).

Table 1-7 Cross-Connections Default Values

Cross-Connection Parameter	Default
CCT	2WAY for both STSp and VT1 cross-connections

1.8.3 Environment

Table 1-8 lists the default environment alarms and controls values applied by the system when they are not explicitly specified during environment alarms and controls provisioning.

Table 1-8 Environment Alarms and Controls Default Values

Commands	Parameter Default
OPR-EXT-CONT	CONTTYPE is provisioned in the respective AID. There is no default for it. It is only used as a filter if entered. DUR always defaults to CONT.
RTRV-ATTR-CONT	There is no default for CONTTYPE. It is only used as a filter if entered.
RTRV-ATTR-ENV	There is no default for both NTFCNCDE and ALMTYPE, which are only used as filters if entered.

Table 1-8 Environment Alarms and Controls Default Values (continued)

Commands	Parameter Default
RTRV-EXT-CONT	CONTTYPE defaults to the control type associated with the AID.
SET-ATTR-ENV	NTFCNCDE defaults to NR. ALMTYPE defaults to NULL. ALMMSG defaults to \“Env Alarm Input 1\”.

1.8.4 Equipment

Table 1-9 lists the default equipment values that are applied by the system when they are not explicitly specified during equipment provisioning.

Table 1-9 Equipment Default Values

Commands	Parameter Default
ALW-SWTOPROTN-EQPT, INH-SWTOPROTN-EQPT, ALW-SWTOWKG-EQPT, and ING-SWTOWKG-EQPT	DIRN defaults to BTH.
ENT-EQPT	PROTID, PRTYPE, RVRTV, and RVTM default to NULL.
SW-DX-EQPT	MODE defaults to NORM.
SW-TOPROTN-EQPT and SW-TOWKG-EQPT	MODE defaults to NORM. DIRN defaults to BTH.

1.8.5 Performance

Table 1-10 lists the default performance values that are applied by the system when they are not explicitly specified during performance provisioning.

Table 1-10 Performance Default Values

Commands	Parameter Default
INIT-REG-<MOD2>	LOCN defaults to NEND (near end).
RTRV-PM-<MOD2>	LOCN defaults to NEND. TMPER defaults to 15 minutes.
RTRV-TH-<MOD2>	MONTYPE defaults to CVL for OCN, EC1, and DSN. MONTYPE defaults to ESP for STSp. MONTYPE defaults to UASV for VT1. MONTYPE defaults to AISSP for the DS1 layer of the DS3XM card. LOCN defaults to NEND. TMPER defaults to 15 minutes.

Table 1-10 Performance Default Values (continued)

Commands	Parameter Default
SET-PMMODE-<STS_PATH>	PMSTATE defaults to ON.
SET-TH-<MOD2>	LOCN defaults to NEND. TMPER defaults to 15 minutes.

1.8.6 Ports

Table 1-11 lists the default port values that are applied by the system when they are not explicitly specified during port provisioning.

Table 1-11 Port Default Values

Ports	Parameter Default
OC-N Line	DCC defaults to N. TMGREF defaults to N. SYNCMSG defaults to Y. SENDDUS defaults to N. PJMON defaults to 0. SFBER defaults to 1E-4. SDBER defaults to 1E-7. MODE defaults to SONET. PST defaults to OOS.
EC1 Line	PJMON defaults to 0 (zero) LBO defaults to 0-225 RXEQUAL is Y PST defaults to defaults to OOS
T1 Line (DS1/DS1N)	LINECDE defaults to AMI. FMT defaults to D4. LBO defaults to 0-133. PST defaults to OOS.
T3 Line (DS3, DS3E, DS3NE, DS3XM)	DS3/T3 LINECDE defaults to 0-225. DS3 PST defaults to OOS. DS3E/DS3NE FMT defaults to UNFRAMED. DS3E/DS3NE LINECDE defaults to B3ZS. DS3E/DS3NE LBO defaults to 0-225. DS3 of DS3XM PST defaults to OOS.

1.8.7 SONET Line Protection

Table 1-12 lists the default SONET line protection values that are applied by the system when they are not explicitly specified during SONET line protection provisioning.

Table 1-12 SONET Line Protection Default Values

Commands	Parameter Default
EX-SW-<OCN>	ST (switch type) is optional and for BLSR protection switches only. ST defaults to BLSR RING switch type.
OC-N Line Protection	PROTID defaults to the protecting port of the protection group (SLOT-#(OCN)PORT-#). It is a string that can have a maximum length of 32 characters RVRTV defaults to N (nonrevertive mode). RVTM defaults to 5.0 minutes. PSDIRN defaults to UNI.
OPR-PROTNSW-<OCN>	ST is optional and for BLSR protection switches only. ST defaults to BLSR RING switch type.

1.8.8 STS and VT Paths

Table 1-13 lists the default STS and VT path values that are applied by the system when they are not explicitly specified during STS and VT path provisioning.

Table 1-13 STS and VT Paths Default Values

STS and VT Paths	Parameter Default
STS Path	SFBER, SDBER, RVRTV, and RVTM apply to path protection STS paths only. • SFBER defaults to 1E-4. • SDBER defaults to 1E-6. • RVRTV defaults to N. • RVTM defaults to empty because RVRTV is N when the path protection STSp is created. J1 is implemented on DS1, DS1N, DS3, DS3E, DS3NE, DS3XM, EC1, OC3, OC48AS, and OC192 cards. TRCMODE defaults to the OFF mode. EXPTRC defaults to a copy of the provisioned string or NULL when TRCMODE is OFF. EXPTRC defaults to the user-entered string when TRCMODE is MANUAL. EXPTRC defaults to a copy of the acquired received string or NULL if the string has not been acquired when TRCMODE is AUTO. INCTRC defaults to the incoming string (NULL) when TRCMODE is OFF. INCTRC defaults to a copy of the received string or NULL if the string has not been received when TRCMODE is MANUAL or AUTO.
VT Path	RVRTV and RVTM apply to path protection VT paths only. • RVRTV defaults to N. • RVTM defaults to empty because RVRTV is N when the path protection VT1 is created.

1.8.9 Synchronization

Table 1-14 lists the default synchronization values that are applied by the system when they are not explicitly specified during synchronization provisioning.

Table 1-14 Synchronization Default Values

Synchronization	Parameter Default
BITS	LINECDE defaults to B8ZS. FMT defaults to ESF. SYNCMSG defaults to Y. PST defaults to OOS.

Table 1-14 Synchronization Default Values (continued)

Synchronization	Parameter Default
NE-SYNCN	TMMDE defaults to EXTERNAL. SSMGEN defaults to GEN1. QRES defaults to SAME-AS-DUS. RVRTV defaults to Y. RVTM defaults to 5.0 minutes.
SYNCN	PRI/SEC QREF defaults to PRS. PRI STATUS defaults to ACT. SEC STATUS defaults to STBY. THIRD QREF defaults to ST3. STATUS defaults to STBY.

1.8.10 Testing

Table 1-15 lists the default testing values that are applied by the system when they are not explicitly specified during testing provisioning.

Table 1-15 Testing Default Values

Commands	Parameter Default
OPR-LPBK	LPBKTYPE defaults to FACILITY.
RLS-LPBK	LPBKTYPE defaults to current existing loopback type.

1.9 Parameter Types

This section provides a description of all message parameter types defined for the TL1 messages used in ONS 15310-MA, ONS 15454, ONS 15454 M2, and ONS 15454 M6. Individual parameters are listed within each command description.

1.9.1 ATAG Description

The ATAG is used for message sequencing. There are four streams of autonomous messages and each stream corresponds to a sequence. The sequence numbers increment by one for each autonomous message within that stream. The format and range of ATAG differs for each stream. The four streams are:

1. Alarmed events: These include REPT ALM and REPT EVT (except REPT EVT SESSION) messages as well as the REPT SW autonomous message.

ATAG format: x.y
where:
x is the sequence number of this alarmed event. This is an integer in the range of 0 to 9999.
y is the sequence number of the previous alarmed event that is related to this alarmed event. This is an integer in the range of 0 to 9999.

If there is no such previous related event, then y will be the same as x. For example, the first time an alarm is raised you will receive the autonomous message:

```
TID-000 1998-06-20 14:30:00
* 1346.1346 REPT ALM T1
"FAC-1-1:MN,LOS,NSA,,,,:\"Loss Of Signal\",DS1-14"
;
```

When this alarmed event/condition is cleared, you will receive the autonomous message:

```
TID-000 1998-06-20 14:31:00
A 1349.1346 REPT ALM T1
"FAC-1-1:CL,LOS,NSA,,,,:\"Loss Of Signal\",DS1-14"
;
```

2. Database change messages: The REPT DBCHG message falls into this category.

   ATAG format: x
   where:
   x is the sequence number of the database change update message. This is an integer in the range of 0 to 9999.

   For example:

```
TID-000 1998-06-20 14:30:00
A 96 REPT DBCHG
"TIME=18-01-05,DATE=1970-01-01,SOURCE=2,USERID=CISCO15,
DBCHGSEQ=96:ENT-EQPT:SLOT-3"
;
```

Note The ATAG is the same as the DBCHGSEQ field in the REPT DBCHG output.

3. Performance monitoring (PM) reports: The REPT PM messages fall into this category.

   ATAG format: x
   where:
   x is the sequence number of the PM report. This is an integer in the range of 0 to 9999.

   For example:

```
TID-000 1998-06-20 14:30:00
A 5 REPT PM DS1
"FAC-3-1:CVL,10,PRTL,NEND,BTH,15-MIN,05-25,14-46"
;
```

   This sequence number is global across all existing PM schedules.

4. Autonomous messages specific to a TL1 session: These messages are usually related to the security aspect of the TL1 session. Only the autonomous messages REPT EVT SESSION and CANC fall under this category.

   ATAG format: x
   where:
   x is the sequence number of the message. This is an integer in the range of 0 to 9999.

   For example:

```
 TID-000 1998-06-20 14:30:00
A 1 CANC
"User"
;
```

1.9.2 CTAG Description

The CTAG is included in each command by the user and is repeated by the NE in the response to allow the user to associate the command and response messages. The valid values for a CTAG are strings of up to 6 characters composed of identifiers (alphanumeric, beginning with a letter) or nonzero decimal numbers (a string of decimal digits with an optional nontrailing period).

A zero in the response field is valid when indicating an error; for example, issuing a semicolon by itself results in:

```
   TID-000 1998-06-20 14:30:00
M 0 DENY IISP
   /* Input, Garbage */
;
```

1.9.3 TID Description

The TID is the name of the NE where the command is addressed. TID is the Telcordia name for the system.

1.9.4 Parameter Notes

The following list contains general notes that apply to parameters:

- If a parameter is set to a value that is inconsistent with something already in the database and that value is not changed to a consistent value, then the command will be denied.
- If a parameter is set to a value that is consistent with what is already in the database, but another parameter in the same command is incompatible, then the command will be denied.
- The correct way to issue a command where parameters might be in conflict is to:
  - Issue that command and change all relevant parameters to compatible values.
  - Issue the command again to change the target values.
- The default values for command attributes can be seen using the RTRV commands, provided they are not altered by a provisioning command.
- The default for an optional field of an ED command is either the provisioned default value or the last provisioned value in the previous ED command.

CHAPTER 2

Procedures and Provisioning

Note The terms "Unidirectional Path Switched Ring" and "UPSR" may appear in Cisco literature. These terms do not refer to using Cisco ONS 15xxx products in a unidirectional path switched ring configuration. Rather, these terms, as well as "Path Protected Mesh Network" and "PPMN," refer generally to Cisco's path protection feature, which may be used in any topological network configuration. Cisco does not recommend using its path protection feature in any particular topological network configuration.

This chapter provides TL1 procedures and provisioning for the Cisco ONS 15310-MA, Cisco ONS 15454, Cisco ONS 15454 M2, and Cisco ONS 15454 M6.

2.1 Setting up TL1 Communication

The period during which a user is logged into the node is called a session. There are three options you can use to open a session (login):

- Cisco Transport Controller (CTC)
- Telnet
- Craft interface

The TL1 password identifier (PID) is masked when accessing a TL1 session using any of these options. When you log out of any of these options, you are closing a session. The ONS 15454, ONS 15454 M2, and ONS 15454 M6 allow a maximum of 20 (19 Telnet sessions and one craft session) concurrent TL1 sessions using any one or any combination of the options listed above. The ONS 15310-MA support a maximum of 20 (18 Telnet sessions and two craft sessions) concurrent TL1 sessions on the customer access panel (CAP). For information about issuing commands to multiple nodes, see the "2.3 TL1 Gateway" section on page 2-24.

Use the following procedures to open a TL1 session through the CTC, Telnet, or craft interface. In the procedures, the Activate and Cancel User commands are shown in their input format. For more information about these and other commands and messages, refer to the *Cisco ONS SONET TL1 Command Guide*.

Open a TL1 Session Through CTC

Step 1 From the PC connected to the ONS node, start Netscape or Internet Explorer.

Step 2 Enter the IP address of the node that you want to communicate with in the Netscape or Internet Explorer Web address (URL) field.

Step 3 Log into the CTC. The IP address on the title bar should match the IP address of the node that you entered in Step 2.

Step 4 When you are logged into CTC, there are two ways to open a TL1 session:

- Click **Tools > Open TL1 Connection**.
- Click the **Open TL1 Connection** button  on the toolbar.

Step 5 From the Select Node dialog box, choose the node that you want to communicate with.

Step 6 Click **OK**.

A TL1 interface window appears. There are three subwindows in the TL1 interface window: Request History, Message Log/Summary Log, and TL1 request. Type commands in the TL1 request window. You will see responses in the Message log window. The Request History window allows you to recall previous commands by double-clicking them.

Step 7 Verify that the Connect button is selected (grayed out).

Step 8 Type the Activate User command in the TL1 request window to open a TL1 session:

ACT-USER:[<TID>]:<UID>:<CTAG>::<PID>;

Step 9 Press **Enter**.

Note You must press Enter after the semicolon in each TL1 command, or the command will not be issued.

Step 10 Type the Cancel User command in the TL1 request window or press the **Disconnect** button to close a TL1 session:

CANC-USER:[<TID>]:<USERID>:<CTAG>;

Step 11 Press **Enter**.

Open a TL1 Session Through Telnet

To communicate with the ONS network element (NE) using TL1 commands through a Telnet session over a craft interface or a LAN connection, you can choose from two ports:

- Port number 3083 is a Telnet port that uses the Telnet protocol and associated Telnet escape sequences.
- Port number 2361 is an alternative Telnet port.

Note Port number 3082 is a raw TCP/IP port; it is not an interactive port and is not recommended for use as an alternate telnet port.

Step 1 At the DOS prompt, type **cmd** and press **Enter**. (The same steps can also be done from a UNIX prompt).

Step 2 At the DOS command prompt type:

Telnet <Node IP Address or Node Name> <Port Number> and press **Enter**.

The Node IP address or Node Name refers to the IP address or Node Name of the node you want to communicate with. Port number is the port (2361 or 3083) where TL1 commands are understood. If the connection is successful, a screen appears with a prompt.

Step 3 Type the Activate User command to open a TL1 session:

ACT-USER:[<TID>]:<UID>:<CTAG>::<PID>;

Note When the semicolon is typed, the command is issued immediately.

Step 4 Type the Cancel User command to close a TL1 session:

CANC-USER:[<TID>]:<USERID>:<CTAG>;

Open a TL1 Session Through a Craft Interface (Cisco ONS 15310-MA, Cisco ONS 15454, Cisco ONS 15454 M2, and Cisco ONS 15454 M6)

The TCC2/TCC2P/TCC3, XTC, and CTX2500 cards have two built-in interface ports for accessing the ONS 15454 and ONS 15310-MA respectively. With one RJ-45 LAN connection, you can access the system using a standard browser interface. In the browser interface, you can perform local and remote Operation, Administration, Maintenance, and Provisioning (OAM&P) functions and open a VT100 emulation window to enter TL1 commands. If a browser is not available, you can access the system using a nine-pin EIA/TIA-232 port. The EIA/TIA-232 port supports VT100 emulation such that TL1 commands can be entered directly without a browser. The ONS 15310-MA has two EIA/TIA-232 ports.

Step 1 Connect the serial cable to the EIA/TIA-232 port on the active TCC2/TCC2P/TCC3, XTC, or CTX2500 card.

Step 2 Configure the terminal emulation software (HyperTerminal):

- Terminal emulation = **vt100**
- Bits per second = **9600**

- Parity = **None**
- Stop BITS = **1**
- Flow control = **None**

Step 3 Press **Enter**. An angle bracket prompt (>) appears.

Step 4 At the > prompt, type the Activate User command to open a TL1 session:

ACT-USER:[<TID>]:<UID>:<CTAG>::<PID>;

Note When the semicolon is typed, the TL1 command is issued immediately.

Step 5 Type the Cancel User command to close a TL1 session:

CANC-USER:[<TID>]:<USERID>:<CTAG>;

2.2 Test Access

Note Test access applies to the ONS 15310-MA, ONS 15454, ONS 15454 M2, and ONS 15454 M6.

Note Refer to the *Cisco ONS SONET TL1 Command Guide* for complete command and autonomous message information.

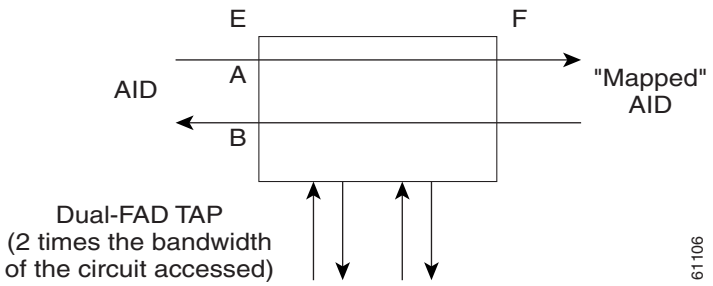
The test access (TACC) feature allows a third-party Broadband Remote Test Unit (BRTU) to create nonintrusive test access points (TAPs) to monitor the circuits on the ONS 15310-MA, ONS 15454, ONS 15454 M2, and ONS 15454 M6 for errors. The test access feature also allows the circuit to be split (intrusive), so that the transmission paths can be tested for bit errors through the use of various bit test patterns. The two BRTUs supported by the ONS 15310-MA, ONS 15454, ONS 15454 M2, and ONS 15454 M6 are the Hekimian/Spirent BRTU-93 (6750) and the TTC/Acterna Centest 650.

The test access functionality provides TL1 commands for creating and deleting TAPs, connecting or disconnecting TAPs to circuit cross-connects, and changing the mode of test access on the ONS 15310-MA, ONS 15454, ONS 15454 M2, and ONS 15454 M6. To view test access information in CTC, in node view click the **Maintenance > Test Access** tabs.

Refer to Telcordia document GR-834-CORE, *Network Maintenance: Access and Testing* and GR-1402-CORE, *Network Maintenance: Access Testing - DS3 HCDS TSC/RTU and DTAU Functional Requirements* for more information about test access.

A TAP provides the capability of connecting the circuit under test to a BRTU. This connection initially provides in-service monitoring capability to permit the tester to determine that the circuit under test is idle. The monitor connection should not disturb the circuit under test. The access point and remote test unit (RTU) also provide the capability of splitting a circuit under test. A split consists of breaking the transmission path of the circuit under test. This is done out of service. The two sides of the access point are called the Equipment (E) and Facility (F) directions. For a 4-wire or 6-wire circuit, the transmission pairs within the access point are defined as the A and B pairs. The circuit under test should be wired into the access point so that the direction of transmission on the A pair is from E to F, and the transmission direction for the B pair is from F to E (Figure 2-1).

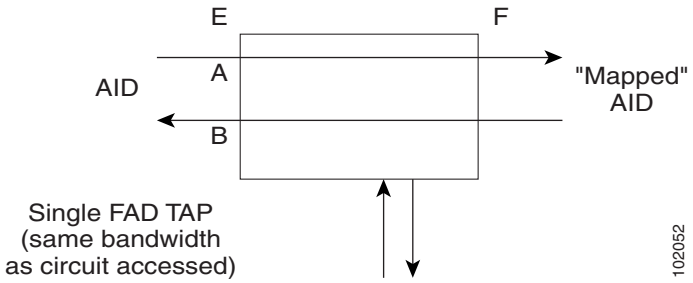
Figure 2-1 Circuit With No Access Dual FAD TAP



A dual facility access digroup (FAD) TAP uses twice the bandwidth of the circuit under test. This can be specified by the TAPTYPE parameter as shown in the ED-<MOD2> command syntax in the "2.2.2 TAP Creation and Deletion" section on page 2-6. The values are SINGLE and DUAL. It defaults to DUAL.

A single FAD TAP uses half the bandwidth as that of the dual FAD, that is, it uses the same bandwidth as the circuit accessed for the TAP creation. This can be specified by the TAPTYPE parameter as shown in the "2.2.2 TAP Creation and Deletion" section on page 2-6. The values are SINGLE and DUAL. The MONEF, SPLTAB, and SPLTEF modes are not supported by single FAD TAPs (Figure 2-2).

Figure 2-2 Circuit With No Access Single FAD TAP



2.2.1 Test Access Terminology

The terminology in Table 2-1 is used in conjunction with test access.

Table 2-1 Test Access Terminology

Term	Definition
BRTU	Broadband remote test unit
DFAD	Dual facility access digroup
FAD	Facility access digroup
FAP	Facility access path
LOOPE	Split/loop access on A and B paths equipment side
LOOPF	Split/loop access on A and B paths facility side
MONE	Monitor access with signal detector on A path

Table 2-1 Test Access Terminology (continued)

Term	Definition
MONF	Monitor access with signal detector on B path
MONEF	Monitor access with signal detector on A and B paths
QRS	Quasi-random signal (bit test pattern)
SPLTA	Split access on A path with signal detector from equipment, QRS on facility side
SPLTB	Split access on B path with signal detector from equipment, QRS on equipment side
SPLTE	Split access on A and B paths with signal detector from equipment, QRS on equipment side
SPLTF	Split access on A and B paths with signal detector from equipment, QRS on facility side
SPLTEF	Split access on A and B paths for testing in both equipment and facility directions
TACC	Test access
TAP	Test access path/point

The following path naming conventions apply to test access:

- E—Equipment test access point direction
- F—Facility test access point direction
- A—Transmission path (the direction of transmission on the A pair is from E to F)
- B—Transmission path (the transmission direction for the B pair is from F to E)

2.2.2 TAP Creation and Deletion

TL1 supports commands to create, delete, connect, change, retrieve, and disconnect TAPs.

2.2.2.1 ED-<rr>

The edit command (ED-<rr>) is used to change an existing port, synchronous transport signal (STS), or Virtual Tributary (VT) to a TAP.

Note <rr> indicates one of the following parameters: **T1, T3, STS1, STS3c, STS6c, STS9c, STS12c, STS24c, STS48c, STS192c, VT1, DS1.**

Input Format:

ED-(T1, T3, STS1, STS3c, STS6c, STS9c, STS12c, STS24c, STS48c, STS192c, VT1, DS1):[<TID>]:<AID>:<CTAG>[:::TACC=<TACC>][TAPTYPE=<TAPTYPE>];

Edit an existing port, STS, or VT and change it to a TAP so it can be used when requesting TACC connections. Includes a new optical parameter, TACC=n, that defines the port, STS, or VT as a TAP with a selected unique TAP number. This TAP number will be used when requesting test access connections to circuit cross-connections under test. The TAP creation will fail if there is a cross-connection already on the port, STS, or VT.

Note
- This command generates a REPT DBCHG message.

- The alarms and conditions on test access paths can be retrieved by the RTRV-ALM-ALL or RTRV-ALM-<MOD2> commands.
- The TAP is a persistent object. It will exist after the user has logged out of the TL1 session.

The following list applies to TAP numbers:

- The TAP number is an integer within the range of 1 to 999. When TACC=0 is specified, the TAP is deleted (if already present).
- The TAP number is unique across T1/T3/STS/VT/DS1 TAPs in the system.
- The TAP number is not editable.

2.2.2.2 ED-T1

When the ED-T1 command is issued with a specified TACC value for a given T1 port/facility, a dual facility access group (DFAD) is created by using the specified port/facility and the consecutive port/facility.

The command in Example 2-1 creates a DFAD on FAC-1-1 and FAC-1-2.

Example 2-1 Create a DFAD on FAC-1-1 and FAC-1-2

```
ED-T1::FAC-1-1:12:::TACC=1;

   DV9-99 1970-01-02 03:16:11
M 12 COMPLD
;
```

Note These ports/facilities cannot be used for the creation of cross-connects until the TAP is deleted.

2.2.2.3 ED-T3

When the ED-T3 command is issued with a specified TACC value for a given T3 port/facility, a DFAD is created by using the specified port/facility and the consecutive port/facility.

The command in Example 2-2 creates a T3 DFAD on FAC-2-1 and FAC-2-2.

Example 2-2 Create a T3 DFAD on FAC-2-1 and FAC-2-2

```
ED-T3::FAC-2-1:12:::TACC=2;

   DV9-99 1970-01-02 03:16:11
M 12 COMPLD
;
```

Note These ports/facilities cannot be used for the creation of cross-connects until the TAP is deleted.

2.2.2.4 ED-DS1

When the ED-DS1 command is issued with a specified TACC value for a given DS1 facility on a DS3XM card, a DFAD is created by using the specified facility and the consecutive port/facility.

The command in Example 2-3 creates DFAD on DS1-2-1-1 and DS1-2-1-2.

Example 2-3 Create a DFAD on DS1-2-1-1 and DS1-2-1-2

```
ED-DS1::DS1-2-1-1:12:::TACC=3;

   DV9-99 1970-01-02 03:16:11
M 12 COMPLD
;
```

Note These ports/facilities cannot be used for the creation of cross-connects until the TAP is deleted.

2.2.2.5 ED-STSn

When the ED-STSn command is issued for a TACC, it assigns the STS for the first two-way test access connection and STS+1 as the second two-way connection. For STS3c, STS9c, STS12c, STS24c, and STS48c, the next consecutive STS of same width is chosen. The TAP creation will fail if either of the consecutive STSs are not available.

The command in Example 2-4 creates a TAP on STS-5-1 and STS-5-2.

Example 2-4 Create a TAP on STS-5-1 and STS-5-2

```
ED-STS1::STS-5-1:12:::TACCC=4

   DV9-99 1970-01-02 03:16:11
M 12 COMPLD
;
```

Note These STSs cannot be used for the creation of cross-connects until the TAP is deleted.

The command in Example 2-5 creates an STS24c dual TAP on STS-6-1 and STS-6-25.

Example 2-5 Create an STS24c Dual TAP on STS-6-1 and STS-6-25

```
ED-STS24C::STS-6-1:12:::TACC=5:

   DV9-99 1970-01-02 03:16:11
M 12 COMPLD
;
```

Note These STSs cannot be used for the creation of cross-connects until the TAP is deleted.

2.2.2.6 ED-VT1

When the ED-VT1 command is issued for a TACC, a VT TAP is created. The specified VT access identifier (AID) is taken as the first VT connection. The second VT connection is made by incrementing the VT group and keeping the VT number the same.

The command in Example 2-6 creates a VT TAP on VT1-1-1-1-1 and VT1-1-1-2-1.

Example 2-6 Create a VT TAP on VT1-1-1-1-1 and VT1-1-1-2-1

```
ED-VT1-1-1-1-1:12:::TACC=6;

   DV9-99 1970-01-02 03:16:11
M 12 COMPLD
;
```

Note These VTs cannot be used for the creation of cross-connects until the TAP is deleted.

2.2.3 Connect Test Access Points

The connect test access points command (CONN-TACC-<rr>) is used to make a connection between the TAP and the circuit or cross-connect under test.

Note <rr> indicates one of the following parameters: **T1, T3, STS1, STS3c, STS6c, STS9c, STS12c, STS24c, STS48c, STS192c, VT1, DS1.**

Input Format:

CONN-TACC-(T1, T3, STS1, STS3C, STS6C, STS9C, STS12C, STS24C, STS48C, STS192c, VT1,DS1):[<TID>]:<AID>:<CTAG>::<TAP>:MD=<MD>;

Connect the port, STS, or VT defined by <AID> to the port, STS, or VT defined by the <TAP> number. The mode of test access to the circuit or cross-connect is specified by <MD>. The mode can be either monitor (nonintrusive), split (intrusive), or loop (intrusive) mode. The various modes are described in the "2.2.9 Test Access Mode Definitions" section on page 2-14.

Note The connection is maintained only for the duration of the TL1 session (nonpersistent).

Note The TAP number is displayed at the output if the CONN-TACC command completes successfully.

The following error codes are supported:

- RTBY—Requested TAP busy
- RTEN—Requested TAP does not exist
- SCAT—Circuit is already connected to another TAP
- SRCN—Requested condition already exists
- IIAC—Invalid access identifier (AID)
- EANS—Access not supported
- SRAC—Requested access configuration is invalid

The command in Example 2-7 creates a connection between TAP number one and the port/facility FAC-1-3 with the access mode defined as MONE. The various modes are described in the "2.2.9 Test Access Mode Definitions" section on page 2-14.

Example 2-7 Create a Connection Between TAP 1 and FAC-1-3

```
CONN-TACC-T1::FAC-1-3:12::1:MD=MONE;

   DV9-99 1970-01-02 02:51:54
M 12 COMPLD
   1
;
```

2.2.4 Change Access Mode

The change access mode command (CHG-ACCMD-<rr>) is used to change the access mode.

Note <rr> indicates one of the following parameters: **T1, T3, STS1, STS3c, STS6c, STS9c, STS12c, STS24c, STS48c, STS192c, VT1, DS1.**

Input Format:

CHG-ACCMD-(T1, T3, STS1, STS3C, STS6C, STS9C, STS12C, STS24C, STS96C, STS48C, STS192c, VT1, DS1):[<TID>]:<TAP>:<CTAG>::<MD>;

Use this command to change the type of test access. This might be a change from monitoring the data to inserting data into the STS. This command can only be applied to an existing TAP connection. If a TAP connection does not exist, a RTEN error is returned.

The following error codes are supported:

- SRCN—Requested condition already exists
- SRAC—Requested access configuration is invalid
- RTEN—Requested TAP does not exist

The command in Example 2-8 changes the access mode of TAP 1 to LOOPE.

Example 2-8 Change TAP 1 Access Mode to LOOPE

```
CHG-ACCMD-T1::1:12::LOOPE;

   DV9-9 1970-01-02 02:59:43
M 12 COMPLD
;
```

Note The access mode cannot be changed if the TAP is not connected.

Note This command generates a REPT DBCHG message.

2.2.5 Retrieve Test Access Point Information

The following sections retrieve TAP information using the RTRV-<rr> and RTRV-TACC commands. Refer to the *Cisco ONS SONET TL1 Command Guide* for specific command formats and examples.

2.2.5.1 RTRV-<rr>

The RTRV-<rr> command retrieves TAP information.

Note A generic ALL AID would behave similarly to an ALL AID such as SLOT-ALL or FAC-1-ALL for all the RTRV-<rr> commands that support a generic ALL AID.

Note <rr> indicates one of the following parameters: **T1, T3, STS1, STS3c, STS6c, STS9c, STS12c, STS24c, STS48c, STS192c, VT1, DS1.**

Input Format:

RTRV-(T1, T3, STS1, STS3C, STS6C, STS9C, STS12C, STS24C, STS48C, STS192c, VT1, DS1):[<TID>]:<AID>:<CTAG>;

This command is modified to include the return of a TAP number if the requested <AID> is defined as a TAP. An optional TACC=<TAPNUMBER> will appear in the output list if the requested <AID> is defined as a TAP. The example in Example 2-9 retrieves TAP information for FAC-1-1.

Example 2-9 Retrieve TAP Information for FAC-1-1

```
RTRV-T1::FAC-1-1:12;

   dv9-99 1970-01-02 02:49:16
M 12 COMPLD
   "FAC-1-1::LINECDE=AMI,FMT=D4,LBO=0-131,TACC=1,TAPTYPE=DUAL:OOS"
;
```

2.2.5.2 RTRV-TACC

The RTRV-TACC command can also be used to retrieve details associated with a TAP.

Input Format:

RTRV-TACC:[<TID>]:<TAP>:<CTAG>;

The TAP is identified by the TAP number. The ALL input TAP value means that the command will return all the configured TACCs in the NE. An example of the RTRV-TACC command is provided in Example 2-10.

Example 2-10 Retrieve Details for TAP 241

```
RTRV-TACC:CISCO:241:CTAG;

   TID-000 1998-06-20 14:30:00
M  001 COMPLD
"241:STS-2-1-1.STS-2-2,MONE,STS-12-1-1,STS-13-1-1"
;
```

2.2.6 Disconnect Test Access Points

TAPs can be disconnected in the following ways:

- Issue the DISC-TACC command.
- Delete or modify the accessed connection.
- Drop the TL1 session for any reason, including logout or a dropped Telnet session.
- Switch or reset a TCC2/TCC2P or XTC card.

The disconnect TAP (DISC-TACC) command disconnects the TAP and puts the connection back to its original state (no access).

Input Format:

DISC-TACC:[<TID>]:<TAP>:<CTAG>;

The command in Example 2-11 disconnects TAP 1 from the circuit/cross-connect under test.

Example 2-11 Disconnect TAP 1 from the Circuit/Cross-Connect Under Test

```
DISC-TACC::1:12;

   DV9-99 1970-01-02 02:59:43
M 12 COMPLD
;
```

Note This command generates a REPT DBCHG message.

The following error codes are supported:

- SADC—Already disconnected
- SRTN—Unable to release TAP

2.2.7 Delete Test Access Points

To delete a TAP, issue the edit TAP command with the TACC set to zero.

Input Format:

ED-<STS_PATH>:[<[TID>]:<AID>:<CTAG>:::TACC=0:;

Note The TACC number must be set to zero in order to delete a TAP.

Note If a TAP is not removed, the STS bandwidth will be stranded.

2.2.8 Test Access Configurations

This section shows single node (Figure 2-3) and multinode (Figure 2-4) test access configurations.

Use the following commands to configure test access:

Step 1 **ED-STS1::STS-1-1-1:90:::TACC=1;**

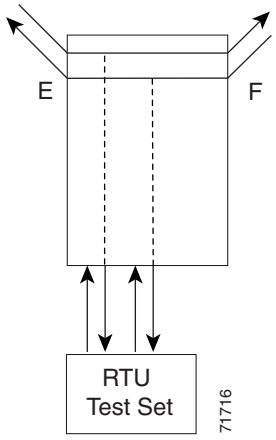
This command changes STS1 and STS2 on Slot 1 to a TAP. The CTAG is 90. It sets the TACC number to 1.

Step 2 **CONN-TACC-STS1::**<AID for E or F depending on MD>**:91::1:MONE**

This command connects the <AID> to the TACC defined by TAP 1 on the E side. The CTAG is 91.

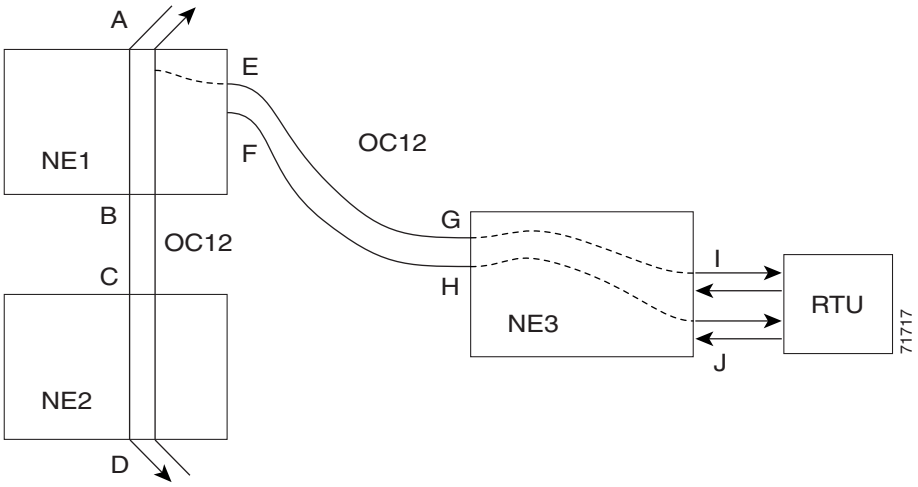
Note The connection made in the CONN-TACC command can use MONE to connect to the F side AID. The AID provided designates the E side and the other automatically becomes the F side. For example, if an <AID F> is supplied to a MONE connection, then the top line would be connected to the other side of the path, or what is shown in Figure 2-3 as the F side. When a CONN-TACC is set up, these designations cannot change until a DISC-TACC or another CONN-TACC command is executed. The connection is based on the AID supplied.

Figure 2-3 Single Node View (Node 1)



In the Figure 2-3 configuration, there might be a single DS-3 port wired up, configured as 14 dual FADs (28 VTs).

Figure 2-4 Multinode View (MONE Example)



The following commands are performed on NE3:

ENT-CRS-STS1::<AID I-G>:100::2WAY;

A connection, not a TAP. CTAG is 100.

ENT-CRS-STS1::<AID J-H>:101::2WAY;

Second connection, not a TAP.

The following commands are performed on NE1:

Assuming the path from A to B is already entered, the A and B points in Figure 2-4 refer to entry and exit points on the node or different cards. The E/F designators refer to the two-way connections from NE3.

The following command creates a TAP with STS-1-1 and STS-1-2 through NE1. TAP number assigned is 4.

ED-STS1::STS-1-1:TACC=4;

The following command connects TAP 4 to the circuit:

CONN-TACC-STS1::<AID A or B>:102::4:<MD>

Note The I and J connections above are TAPs in Figure 2-3, but normal connections in the Figure 2-4.

2.2.9 Test Access Mode Definitions

The following diagrams show what the different test access modes (<MD>) refer to. Figure 2-5 shows a circuit with no access (dual FAD TAP) and Figure 2-6 shows a circuit with no access (single FAD TAP). The subsections that follow show the circuits in each test access mode. The QRS can be generated by an outside source, for example, the empty connection of the BRTU.

The subsections that follow describe the modes:

MONE, MONF, and MONEF access modes are Non-Service Affecting and can be applied to an In Service (IS) port state.

LOOPE, LOOPF, SPLTE, SPLTF, SPLTEF, SPLTA, SPLTB, and SPLTAB access modes are intrusive and can be applied only to a circuit or /port that is in the Out Of Service, Maintenance (OOS_MT) port state. The NE will change the state of the circuit under test to OOS_MT during the period of TACC and restore it to the original state when the connection between the TAP and the circuit is dropped.

Figure 2-5 Circuit With No Access (Dual FAD TAP)

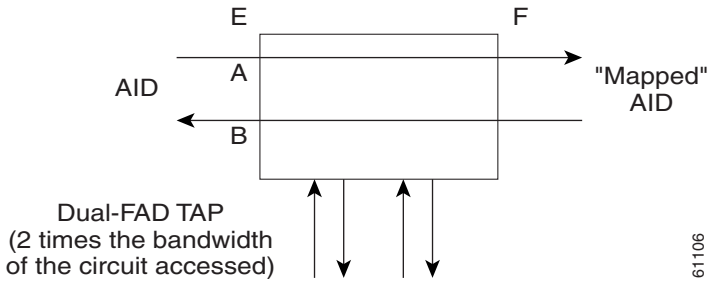
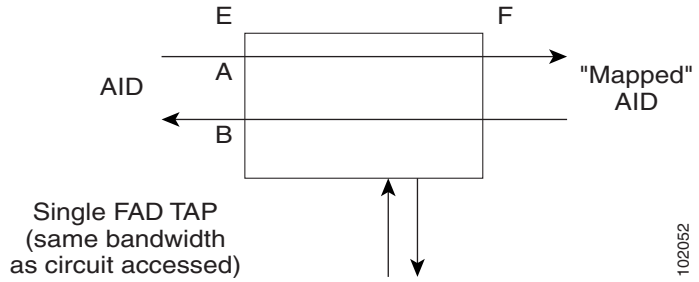


Figure 2-6 Circuit With No Access (Single FAD TAP)



2.2.9.1 MONE

Monitor E (MONE) mode indicates a monitor connection provided from the FAD to the A transmission path of the accessed circuit (Figure 2-7 and Figure 2-8). This is a nonintrusive mode.

Figure 2-7 MONE Access Mode Single TAP

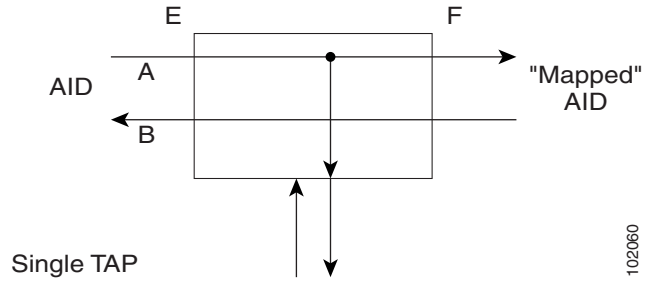
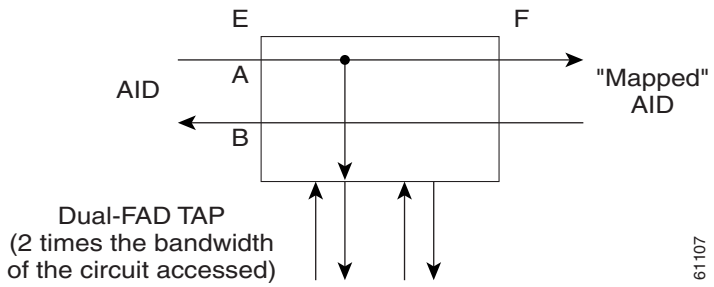


Figure 2-8 MONE Access Mode Dual TAP



2.2.9.2 MONF

Monitor F (MONF) mode indicates that the FAD is providing a monitor connection to the B transmission path of the accessed circuit (Figure 2-9 and Figure 2-10). This is a nonintrusive mode.

Figure 2-9 MONF Access Mode Single TAP

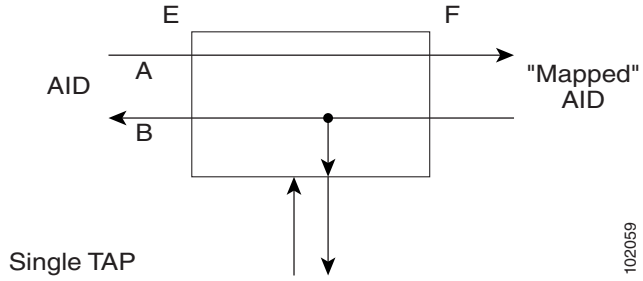
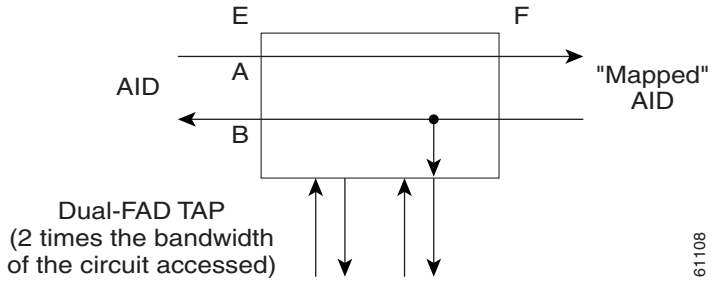


Figure 2-10 MONF Access Mode Dual TAP



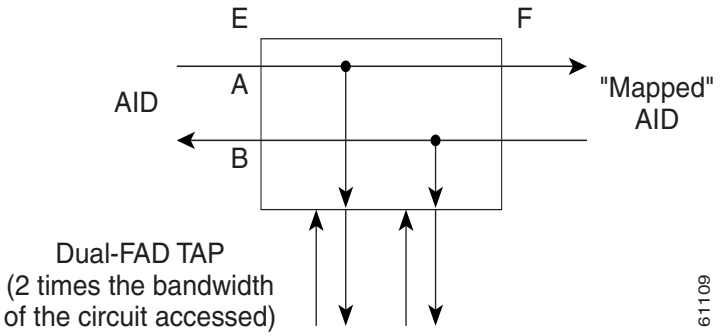
Note The MONE and SPLTA modes are applicable to unidirectional circuits from E to F. The MONF and SPLTB modes are applicable to unidirectional circuits from F to E.

2.2.9.3 MONEF

Monitor EF (MONEF) mode is a monitor connection provided from the FAD1 (odd pair) to a DFAD, to the A transmission path, and from FAD2 (even pair) of the same DFAD, to the B transmission path of the accessed circuit. This is a nonintrusive mode (Figure 2-11).

MONEF mode for T3 (DS3 high capacity digital service [HCDS]) indicates that the odd pair of an FAP is providing a monitor connection to the A transmission path and from the even pair of an FAP to the B transmission path of the accessed circuit.

Figure 2-11 MONEF Access Mode Dual TAP



2.2.9.4 SPLTE

Split E (SPLTE) mode splits both the A and B paths and connects the E side of the accessed circuit to the FAD (Figure 2-12 and Figure 2-13).

Note QRS is not supported on the ONS 15454. The connection will remain as is.

Figure 2-12 SPLTE Access Mode Single TAP

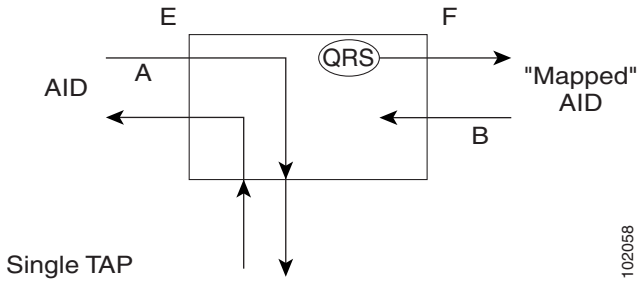
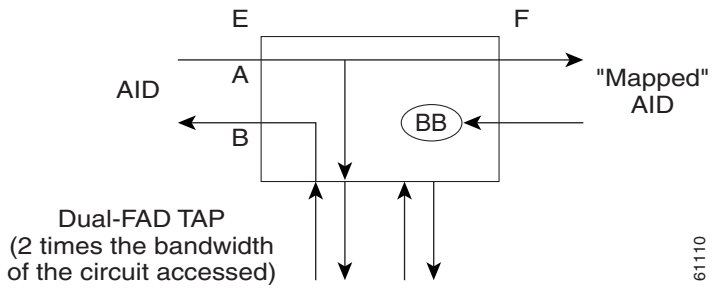


Figure 2-13 SPLTE Access Mode Dual TAP



2.2.9.5 SPLTF

Split F (SPLTF) mode splits both the A and B paths and connects the F side of the accessed circuit to the FAD (Figure 2-14 and Figure 2-15).

Note QRS is not supported on the ONS 15454. The connection will remain as is.

Figure 2-14 SPLTF Access Mode Single TAP

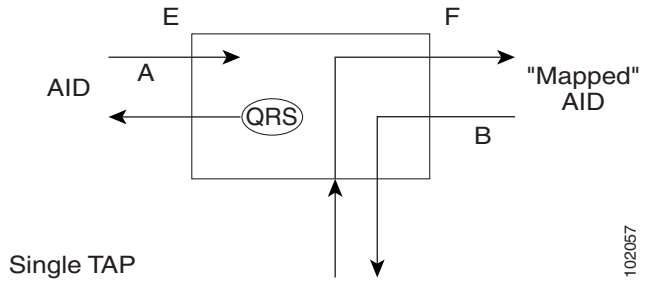
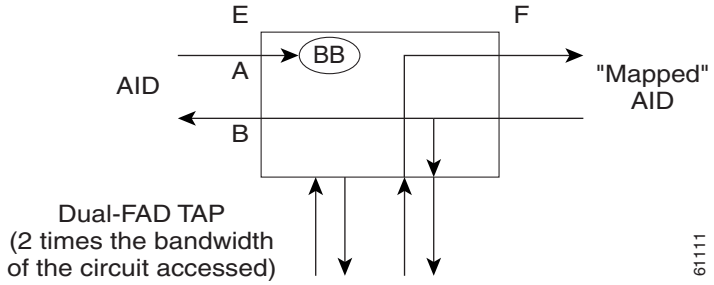


Figure 2-15 SPLTF Access Mode Dual TAP

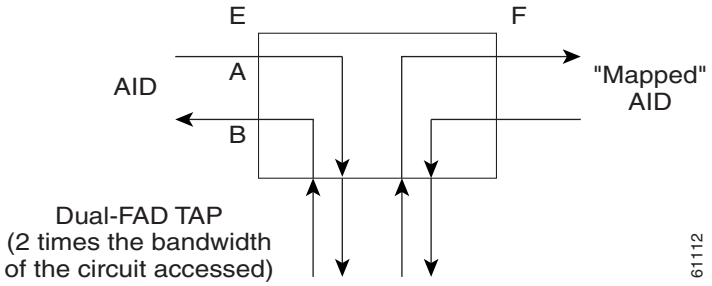


2.2.9.6 SPLTEF

Split EF (SPLTEF) mode for T1 (DS1 HCDS) splits both the A and B paths, connects the E side of the accessed circuit to FAD1 and the DFAD pair, and connects the F side to the FAD2 of the same DFAD pair (Figure 2-16).

SPLTEF mode for T3 (DS3 HCDS) splits both the A and B paths and connects the E side of the accessed circuit to the odd pair of the FAP and the F side to the even pair of the FAP.

Figure 2-16 SPLTEF Access Mode Dual TAP



2.2.9.7 LOOPE

Loop E (LOOPE) mode splits both the A and B paths, connects the incoming line from the E direction to the outgoing line in the E direction, and connects this looped configuration to the FAD (Figure 2-17 and Figure 2-18). Loop E and F modes are basically identical to the SPLT E and F modes except that the outgoing signal is the incoming signal and not the signal from the remote test unit (RTU).

Note QRS is not supported on the ONS 15454. The connection will remain as is.

Figure 2-17 LOOPE Access Mode Single TAP

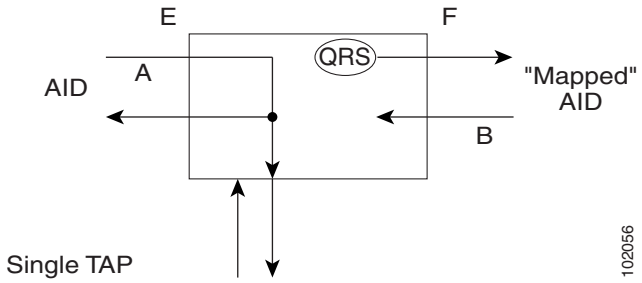
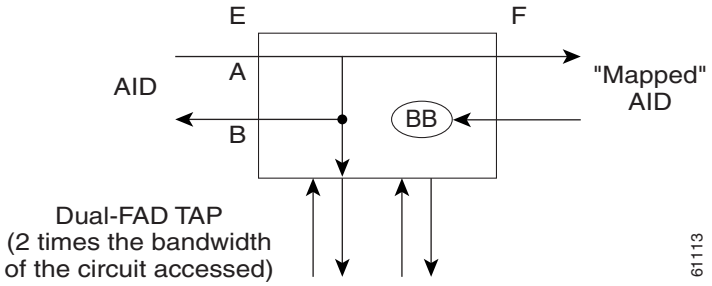


Figure 2-18 LOOPE Access Mode Dual TAP



2.2.9.8 LOOPF

Loop F (LOOPF) mode splits both the A and B paths, connects the incoming line from the F direction to the outgoing line in the F direction and connects this looped configuration to the FAD (Figure 2-19 and Figure 2-20).

Note QRS is not supported on the ONS 15454. The connection will remain as is.

Figure 2-19 LOOPF Access Mode Single TAP

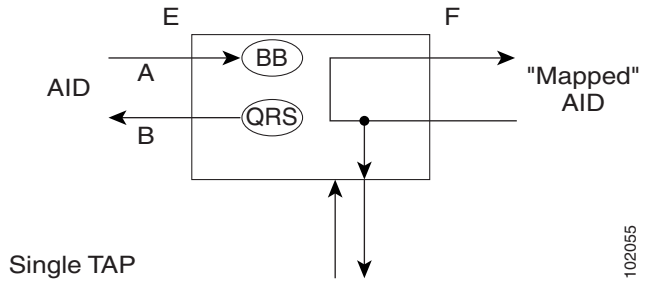
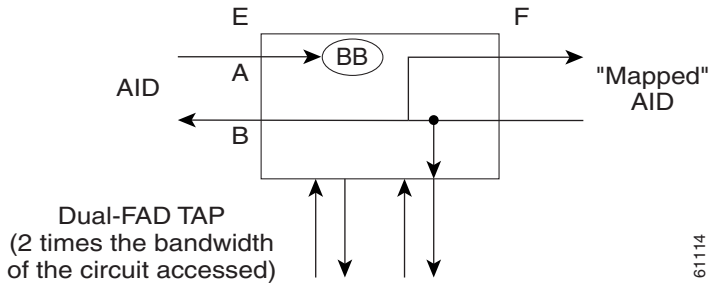


Figure 2-20 LOOPF Access Mode Dual TAP



2.2.9.9 SPLTA

Split A (SPLTA) mode indicates that a connection is provided from both the E and F sides of the A transmission path of the circuit under test to the FAD and splits the A transmission path (Figure 2-21 and Figure 2-22). This mode is similar to the SPLTE and SPLTF modes, except the signals are sent to the RTU, not the NE signal configuration.

Figure 2-21 SPLTA Access Mode Single TAP

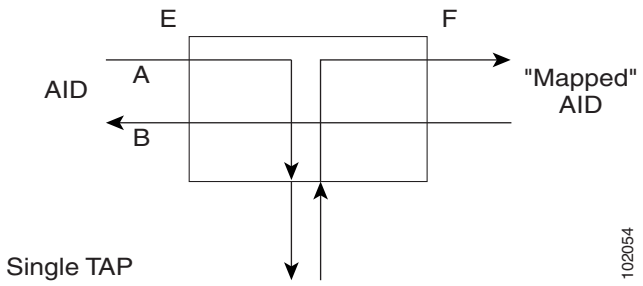
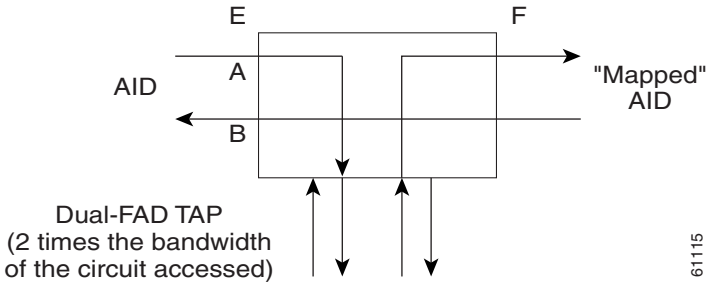


Figure 2-22 SPLTA Access Mode Dual TAP



2.2.9.10 SPLTB

Split B (SPLTB) mode indicates that a connection is provided from both the E and F sides of the B transmission path of the circuit under test to the FAD and splits the B transmission path (Figure 2-23 and Figure 2-24).

Figure 2-23 SPLTB Access Mode Single TAP

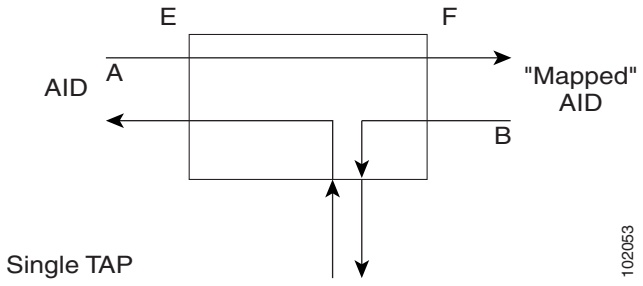
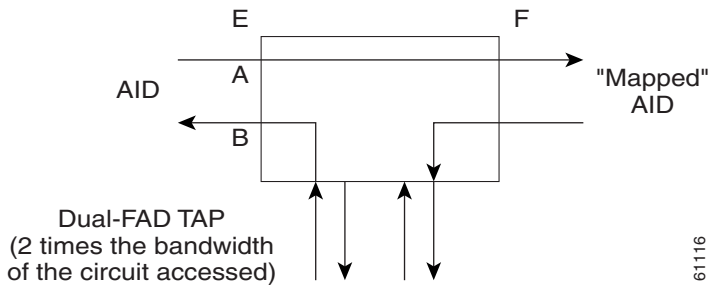


Figure 2-24 SPLTB Access Mode Dual TAP



2.2.10 Unmapped AID Test Access Point Connections

The ONS 15454, ONS 15454 M2, and ONS 15454 M6 support connections to unmapped AIDs (unmapped circuits). The TAPs can be connected to an unmapped AID, for example, an AID that does not have a cross-connect on it. The access modes supported are: MONE, SPLTE, and LOOPE.

Example 2-12 creates a TAP on STS-5-1 and STS-5-2.

Example 2-12 Create a TAP on STS-5-1 and STS-5-2

```
ED-STS1::STS-5-1:12:::TACC=1;

   DV9-99 1970-01-02 03:16:11
M 12 COMPLD
;
```

Example 2-13 creates an unmapped AID connection with the MONE access mode.

Example 2-13 Create an Unmapped AID Connection with the MONE Access Mode

```
CONN-TACC-STS1::STS-5-3:12::1:MD=MONE;

   DV9-99 1970-01-02 02:51:54
M 12 COMPLD
   1
;
```

Note STS-5-3 does not have a cross-connect on it. STS-5-3 becomes unusable until the connection is disconnected by the DISC-TACC command.

Note The <AID> provided in the CONN-TACC command designates the E side and the other automatically becomes the F side.

Note In the case of all one-way circuits (1-way, UPSR_HEAD, UPSR_DROP, UPSR_DC, UPSR_EN), if the <AID> specified is the source AID, the direction is designated as From E in Table 2-2 on page 2-24. If the <AID> specified is the destination AID or the drop side, the direction is designated as From F in Table 2-2 on page 2-24.

2.2.10.1 One-Way Circuit

The examples in this section assume that an STS TAP is already created with a TAP number of 1.

ENT-CRS-STS1::STS-5-1,STS-5-2:12::1WAY;
DV9-99 1970-07-01 20:29:06
M 12 COMPLD;

CONN-TACC-STS1::STS-5-1:12::1:MD=MONF;
DV9-99 1970-01-01 20:29:47
M 12 DENY
EANS
STS-5-1
/*INCORRECT TAP MODE*/

The <AID> specified in the above CONN-TACC command is the source AID for the one-way circuit. In this case, only MONE and SPLTA modes are allowed because there is no B path in the case of a one-way circuit (see Table 2-2 on page 2-24).

CONN-TACC-STS1::STS-5-1:12::1:MD=MONE;
DV9-99 1970-01-01 20:30:09
M 12 COMPLD

DISC-TACC::1:12;
DV9-99 1970-01-01 20:30:20
M 12 COMPLD
;

However, if the AID specified is the destination AID, as shown below, the modes allowed are MONF and SPLTB.

CONN-TACC-STS1::STS-5-2:12::1:MD=MONF;
DV9-99 1970-01-01 20:30:32
M 12 COMPLD

Note

- The same examples apply for UPSR_HEAD, UPSR_DROP, UPSR_DC and UPSR_EN, which are all one-way circuits.
- The connections are made only to the working path, irrespective of which path is currently active.

2.2.10.2 Two-Way Circuits

For two-way circuits, all the modes are allowed, as shown in Table 2-2. The same applies for UPSR_UPSR and path protection circuit types. In the case of UPSR_UPSR and path protection circuits, the working path is connected irrespective of which path is currently active.

2.2.10.3 Unmapped AID

As explained in the "2.2.10 Unmapped AID Test Access Point Connections" section on page 2-22, connections can be made to an AID without a cross-connect on it. The modes supported are MONE, SPLTE, and LOOPE, as shown in Table 2-2.

Note The AID provided in the CONN-TACC command designates the E side and the other automatically becomes the F side.

Table 2-2 Modes Supported by Circuit Type

	MONE	MONF	MONEF	SPLTE	SPLTF	SPLTEF	LOOPE	LOOPF	SPLTA	SPLTB
1-way (from E)[1]	X	—	—	—	—	—	—	—	X	—
1-way (from F)[2]		X	—	—	—	—	—	—	—	X
2-way	X	X	X	X	X	X	X	X	X	X
Path Protection	X	X	X	X	X	X	X	X	X	X
UPSR_HEAD (from E)	X	—	—	—	—	—	—	—	X	
UPSR_HEAD (from F)	—	X	—	—	—	—	—	—	—	X
UPSR_DROP UPSR_DC UPSR_EN (from E)	X	—	—	—	—	—	—	—	X	—
UPSR_DROP UPSR_DC UPSR_EN (from F)	—	X	—	—	—	—	—	—	—	X
UPSR_UPSR	X	X	X	X	X	X	X	X	X	X
Unmapped AID	X	—	—	X	—	—	X	—	—	—

1. If the AID specified is the source AID, the direction is designated as “from E” in all one-way circuits (1-way, UPSR_HEAD, UPSR_DROP,UPSR_DC, and UPSR_EN).
2. If the AID specified is the destination AID or the drop side, the direction is designated as “from F” in all one-way circuits (1-way, UPSR_HEAD, UPSR_DROP,UPSR_DC, and UPSR_EN).

2.3 TL1 Gateway

This section describes the TL1 gateway and provides procedures and examples for implementing TL1 gateway on the ONS 15310-MA, ONS 15454, ONS 15454 M2, and ONS 15454 M6.

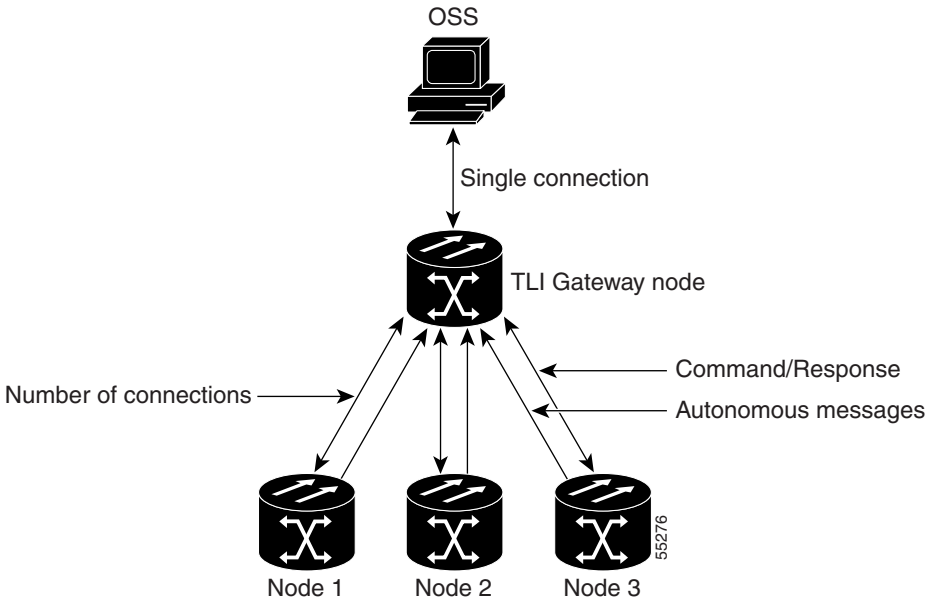
2.3.1 Gateway Network Element Topology

You can issue TL1 commands to multiple nodes through a single connection using the TL1 gateway. Any node can serve as a Gateway Network Element (GNE), End Network Element (ENE), or Intermediate Network Element (INE). A node becomes a GNE when a TL1 user connects to it and enters a command destined for another node. An ENE is an end node because it processes a TL1 command that is passed to it from another node. An INE is an intermediate node because of topology; it has no special hardware, software, or provisioning.

To implement the TL1 gateway, use the desired ENE's TID in the ACT-USER command to initiate a session between the GNE and the ENE. After a session is established, you need to enter the ENE's TID in all of the subsequent commands that are destined for the ENE. From the GNE, you can access several remote nodes, which become the ENEs. The ENEs are the message destinations or origins. The INE handles the data communications channel (DCC) TCP/IP packet exchange.

The GNE Session is the connection that multiplexes TL1 messages between the operations support system (OSS)/craftsperson and the GNE. The GNE demulitplexes incoming OSS TL1 commands and forwards them to the remote ENE. The GNE also multiplexes incoming responses and autonomous messages to the GNE Session. The ENE Session is the connection that exchanges messages between the GNE and the remote ENE. Figure 2-25 shows the GNE topology.

Figure 2-25 Example of a GNE Topology



2.3.2 TL1 Sessions

Each NE can support up to a maximum of 20 concurrent communication sessions (connections from an OS/NE to the GNE). The TL1 connections can be made through telnet sessions from the LAN or from the craft/serial port connection on the NE. One TL1 session is reserved for the active serial port connection. The remaining 19 sessions are used for TL1 sessions through the LAN (wire-wrap, active serial port, or DCC). Table 2-3 shows the number of serial port and LAN connections per platform.

Table 2-3 Number of TL1 Sessions per Platform

Platform	Number of Serial Port Sessions	Number of LAN Sessions	Total Number of TL1 Sessions
Cisco ONS 15310-MA	2	18	20
Cisco ONS 15454	1	19	20
Cisco ONS 15454 M2	1	19	20
Cisco ONS 15454 M6	1	19	20

2.3.3 TL1 Gateway and ENE Sessions

Only a limited number of TL1 users logged into an NE at any given time can establish sessions to other ENEs. The active serial port sessions are reserved and can always become a GNE session. The number of ENE sessions is based on the number of gateway communications sessions (GNE sessions).

Each NE can support up to 12 concurrent communication gateway sessions, depending on the NE type. The maximum number of ENE sessions also varies depending on the NE type.

You can dynamically distribute the maximum number of ENE sessions to balance the number of concurrent gateway communication sessions. The GNE treats the concurrent gateway communication sessions and ENE/GNE limit as a resource pool. It continues to allocate resources until the pool is exhausted. When the pool is exhausted, the GNE returns an "All Gateways in Use" message or an "All ENE Connections in Use" message.

Note The speed of the TL1 gateway and the maximum number of connections are limited by shared system resources, such as CTC, CTM, etc. The response time is slow as connections are increased and activity on these connections increases. Alarm storms, additional users, network latency, etc. also increase response time.

The gateway resource pools for each platform are shown in Table 2-4.

Table 2-4 Gateway Resource Pool

Platform	Maximum Number of GNE Sessions	Maximum Number of ENEs over IP DCC	Maximum Number of ENEs over OSI DCC
Cisco ONS 15310-MA	7 (5 + 2)	112	20
Cisco ONS 15454	11 (10 + 1)[1]	176	176[2]
Cisco ONS 15454 M2	11 (10 + 1)[3]	176	176[4]
Cisco ONS 15454 M6	11 (10 + 1)[5]	176	176[6]

1. If there are any active Socket Over TL1 sessions, the maximum number of GNE sessions that can be established is equal to the number of GNE sessions possible minus the number of Socket Over TL1 sessions. For example, if there are two active Socket Over TL1 sessions, the maximum number of GNE sessions for Cisco ONS 15454 is nine (11-2=9).
2. If there are any active COPY-RFILE command instances, the maximum number of ENE sessions over OSI DCC that can be established is equal to the number of possible ENE sessions over OSI DCC minus the number of COPY-RFILE command instances. For example, if there are 10 active COPY-RFILE command instances, the maximum number of ENE sessions over OSI DCC for Cisco ONS 15454 is 166 (176-10=166).
3. If there are any active Socket Over TL1 sessions, the maximum number of GNE sessions that can be established is equal to the number of GNE sessions possible minus the number of Socket Over TL1 sessions. For example, if there are two active Socket Over TL1 sessions, the maximum number of GNE sessions for Cisco ONS 15454 is nine (11-2=9).
4. If there are any active COPY-RFILE command instances, the maximum number of ENE sessions over OSI DCC that can be established is equal to the number of possible ENE sessions over OSI DCC minus the number of COPY-RFILE command instances. For example, if there are 10 active COPY-RFILE command instances, the maximum number of ENE sessions over OSI DCC for Cisco ONS 15454 is 166 (176-10=166).
5. If there are any active Socket Over TL1 sessions, the maximum number of GNE sessions that can be established is equal to the number of GNE sessions possible minus the number of Socket Over TL1 sessions. For example, if there are two active Socket Over TL1 sessions, the maximum number of GNE sessions for Cisco ONS 15454 is nine (11-2=9).
6. If there are any active COPY-RFILE command instances, the maximum number of ENE sessions over OSI DCC that can be established is equal to the number of possible ENE sessions over OSI DCC minus the number of COPY-RFILE command instances. For example, if there are 10 active COPY-RFILE command instances, the maximum number of ENE sessions over OSI DCC for Cisco ONS 15454 is 166 (176-10=166).

Examples of GNE/ENE resource alocation are provided in Table 2-5.

Table 2-5 Examples of Ideal ENE to GNE Resource Allocations

Applicable Cards	Number of GNE Communication Sessions	Number of ENEs over IP DCC	Number of ENEs over OSI DCC
15454 (TCC/TCC+/TCC2/TCC2P/TCC3), 15310-MA (CTX-2500)	1	16	16
15454 (TCC/TCC+/TCC2/TCC2P/TCC3), 15310-MA (CTX-2500)	2	32	32
15454 (TCC/TCC+/TCC2/TCC2P/TCC3), 15310-MA (CTX-2500)	3	48	48
15454 (TCC/TCC+/TCC2/TCC2P/TCC3), 15310-MA (CTX-2500)	4	64	64
15454 (TCC/TCC+/TCC2/TCC2P/TCC3), 15310-MA (CTX-2500)	5	80	80
15454 (TCC/TCC+/TCC2/TCC2P/TCC3), 15310-MA (CTX-2500)	6	96	88
15454 (TCC2/TCC2P/TCC3), 15310-MA (CTX-2500)	7	112	88
15454 (TCC2/TCC2P/TCC3)	8	128	88
15454 (TCC2/TCC2P/TCC3)	9	144	88
15454 (TCC2/TCC2P/TCC3)	10	160	88
15454 (TCC2/TCC2P/TCC3)	11	176	88

2.3.4 Implementing TL1 Gateway

Note Issuing commands to specific nodes in the network is accomplished by entering a unique node name in the TID field in each TL1 message. The TID field is synonymous with the name of the node and is the second token in a TL1 command.

The following procedures demonstrate TL1 gateway on a four-node ring (without TL1 gateway in Figure 2-26 and with TL1 gateway in Figure 2-27), where:

- Node 0 is the GNE.
- Node 1 is the ENE 1.
- Node 2 is the INE 2.
- Node 3 is the ENE 3.

Figure 2-26 Four-Node Ring Without TL1 Gateway

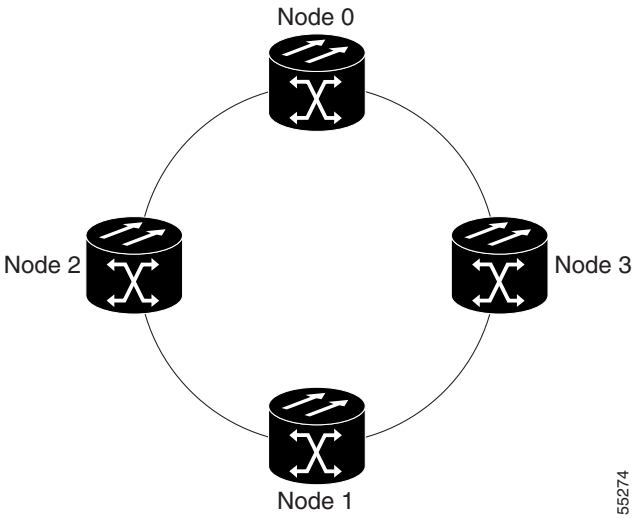
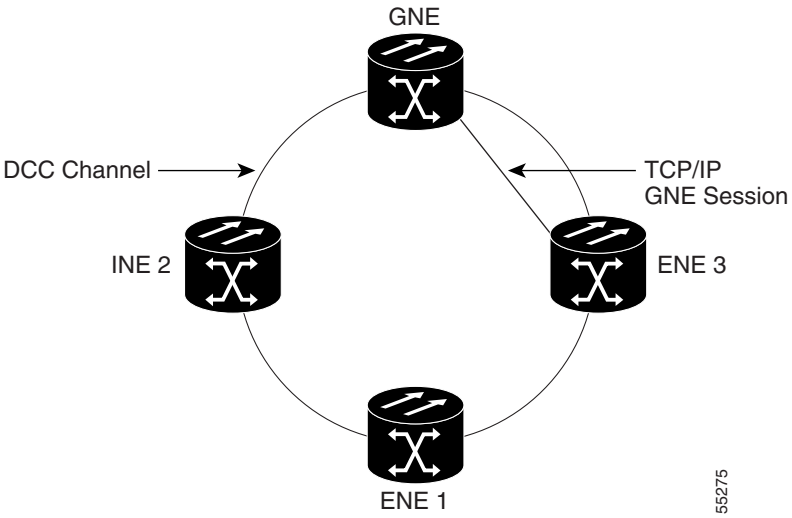


Figure 2-27 Four-Node Ring With TL1 Gateway



Log Into a Remote ENE

Step 1 Telnet or connect through the serial port to Node 0, which will become the GNE.

Step 2 To connect to the ENE 1 node, enter the TL1 login command using the following input example:

ACT-USER:NODE1:USERNAME:1234:PASSWORD;

The GNE forwards the login to ENE 1. After successful login, ENE 1 sends a COMPLD response.

Step 3 When you are logged into ENE 1, enter the following TL1 login command to connect to ENE 3:

ACT-USER:NODE3:USERNAME:1234:PASSWORD;

The GNE forwards the login to ENE 3. After successful login, the ENE 3 sends a COMPLD response.

Forward Commands by Specifying the ENE TID (Node 1 or Node 3)

When you are logged into ENE 1 and ENE 3, enter a command and designate a specific TID. To retrieve the header of Node 1, enter the following command:

RTRV-HDR:NODE1::1;

To retrieve the header of Node 3, enter the following command:

RTRV-HDR:NODE3::3;

Receive Autonomous Messages from the Remote ENE

To receive autonomous messages from the remote ENE, you must log into the remote ENE. When you are logged in, you will begin to receive autonomous messages. The source of the message is identified in the header of the message.

Log Out of a Remote ENE

To disconnect from a remote ENE, you must use the CANC-USER command. Use the following command to disconnect from ENE 1:

CANC-USER:NODE1:USERNAME:1;

Use the following command to disconnect from ENE 3:

CANC-USER:NODE3:USERNAME:3;

The GNE forwards the logout to the remote ENEs. The GNE/ENE TCP session is closed.

2.4 Ring Provisioning

This section provides information and sample procedures for setting up STS or VT circuits over existing path protection and bidirectional line switch ring (BLSR) configurations using TL1, including:

- Path Protection topology
- Path Protection cross-connections
- Ring-to-ring interconnection
- One-way drop and continue

For VTs, add the normal VT Group and VT ID extensions. These examples also assume that the slots/ports have been autoprovisioned (through a plug-in event) and that the ports involved have been placed into the IS state using a port configuration command, for example, ED-OCN.

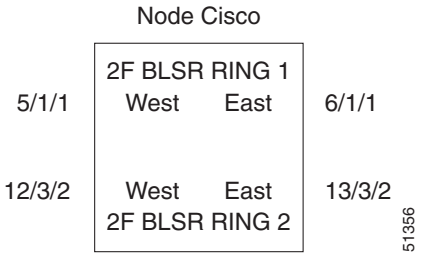
Note Because the ONS 15454, ONS 15454 M2, and ONS 15454 M6 implement logical path protection, there are no defined east and west ports. Instead, the east STS path for one circuit can exit a different port than the east STS path of another circuit, even though the west STS paths for both circuits might share the same port.

Note The ONS 15310-MA do not support BLSR.

2.4.1 Two-Fiber BLSR to Two-Fiber BLSR Connection Example

All protection for a two-fiber BLSR interconnecting to a two-fiber BLSR is performed at the line level. You can make the connection with a two-way cross-connect from an STS on the working side of the two-fiber BLSR span of Ring 1 to an STS on the working side of a two-fiber BLSR span on Ring 2. The connections can be east to east, east to west, west to east, and west to west. This example, illustrated in Figure 2-28, uses Ring 1 west to Ring 2 east and assumes an OC12-4 card in Slots 12 and 13 for subtending to a two-fiber BLSR (Ring 2).

Figure 2-28 Two-Fiber BLSR to Two-Fiber BLSR

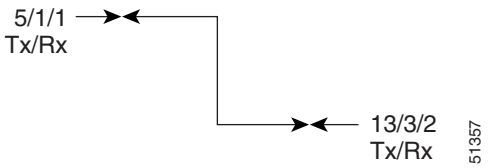


Use the following command to create a two-way connection from 5/1/1 to 13/3/2:

ENT-CRS-STS1:CISCO:STS-5-1,STS-13-26:CTAG4::2WAY;

This is shown in Figure 2-29.

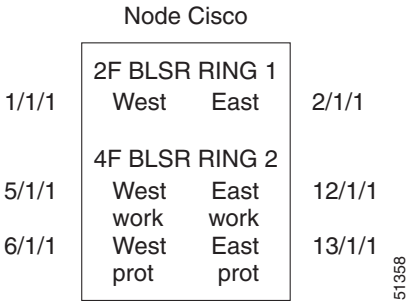
Figure 2-29 Two-Way Connection from 5/1/1 to 13/3/2



2.4.2 Two-Fiber BLSR to Four-Fiber BLSR Connection Example (ONS 15454)

All protection for a two-fiber BLSR interconnecting to a four-fiber BLSR is performed at the line level. You can make the connection with a simple two-way cross-connect from the appropriate side, east or west, of the two-fiber BLSR to the working fiber of the appropriate side, east or west, of the four-fiber BLSR, as shown in Figure 2-30.

Figure 2-30 Two-Fiber BLSR to Four-Fiber BLSR

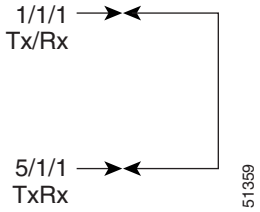


Use the following command to create a two-way connection from 1/1/1 to 5/1/1:

ENT-CRS-STS1:CISCO:STS-1-1,STS-5-1:CTAG5::2WAY;

This is shown in Figure 2-31.

Figure 2-31 Two-Way Connection from 1/1/1 to 5/1/1

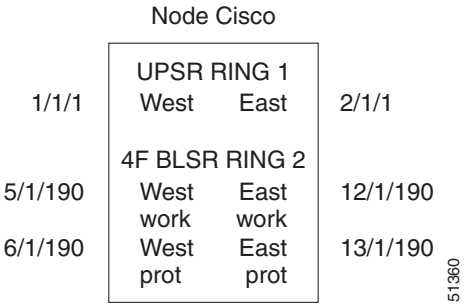


In the event of a failure, the software will automatically switch the traffic to the appropriate line and path.

2.4.3 Path Protection to Four-Fiber BLSR Connection Example (ONS 15454)

This example uses the west span of the four-fiber BLSR (Ring 2) for the active path of the circuit. The example also assumes that the four-fiber BLSR travels over OC-192 spans, as shown in.

Figure 2-32 Path Protection to Four-Fiber BLSR

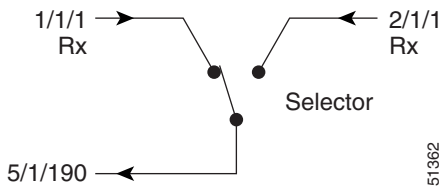


Use the following command to create a selector between 1/1/1 and 2/1/1 to Ring 2 (5/1/190)”

ENT-CRS-STS1:CISCO:STS-1-1&STS-2-1&STS-5-190:CTAG6::2WAY;

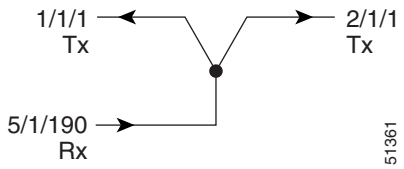
This is shown in Figure 2-33.

Figure 2-33 Selector Between 1/1/1 and 2/1/1 to Ring 2 (5/1/190)



The command also creates a bridge from 5/1/190 to Ring 1 (1/1/1 and 2/1/1), as shown in Figure 2-34.

Figure 2-34 Bridge From 5/1/190 to Ring 1 (1/1/1 and 2/1/1)



2.4.4 One-Way Drop and Continue

The following examples show how to create a one-way drop and continue cross-connect. The examples use three nodes (Node 1, Node 2, and Node 3) in a ring configuration (Figure 2-35). Node 1 is the source node, Node 2 has the drop and continue, and Node 3 is the destination.

Figure 2-35 One-Way Drop and Continue

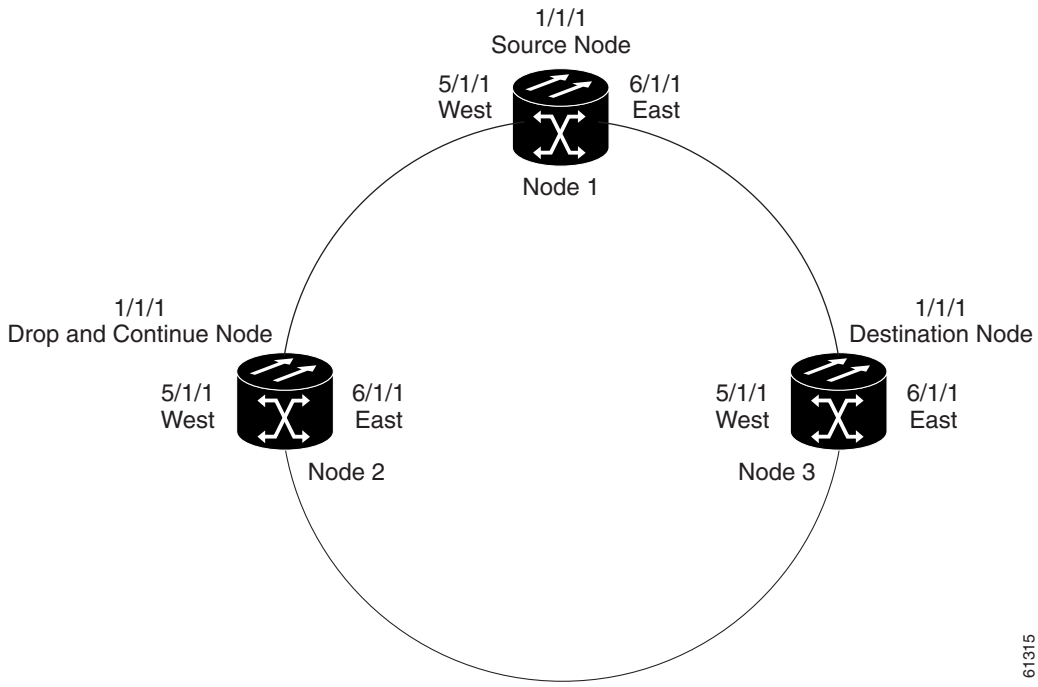
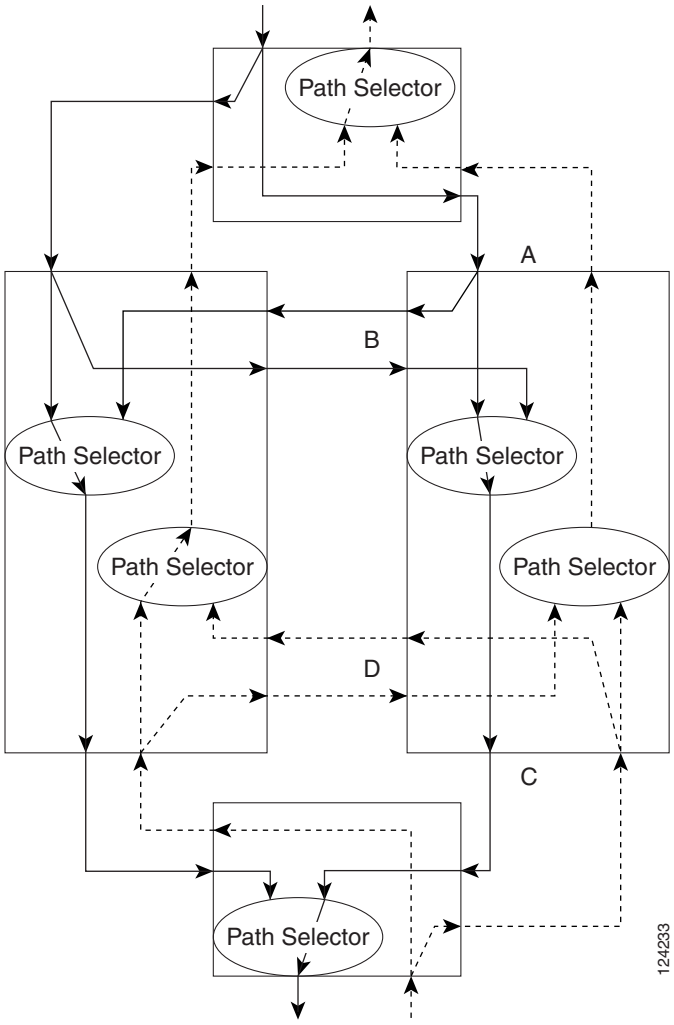


Figure 2-36 shows a circuit diagram example of the orientation of AIDs associated with the ENT-CRS command used to establish drop and continue connections.

Figure 2-36 Orientation of AIDs Used to Establish Drop and Continue Connections

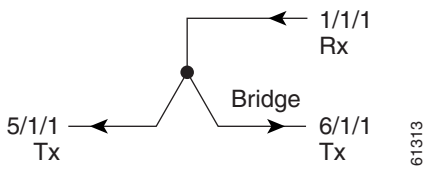


2.4.4.1 Node 1 Configuration Example (Source Node)

To configure Node 1 in the one-way drop-and-continue example, issue the following command on Node 1 (see Figure 2-37):

ENT-CRS-STSn::STS-1-1,STS-5-1&STS-6-1:CTAG::1WAY;

Figure 2-37 Bridge from 1/1/1 to 5/1/1 and 6/1/1

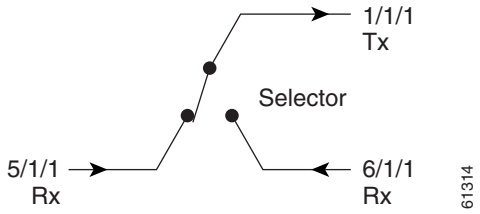


2.4.4.2 Node 2 Configuration Example (Drop and Continue Node)

To configure Node 2 in the one-way drop-and-continue example, issue the following command on Node 2 (see Figure 2-38):

ENT-CRS-STSn::STS-5-1&STS-6-1,STS-1-1:CTAG::1WAYDC;

Figure 2-38 Selector Between 5/1/1 and 6/1/1 to 1/1/1

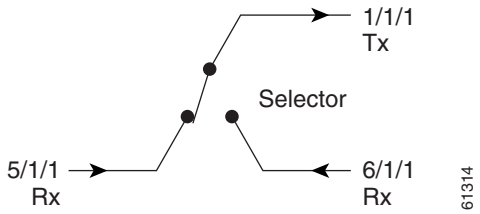


2.4.4.3 Node 3 Configuration Example (Destination Node)

To configure Node 3 in the one-way drop-and-continue example, issue the following command on Node 3 (see Figure 2-39):

ENT-CRS-STSn::STS-5-1&STS-6-1,STS-1-1:CTAG::1WAY;

Figure 2-39 Selector Between 5/1/1 and 6/1/1 to 1/1/1



2.5 PCA Provisioning

You can provision or retrieve protection channel access (PCA) cross-connections on two-fiber and four-fiber BLSR topologies at these supported OC rates: OC-12 (two-fiber only), OC-48, and OC-192. The traffic on the protection channel is referred to as extra traffic and has the lowest priority level. Extra traffic will be preempted by any working traffic that requires the use of the protection channel.

In a two-fiber BLSR, the extra traffic is provisioned on the upper half of the bandwidth path. In a four-fiber BLSR, the extra traffic is provisioned on the protect fiber. The PCA provisioning feature allows you to establish the PCA cross-connection on the protection path of the two-fiber BLSR and the protection channel of the four-fiber BLSR only when the query is an explicit request.

There are two PCA connection types: 1WAYPCA and 2WAYPCA. The PCA cross-connection is provisioned only when the user provides an explicit request using the ENT-CRS-STSp/VT1 commands. If the cross-connection is a PCA cross-connection, either 1WAYPCA or 2WAYPCA is shown in the cross-connect type field of the RTRV-CRS-STSp/VT1 command output.

1WAYPCA and 2WAYPCA are only used in the TL1 user interface to provide usability and visibility for the user to specify a PCA cross-connection type in the TL1 cross-connection commands.

The following restrictions apply to PCA provisioning:

- The network must be configured as either a two-fiber or four-fiber OC-12, OC-48, or OC-192 BLSR.
- The STS or VT1 path cross-connection can be established with TL1 commands (ENT-CRS-xxx).
- Because the RTRV-CRS-xxx command does not include the optional CTYPE field to specify a connection type, the output result reports the matched cross-connections based on the queried AID(s); therefore, the retrieved cross-connection inventory can include both PCA and non-PCA cross-connections.

2.5.1 Provision a PCA Cross-Connection

Example 2-14 shows the input format for provisioning a PCA cross-connection.

Example 2-14 Provision a PCA Cross-Connect: Input Format

```
ENT-CRS-<PATH>:[<TID>]:<FROM>,<TO>:<CTAG>::[<CCT>][::];
<PATH>::={STS_PATH, VT1}
[<CCT>]::={1WAY, 1WAYDC, 1WAYEN, 2WAY, 1WAYPCA, 2WAYPCA},
{STS_PATH}::={STS1, STS3C, STS6C, STS9C, STS12C, STS24C, STS48C, STS192C}
```

Where:

- STS represents all of the STS bandwidth cross-connections.
- VT1 represents all of the VT1_5 cross-connections.
- CCT defaults to 2WAY.

Example 2-15 shows an input example of provisioning an STS3C PCA cross-connection.

Example 2-15 Provision a PCA Cross-Connect: Example

```
ENT-CRS-STS3C::STS-1-1,STS-2-1:123::2WAYPCA;
```

Note If the cross-connect type (CCT) of this cross-connection provisioning command is either 1WAYPCA or 2WAYPCA, and the NONE value of both <FROM> and <TO> AID is PCA AID, an IIAC (Input, Invalid PCA AIDs) error message is returned.

Note If sending this command with a non-PCA CCT, and one (or two) AIDs is/are the PCA AIDs, an IIAC (The PCA AID Is Not Allowed for the Queried CCT Type) error message is returned.

2.5.2 Retrieve a PCA Cross-Connection

Use the input format in Example 2-16 to retrieve a PCA cross-connection.

Example 2-16 Retrieve a PCA Cross-Connect: Input Format

```
RTRV-CRS-[<PATH>]:[<TID>]:<AID>:<CTAG>[::::];<PATH>::={STS_PATH, VT1, STS}
```

If PATH is STS, it will retrieve all the STS cross-connections based on the queried AIDs.

<AID>={FacilityAIDs, STSAIDs, VTAIDs, ALL}

Example 2-17 shows the output format of the PCA STSp cross-connection retrieval command.

Example 2-17 Output Format of PCA STSp Cross-Connect Retrieve Command

```
"<FROM>,<TO>:2WAYPCA,STS3C"
```

Example 2-18 shows the output format of the PCA VT cross-connection retrieval command.

Example 2-18 Output Format of PCA VT Cross-Connect Retrieve Command

```
"<FROM>,<TO>:2WAYPCA"
```

2.6 FTP Software Download

Note FTP timeout is 30 seconds and is not user-configurable.

The file transfer protocol (FTP) software download feature downloads a software package to the inactive flash partition residing on either the TCC2/TCC2P/TCC3, XTC, CTX2500, or TSC card. FTP software download provides for simplex and duplex TCC2/TCC2P/TCC3, XTC, CTX2500, or TSC card downloads, success and failure status, and in-progress status at 20 percent increments.

2.6.1 COPY-RFILE

The COPY-RFILE command downloads a new software package from the location specified by the FTP URL into the inactive flash partition residing on either the TCC2/TCC2P/TCC3, XTC, CTX2500, or TSC card. COPY-RFILE can also be used to backup and restore the database file.

Note Since Software Release 5.0, PACKAGE_PATH is relative to your home directory, instead of being an absolute path from the root directory of the NE. If you want to specify an absolute path, start the path with the string '%2F'.

Input format:

COPY-RFILE:[<TID>]:<SRC>:<CTAG>::TYPE=<XFERTYPE>,[SRC=<SRC1>],[DEST=<DEST>],[OVWRT=<OVWRT>],[FTTD=<FTTD>];

where:

- <SRC> is the type of file being transferred.
- <XFERTYPE> is the file transfer protocol.
- <SRC1> specifies the source of the file to be transferred. Only the FTP URL is supported. SRC1 is a string. In a nonfirewall environment, the format for the URL is:

  "FTP://FTP_USER[:FTP_PASSWORD]]@FTP_HOST_IP[:FTP_PORT]/PACKAGE_PATH[:TYPE=I]"

  where:

  - FTP_USER is the user ID used to connect to the computer with the package file.
  - FTP_PASSWORD is the password used to connect to the computer with the package file.
  - FTP_HOST_IP is the IP address of the computer with the package file. DNS lookup of hostnames is not supported.
  - FTP_PORT defaults to 21.
  - PACKAGE_PATH is the long path name to the package file starting from the home directory of the logged-in user.

    In a firewall environment, the host name should be replaced with a list of IP addresses, each separated by an ampersand (@) character. The first IP address should be for the computer where the package file is stored. Subsequent IP addresses are for firewall computers moving outward toward the edge of the network until the final IP address listed is the computer that outside users use to first access the network.

    For example, if your topology is:

    "FTPHOST <-> GNE3 <->GNE2 <-> GNE1 <-> ENE"

    the FTP URL is:

    FTP://FTP_USER:FTP_PASSWORD@FTP_HOST_IP@GNE3@GNE2@GNE1/PACKAGE_PATH
- <DEST> specifies the destination of the file to be transferred. The comments for the SRC parameter are also valid here. <DEST> is a string.
- If <OVWRT> is YES, then files are overwritten. Currently only YES is supported. Using a NO value for <OVWRT> will result in an error message.
- <FTTD> is the format of the URI, should be "FTTD://[FTTD_USER][:FTTD_PASSWORD]]@FTTD_HOST_TID" where:
  - FTTD_USER is the user ID to connect to the FTTD host.
  - FTTD_PASSWORD is the password used to connect to FTTD host.
  - FTTD_HOST_IP is the TID of the FTTD host/. DNS and network service access point (NSAP) names are not supported.

Note

- FTP is the only allowed file transfer method.
- The use of the SWDL and the extended FTP URL syntax are required by the COPY-RFILE syntax.

2.6.2 APPLY

The APPLY command can activate or revert software depending on the version of software loaded on the active and protect flash. An error is returned if the node is attempting to activate to an older software load or trying to revert to a newer software load. If this command is successful, the appropriate flash is selected and the TCC2/TCC2P/TCC3, XTC, CTX2500, or TSC card will reboot.

The input format for the APPLY command is as follows:

APPLY:[<TID>]::<CTAG>[::<MEM_SW_TYPE>];

where:

- <MEM_SW_TYPE> indicates the memory switch action during the software upgrade.

2.6.3 REPT EVT FXFR

REPT EVT FXFR is an autonomous message used to report the start, completion, and completed percentage status of the FTP software download. REPT EVT FXFR also reports any failure during the software upgrade including invalid package, invalid path, invalid userid/password, and loss of network connection.

Note The "FXFR_RSLT" is only sent when the "FXFR_STATUS" is COMPLD.

The "BYTES_XFRD" is only sent when the "FXFR_STATUS" is IP or COMPLD.

The output format of the REPT EVT FXFR message is as follows:

```
   SID DATE TIME
A  ATAG REPT EVT FXFR
   "<FILENAME>,<FXFR_STATUS>,[<FXFR_RSLT>],[<BYTES_XFRD>]"
;
```

where:

- <FILENAME> indicates the transferred file path name and is a string. When a package is being transferred between the FTP server and the controller cards, the filename field will contain the string "active". Following this transfer, if there is a second controller card on the node, the file will be copied over to the second card. While this is happening, REPT EVT FXFR messages will be generated with a filename of "standby".
- <FXFR_STATUS> indicates the file transferred status: Start, IP (in progress), or COMPLD.
- <FXFR_RSLT> indicates the file transferred result: success or failure. <FXFR_RSLT> is optional.
- <BYTES_XFRD> indicates the transferred byte count. <BYTES_XFRD> is a string and is optional.

2.6.4 Downloading New Software

The following procedure downloads new software to the TCC2/TCC2P, XTC, CTX2500, or TSC card using TL1.

Download New Software

Note Only Superusers can download and activate software.

Step 1 Copy the new software package (for example, 15XXX-0340-X02E-2804.pkg) to an FTP host.

Step 2 Establish a TL1 session with the target NE.

Step 3 Log in with the ACT-USER command.

Step 4 Check the working and protect software on the NE by issuing the RTRV-NE-GEN command.

Input example:

RTRV-NE-GEN:::1;

The output should be similar to the following:

```
   VA454-94 1970-01-06 22:22:12
M 1  COMPLD
  "IPADDR=10.76.44.112,IPMASK=255.255.255.128,DEFRTR=10.76.44.1,IPV6ENABLE=N,II
OPPORT=57790,NAME=\"310-MA-SDH-112\",SWVER=9.00.00,LOAD=09.00-008G-19.05,PROTS
WVER=9.00.00,PROTLOAD=09.00-008F-06.23,DEFDESC=\"Factory
Defaults\",PLATFORM=15310,MASDH,SECUMODE=NORMAL,SUPPRESSIP=NO,MODE=SING
LESHELF,AUTOPM=NO,SERIALPORTECHO=Y,OSIROUTINGMODE=ES,NET=39840F8000000
000000000000000059B12DB3000"
;
```

Step 5 Issue the COPY-RFILE command. This command will initiate the download process. See the "2.6.1 COPY-RFILE" section on page 2-36 for command syntax.

In Example 2-19, the package is located in "/%2FUSR/CET/VINTARA" in the host 10.77.22.199. The user ID and passwords are TL1 and CISCO454. The directory path of the package is similar to what you will see during an FTP session.

Example 2-19 Issue the COPY-RFILE Command

```
COPY-RFILE::RFILE-
PKG:CTAG::TYPE=SWDL,SRC="FTP://TL1:CISCO454@10.77.29.199
/%2FUSR/CET/VINTARA/15454-0340-X02E-2804.PKG";

   DEV208 1970-01-10 11:51:57
M   CTAG  COMPLD
;
```

Step 6 If any of the parameters are wrong or if the host is not accessible, a REPT EVT FXFR message will report errors. A download failure can result from one or more of the following:

- Directory path of the package is invalid or not found
- Package is invalid
- Package not found on specified path

- User ID/password or host name is invalid
- Host is not accessible
- Firewall user ID/password or host is invalid
- Node rebooted/lost connection during download
- Software download is already in progress
- The node or the host timed out during FTP protocol (see Example 2-20)

Example 2-20 REPT EVT FXFR when Node or Host Timed Out During FTP Protocol

```
DEV208 1970-01-10 11:52:02
A  2816.2816 REPT EVT FXFR
   "SLOT-11:SFTWDOWN-FAIL,TC,,,,,,,:\"SOFTWARE DOWNLOAD FAILED\",TCC
;
```

Step 7 If the download is successful, the REPT EVT FXFR message will report an active start, as shown in Example 2-21.

Example 2-21 REPT EVT FXFR Message Reporting an Active Start

```
DEV208 1970-01-10 11:52:15
A  2818,2818 REPT EVT FXFR
   "ACTIVE START"
;
```

Step 8 A SFTDOWN minor alarm is raised to indicate that the software download is in progress (Example 2-22). The SFTDOWN alarm will clear when the download is complete.

Example 2-22 SFTDOWN Minor Alarm

```
DEV208 1970-01--10 11:52:15
*  2817.2817 REPT ALM EQPT
   "SLOT-7:MN,SFTWDOWN,NSA,,,,:\"SOFTWARE DOWNLOAD IN PROGRESS\",TCC"
;
```

Use the in-progress status at any time during the software download to verify the RTRV-NE-GEN command (Example 2-23).

Example 2-23 RTRV-NE-GEN Command

```
RTRV-NE-GEN

   VA454-94 1970-01-06 22:22;12
M  1  COMPLD
   "IPADDR=10.76.44.112,IPMASK=255.255.255.128,DEFRTR=10.76.44.1,IPV6ENABLE=N,II
OPPORT=57790,NAME=\"310-MA-SDH-112\",SWVER=9.00.00,LOAD=09.00-008G-19.05,PROTSWV
ER=9.00.00,PROTLOAD=09.00-008F-06.23,DEFDESC=\"Factory Defaults\",PLATFORM=15310
MASDH,SECUMODE=NORMAL,SUPPRESSIP=NO,MODE=SINGLESHELF,AUTOPM=NO,SERIALPORTECHO=Y,
OSIROUTINGMODE=ES,NET=39840F8000000000000000000000059B12DB3000"
;
```

Step 9 The download progress is reported by the REPT EVT FXFR message, which will report a message after every 20 percent of download is complete as shown in Example 2-24.

Example 2-24 REPT EVT FXFR Messages During Software Download

```
DEV208 1970-01-10 11:53:12
A  2820,2820 REPT EVT FXFR
   "ACTIVE,IP,,20"
;

DEV208 1970-01-10 11:53:12
A  2820,2820 REPT EVT FXFR
   "ACTIVE,IP,,40"
;

DEV208 1970-01-10 11:53:12
A  2820,2820 REPT EVT FXFR
   "ACTIVE,IP,,60"
;

DEV208 1970-01-10 11:53:12
A  2820,2820 REPT EVT FXFR
   "ACTIVE,IP,,80"
;
```

Step 10 If the TL1 session times out during download or if the user terminates the TL1 session, the download will continue. The download completion can be confirmed by issuing the RTRV-NE-GEN command and verifying the PROTLOAD (Example 2-25).

Example 2-25 Verifying the PROTLOAD

```
RTRV-NE-GEN:::1;

   VA454-94 1970-01-06 22:22:12
M  1  COMPLD
   "IPADDR=10.76.44.112,IPMASK=255.255.255.128,DEFRTR=10.76.44.1,IPV6ENABLE=N,II
OPPORT=57790,NAME=\"310-MA-SDH-112\",SWVER=9.00.00,LOAD=09.00-008G-19.05,PROTSWV
ER=9.00.00,PROTLOAD=09.00-008F-06.23,DEFDESC=\"Factory Defaults\",PLATFORM=15310
MASDH,SECUMODE=NORMAL,SUPPRESSIP=NO,MODE=SINGLESHELF,AUTOPM=NO,SERIALPORTECHO=Y,
OSIROUTINGMODE=ES,NET=39840F8000000000000000000000059B12DB3000"
;
```

Step 11 REPT EVT FXFR confirms the completion of the software download (Example 2-26).

Example 2-26 Confirm Download Completion

```
DEV208 1970-01-10 12:01:16
A  2825,2825 REPT EVT FXFR
   "ACTIVE,COMPLD,SUCCESS"
;
```

Step 12 The SFTDOWN alarm clears when the download is complete (Example 2-27).

Example 2-27 Download is Complete

```
DEV208 1970-01-10 11:52:15
*  2826,2817 REPT ALM EQPT
   "SLOT-7:CL,SFTWDOWN,NSA,,,,:\"SOFTWARE DOWNLOAD IN PROGRESS\",TCC"
;
```

2.6.5 Activating New Software

After the software is successfully downloaded, the new software that resides in the protect load must be activated to run on the NE. The APPLY command can be used to activate and revert depending on the version of the protect software and the newly downloaded software (see the "2.6.2 APPLY" section on page 2-38 for correct APPLY syntax).

Activate New Software

Step 1 If the protect software is newer than the working software, activate it as shown:

APPLY::1::ACT;

```
   DEV208 1970-01-10 13:40:53
M  1 COMPLD
;
```

An error is reported if a revert is attempted with a newer protect software.

Step 2 If the APPLY command is successful, log out of the TL1 session using the CANC-USER command:

CANC-USER::CISCO15:1;

```
  VA454-94 1970-01-07 01:18:18
M  1  COMPLD
;
```

After a successful completion of the APPLY command, the NE will reboot and the TL1 session will disconnect. When the NE comes up after the reboot, it will be running the new software. Traffic switches are possible during activation.

2.6.6 Remote Software Download/Activation Using the GNE

In a network with Section data communications channel (SDCC)-connected ONS 15310-MAs, ONS 15454s, ONS 15454 M2s, and ONS 15454 M6s remote download and activation are possible using the GNE/ENE feature supported in TL1. The GNE must be connected by a LAN and the remaining ENEs can download the new software package through fiber from the GNE.

For remote software downloading, complete the steps in the "Download New Software" procedure on page 2-39 and the "Activate New Software" procedure on page 2-42, but ensure that the TID in each command is filled with the ENE node name.

Each GNE can support 20 (TCC2/TCC2P/TCC3) or 6 (XTC, CTX2500) concurrent communication gateway sessions and up to a maximum of 176 (TCC2/TCC2P/TCC3) or 96 (XTC, CTX2500) ENEs/GNEs. For more information on TL1 gateway, see the "2.3 TL1 Gateway" section on page 2-24.

After activating the nodes (Example 2-28), five simultaneous software downloads can be initiated using the COPY-RFILE command with appropriate TIDs, as shown in Example 2-29. All downloads will be independent of each other and download speeds might differ.

Example 2-28 Activating the Nodes for Simultaneous Software Downloads

```
ACT-USER:NODE1:CISCO15:1;
ACT-USER:NODE2:CISCO15:1;
ACT-USER:NODE3:CISCO15:1;
ACT-USER:NODE4:CISCO15:1;
ACT-USER:NODE5:CISCO15:1;
```

Example 2-29 Downloading Software on Multiple Nodes Simultaneously

```
COPY-RFILE:NODE1:RFILE-PKG:CTAG::TYPE=SWDL,SRC="FTP://TL1:
CISCO454@10.77.29.199/USR/CET/VINTARA/15454-0340-X02E-2804.PKG";

COPY-RFILE:NODE2:RFILE-PKG...
COPY-RFILE:NODE3:RFILE-PKG...
COPY-RFILE:NODE4:RFILE-PKG...
COPY-RFILE:NODE5:RFILE-PKG...
```

To download software to an ENE through a GNE, the FTTD URL in the COPY-RFILE command must be used as shown in Example 2-30. The FTTD parameter has the following format: "FTTD://USERID:PASSWORD@TL1 GNE NODENAME:21". Prior to Release 6.0, Port 21 is mandatory. In Release 6.0 and later, Port 21 is optional.

Example 2-30 Downloading Software to an ENE through a GNE

```
GNE = NODE1
ENE = NODE2

COPY-RFILE:NODE2:RFILE-PKG:1::TYPE=SWDL,SRC=FTP://USER-ID:PASSWORD@HOST-IP//USERS/JDOE/
15454-XXXX-XXXX-XXXX.PKG,OVWRT=YES,FTTD="FTTD://USERID:PASSWORD@NODE1:21"
```

Individual REPT EVT FXFR messages can be isolated using the node names. RTRV-NE-GEN also requires the individual node names entered in the TID in order to retrieve a specific download status.

Activate the software using the APPLY command (Example 2-31) on all of the nodes using the GNE node.

Note Activate the GNE last, after activating all the ENEs, or else ENE connectivity will be lost when the GNE starts to reboot for activation.

Example 2-31 Activate the Software Load

```
APPLY:NODE1::1::ACT;
APPLY:NODE2::1::ACT;
APPLY:NODE3::1::ACT;
APPLY:NODE4::1::ACT;
APPLY:NODE5::1::ACT;
```

2.7 Scheduled PM Report

The scheduled performance monitoring (PM) report is a feature that extends the capability of PM reporting for the Cisco ONS 15310-MA, Cisco ONS 15454, Cisco ONS 15454 M2, and Cisco ONS 15454 M6. With a scheduled PM report, the system automatically and periodically generates the PM report of any specified facility or cross-connection.

Note

- The current maximum number of schedules allowed to be created for an NE is 1000. If the limit has been reached and the user tries to create more schedules on the NE, the error message "Reach Limits Of MAX Schedules Allowed. Can Not Add More" is returned.
- Identical schedules for an NE are not allowed. Two schedules are considered identical if they have the same AID, MOD2 type, performance monitor type, performance monitor level, location, direction and time period.
- An error message "Duplicate Schedule" is returned if you create a schedule that is a duplicate of an existing schedule. However, if the existing schedule expires (and the parameter <NUMINVL> is equal to zero when retrieved by the RTRV-PMSCHED command, which means that no more performance monitoring reports are to be sent), then the new schedule with the identical parameter will replace the existing schedule.
- When you create a PM schedule, the minimum report interval should not be less than five minutes.
- Refer to the *Cisco ONS SONET TL1 Command Guide* for complete command and autonomous message information.

2.7.1 Create a PM Schedule and Receive an Autonomous PM Report

Issue the SCHED-PMREPT-<MOD2> command to create a PM schedule.

Note The minimum interval for the PM schedule cannot be set to less than five minutes.

Issue the ALW-PMREPT-ALL command to allow the current TL1 session to be able to receive the autonomous PM report.

2.7.2 Manage PM Schedules

Use the following commands to manage PM schedules:

- Create a PM schedule by issuing the SCHED-PMREPT-<MOD2> command.
- Delete a PM schedule by issuing the SCHED-PMREPT-<MOD2> command with the <NUMREPT> parameter equal to zero.

Note The PM schedules created on a facility or a cross-connect will be automatically deleted if the card or the cross-connect are unprovisioned.

- Retrieve all the PM schedules created on the node by issuing the RTRV-PMSCHED-ALL command. Retrieve a particular MOD2 type of PM schedule by issuing the RTRV-PMSCHED-<MOD2> command.

Note The system will not automatically delete the schedules that are expired. For example, assume that a schedule is created to report PM 10 times. After 10 PM reports are sent, the schedule is expired. The expired schedule can be identified by its <NUMINVL> field (equal to zero) in the response of RTRV-PMSCHED.

2.7.3 Enable or Disable a TL1 Session to Receive Autonomous PM Reports

Enable a TL1 session to receive a scheduled PM report by issuing the ALW-PMREPT-ALL command.

Note By default, a TL1 session is disabled to receive PM reports. The ALW-PMREPT-ALL command enables a TL1 user to receive all the scheduled PM and automatic autonomous performance monitoring (AutoPM) reports from the system, regardless of whether or not the schedule is created by this TL1 user or by any other TL1 user.

Disable a TL1 session to receive any scheduled PM report by issuing the INH-PMREPT-ALL command.

2.8 Automatic Autonomous PM

The automatic autonomous performance monitoring (AutoPM) report is a feature that extends the capability of PM reporting for the Cisco ONS 15310-MA, Cisco ONS 15454, Cisco ONS 15454 M2, and Cisco ONS 15454 M6. With this feature enabled, the system automatically generates the PM report for all cross-connections. AutoPM is disabled by default. When enabled, an automatic report is generated every 15 minutes, which is the default interval.

AutoPM can be enabled or disabled only through CTC. Refer to the “Monitor Performance” chapter in the *Cisco ONS 15454 Procedure Guide* for the procedure.

Issue the RTRV-NE-GEN TL1 command on the node to retrieve the AutoPM configuration.

To enable or disable a TL1 session to receive AutoPM reports see the “2.7.3 Enable or Disable a TL1 Session to Receive Autonomous PM Reports” section on page 2-45.

2.9 Bridge and Roll

Bridge and Roll functionality in the Cisco ONS 15310-MA, Cisco ONS 15454, Cisco ONS 15454 M2, and Cisco ONS 15454 M6 allows live traffic to be moved (rolled) from one entity to another. This section provides information and sample procedures for single-rolling, dual-rolling, and protection rolling for one-way or two-way circuits using TL1 commands, including:

- Path Level Rolling—Rolls cross-connections at the VT1.5, STS1, and STSNc rate for all supported time division multiplexing (TDM) drops (OC3, OC12, OC48, and OC192). Individual rolls are done at the Path level.
- Line Level Rolling—Rolls all cross-connections from one port/facility to another port/facility.
- Bulk Rolling—Rolls a subset of cross-connections from one port/facility to another port/facility.

There are two roll modes:

- In automatic mode, the leg to be rolled is automatically dropped upon detection of a valid input signal on the new path.
- In manual mode, the leg to be rolled is retained upon detection of a valid signal on the new path. The leg must be dropped manually.

Caution If you have created a roll on the circuit and it has detected a valid signal, do not cancel it. Cancelling a valid roll will cause a traffic hit of more than 1300 ms. If you want to revert back from a valid roll, complete the roll and use bridge and roll again to roll it back.

Caution Performing bridge and roll on an STS-192c (ONS 15454) might cause a traffic hit of 50 ms.

Note The path width rules for creating circuits apply when rolling circuits. For example, if you roll an STS3c starting at STS#1, you cannot roll it to another port and start it at STS#2. You have to start it at STS#1.

2.9.1 Restrictions

The following restrictions apply for bridge and roll using TL1 in this release:

- Rolling is not allowed on electrical cards or Ethernet cards.
- Rolling is not allowed on hairpin circuits.
- Rolling is not allowed on monitor circuits.
- Rolling is not allowed on any cross-connection that is involved in test access.
- Rolling is not allowed on any cross-connection that is involved in cross-connect loopbacks.
- Rolling is not allowed on any port that is involved in facility or equipment loopbacks. This restriction applies to both “roll from” and “roll to.”
- When rolling on a 1+1 protected circuit, the “roll to” cannot be on the protect port of the protection group.
- Rolling on a BLSR protected circuit cannot violate the rules governing BLSR circuits: a circuit that traverses a BLSR must use the same STS number on the ring between source and destination.
- Rolling on a BLSR protected circuit will be denied if there is an existing protection switch on the ring. If the protection switch happens after the roll is initiated, the system will not monitor valid signals on the “roll to” path until the protection switching is cleared.
- Rolling on a path protection protected circuit cannot violate the rules governing path protection circuits: path protection circuits must have one bridge and one selector.
- The bridge and selector of a path protection protected circuit cannot be rolled away.
- In the case of a dual roll on a path protection protected circuit, both roll points have to be on either the working or protect path of the circuit. For example, you cannot specify one roll point on the working path and the other roll point on the protect path of the circuit being rolled.
- When rolling on a path protection protected circuit, the “roll to” cannot be line protected (1+1 or BLSR protected). TL1 can only ensure this on the bridge and selector node, not on the intermediate node.

- When rolling on a mixed protection circuit, the roll points have to be within the same protection domain.
- Rolling using TL1 can be performed on a CTC-created cross-connection.

Note If a roll is created using TL1, it cannot be edited or deleted by CTC.

- Rolling using TL1 can be performed on a TL1 cross-connection.

Note If a roll is created using CTC, it cannot be edited or deleted by TL1.

- If the intermediate path of a circuit is being rolled away to another circuit, the second circuit cannot carry any live traffic.

Note After a roll is completed, the second circuit will form the new intermediate path of the original circuit.

- Rolling cannot be performed on VT tunnels or VT aggregation point (VAP) circuits passing through less than four nodes.

The following restrictions apply for bridge and roll using TL1 VCAT in this release:

- For VCAT circuits that are not open-ended, you cannot change the source or destination of the circuit.
- For open-ended VCAT circuits, you can change the source or destination of the circuit, but only on the open end.

The following restrictions apply for bridge and roll using TL1 common-fiber-routed VCAT circuits in this release:

- Rolling cannot change the common fiber property of a common-fiber-routed VCAT circuit.
- When rolling on a VCAT member circuit, in order not to change the common fiber property of a common-fiber-routed VCAT circuit, you can roll the member from one time slot to a different time slot within the same fiber.

2.9.2 Bridge and Roll TL1 Commands

The following commands are used for bridge and roll. Refer to the *Cisco ONS SONET TL1 Command Guide* for full command descriptions including input and output formats and examples.

- DLT-BULKROLL-<OCN_TYPE>

  This command deletes or completes an attempted rolling operation. This command supports Line-level rolling and bulk rolling. It cannot be used for Path-level rolling. The rolls that are created using the ENT-BULKROLL-<OCN_TYPE> command can be deleted using the DLT-BULKROLL-<OCN_TYPE> command.

- DLT-ROLL-<MOD_PATH>

  This command deletes an attempted rolling operation or completes an attempted rolling operation.

- ED-BULKROLL-<OCN_TYPE>

This command edits information about rolling traffic from one endpoint to another without interrupting service. This command can use the CMDMDE option to force a valid signal. The only parameter that can be edited is CMDMDE. The time slots cannot be edited. This commands supports Line-level rolling and bulk rolling. It cannot be used for Path-level rolling.

- ED-ROLL-<MOD_PATH>

  This command edits information about rolling traffic from one endpoint to another without interrupting service. This command can use the CMDMDE option to force a valid signal. The only parameter that can be edited is CMDMDE. The time slots cannot be edited.

- ENT-BULKROLL-<OCN_TYPE>

  This command enters information about rolling traffic from one endpoint to another without interrupting service. This commands supports Line-level and bulk rolling. It cannot be used for single Path-level rolling.

- ENT-ROLL-<MOD_PATH>

  This command enters information about rolling traffic from one endpoint to another without interrupting service. This command supports STS and VT Path-level rolling only.

- RTRV-BULKROLL-<OCN_TYPE>

  This command retrieves roll data parameters. This command supports Line-level rolling and bulk rolling. It cannot be used for Path-level rolling.

- RTRV-ROLL-<MOD_PATH>

  This command retrieves roll data parameters.

2.9.3 Two-Way Circuit Single Roll and Dual Roll Procedures

Single roll operation moves either the source or destination of a circuit to a new endpoint: onto the same node or onto a different node. In a single-roll operation, you only choose one roll point during the process.

Dual roll operation reroutes a segment between two roll points of a circuit. The new route can be one of the following:

- A new link (no circuit is required)
- Another circuit (created before or during the bridge and roll process

In dual roll operation, you choose two roll points during the process.

Create a Two-Way Circuit Single Roll or Dual Roll

To create a two-way circuit single roll or dual roll, enter the ENT-ROLL-<MOD_PATH> command or the ENT-BULKROLL-<OCN_TYPE> command depending on the type of roll you want to perform.

The input formats are as follows:

- **ENT-ROLL-<MOD_PATH>:[<TID>]:<FROM>,<TO>:<CTAG>:::RFROM=<RFROM>, RTO=<RTO>,RMODE=<RMODE>,[CMDMDE=<CMDMDE>];**
- **ENT-BULKROLL-<MOD_PATH>:[<TID>]:<FROM>:<CTAG>:::RTOSTART=<RTOSTART> ,[RFROMSTART=<RFROMSTART>],[RFROMEND=<RFROMEND>],[RMODE=<RMOD E>],[CMDMDE=<CMDMDE>];**

Step 1 Choose the type of roll that you want to perform and enter the corresponding command:

- For automatic rolling onto the same facility, but different STS (Path roll), use an ENT-ROLL command similar to the following example:

  ENT-ROLL-STS1:CISCO:STS-1-1-1,STS-2-1-1:1:::RFROM=STS-2-1-1, RTO=STS-3-1-1,RMODE=AUTO,CMDMDE=FRCD;

- For manual rolling onto the same facility, but different STS (Path roll), use an ENT-ROLL command similar to the following example:

  ENT-ROLL-STS1:CISCO:STS-1-1-1,STS-2-1-1:1:::RFROM=STS-2-1-1, RTO=STS-3-1-1,RMODE=MAN,CMDMDE=FRCD;

- For rolling onto a different facility with the same or different STS (Line roll), use an ENT-BULKROLL command similar to the following example:

  ENT-BULKROLL-OC48:CISCO:FAC-5-1:123:::RFROMSTART=STS-5-1-1, RTOSTART=STS-6-1-1,RMODE=AUTO,CMDMDE=FRCD;

  This command will roll all the STS and VT paths to a facility on Slot 6 with the same STS as shown in Table 2-6.

Table 2-6 Two-Way Circuit Single or Dual Line Roll with ENT-BULKROLL

Paths	Before Roll	After Roll
STS#1	STS-5-1-1	STS-6-1-1
STS#2	STS-5-1-2	STS-6-1-2
VT#1 on STS#3	VT1-5-1-3-1-1	VT1-6-1-3-1-1
VT#2 on STS#3	VT1-5-1-3-2-4	VT1-6-1-3-2-4
STS#4	STS-5-1-4	STS-6-1-4
STS#5	STS-5-1-5	STS-6-1-5
VT#3 on STS#6	VT1-5-1-6-1-1	VT1-6-1-6-1-1

- For rolling a set of circuits onto a different facility (bulk roll), use an ENT-BULKROLL command similar to the following example:

  ENT-BULKROLL-OC48:CISCO:FAC-5-1:123:::RFROMSTART=STS-5-1-1, RTOSTART=STS-6-1-1,RFROMEND=STS-5-1-4,RMODE=AUTO,CMDMDE=FRCD;

  This command will roll the paths shown in Table 2-7.

Table 2-7 Two-Way Circuit Single or Dual Bulk Roll with ENT-BULKROLL

Paths	Before Roll	After Roll
STS#1	STS-5-1-1	STS-6-1-1
STS#2	STS-5-1-2	STS-6-1-2
VT#1 on STS#3	VT1-5-1-3-1-1	VT1-6-1-3-1-1
VT#2 on STS#3	VT1-5-1-3-2-4	VT1-6-1-3-2-4
STS#4	STS-5-1-4	STS-6-1-4

Step 2 If you performed a manual roll, you must confirm the circuit is valid by issuing the RTRV-BULKROLL-<OCN_TYPE> command:

Input format:

RTRV-BULKROLL-<OCN_TYPE>:[<TID>]:<SRC>:<CTAG>;

Input example:

RTRV-BULKROLL-OC12:CISCO:FAC-3-1:1;

2.9.4 One-Way Circuit Single Roll and Dual Roll Procedures

Single roll operation moves either the source or destination of a circuit to a new endpoint: onto the same node or onto a different node. In single roll operation, you only choose one roll point during the process.

Dual roll operation reroutes a segment between two roll points of a circuit. In dual roll operation, you choose two roll points during the process.The new route can be one of the following:

- A new link (no circuit is required)
- Another circuit (created before or during the bridge and roll process

Create a One-Way Circuit Single Roll

To create a one-way circuit single roll, enter the ENT-ROLL-<MOD_PATH> command or the ENT-BULKROLL-<OCN_TYPE> command depending on the type of roll you want to perform.

Input formats:

- **ENT-ROLL-<MOD_PATH>:[<TID>]:<FROM>,<TO>:<CTAG>:::RFROM=<RFROM>, RTO=<RTO>,RMODE=<RMODE>,[CMDMDE=<CMDMDE>];**

  Note For a one-way destination roll, the roll mode (RMODE) must be manual (MAN).

- **ENT-BULKROLL-<OCN_TYPE>:[<TID>]:<FROM>:<CTAG>::: RTOSTART=<RTOSTART>,[RFROMSTART=<RFROMSTART>], [RFROMEND=<RFROMEND>],RMODE=<RMODE>,[CMDMDE=<CMDMDE>];**

Step 1 Choose which type of roll you want to perform and enter the corresponding command:

- For automatic rolling onto the same facility, but different STS (path roll), use an ENT-ROLL command similar to the following example:

  ENT-ROLL-STS1:CISCO:STS-1-1-1,STS-2-1-1:1:::RFROM=STS-2-1-1, RTO=STS-3-1-1,RMODE=AUTO,CMDMDE=FRCD;

- For manual rolling onto the same facility, but different STS (path roll), use an ENT-ROLL command similar to the following example:

  ENT-ROLL-STS1:CISCO:STS-1-1-1,STS-2-1-1:1:::RFROM=STS-2-1-1, RTO=STS-3-1-1,RMODE=MAN,CMDMDE=FRCD;

- For rolling onto a different facility with the same or different STS (line roll), use an ENT-ROLL command similar to the following example:

  ENT-ROLL-STS1:CISCO:STS-1-1-1,STS-2-1-1:1:::RFROM=STS-2-1-1, RTO=STS-3-1-1,RMODE=AUTO,CMDMDE=FRCD;

  This command will roll all the STS and VT paths to a facility on Slot 6 with the same STS as shown in Table 2-8.

Table 2-8 One-Way Circuit Single Line Roll with ENT-BULKROLL

Paths	Before Roll	After Roll
STS#1	STS-5-1-1	STS-6-1-1
STS#2	STS-5-1-2	STS-6-1-2
VT#1 on STS#3	VT1-5-1-3-1-1	VT1-6-1-3-1-1
VT#2 on STS#3	VT1-5-1-3-2-4	VT1-6-1-3-2-4
STS#4	STS-5-1-4	STS-6-1-4
STS#5	STS-5-1-5	STS-6-1-5
VT#3 on STS#6	VT1-5-1-6-1-1	VT1-6-1-6-1-1

- For rolling a set of circuits onto a different facility (bulk roll), use an ENT-BULKROLL command similar to the following example:

  ENT-BULKROLL-OC48:CISCO:FAC-5-1:123:::RTOSTART=STS-6-1-1, RFROMSTART=STS-5-1-1,RFROMEND=STS-5-1-4,RMODE=AUTO,CMDMDE=FRCD;

  This command will roll the paths shown in Table 2-9.

Table 2-9 One-Way Circuit Single Bulk Roll with ENT-BULKROLL

Paths	Before Roll	After Roll
STS#1	STS-5-1-1	STS-6-1-1
STS#2	STS-5-1-2	STS-6-1-2
VT#1 on STS#3	VT1-5-1-3-1-1	VT1-6-1-3-1-1
VT#2 on STS#3	VT1-5-1-3-2-4	VT1-6-1-3-2-4
STS#4	STS-5-1-4	STS-6-1-4

Step 2 If you performed a manual roll, you must confirm that the circuit is valid by issuing the RTRV-BULKROLL-<OCN_TYPE> command.

Input format:

RTRV-BULKROLL-<OCN_TYPE>:[<TID>]:<SRC>:<CTAG>;

Input example:

RTRV-BULKROLL-OC12:CISCO:FAC-3-1:1;

Create a One-Way Circuit Dual Roll

In this procedure, both the source and destination nodes are rolled. There are two types of dual rolls:

- Dual roll for a single circuit within the same facilities but to a different time slot
- Dual roll for a single circuit from one span card to another span card

Step 1 Determine the type of roll that you want to perform on the source node and follow the steps in the "Create a One-Way Circuit Single Roll" section on page 2-50.

Step 2 Determine the type of roll that you want to perform on the destination node and follow the steps in the "Create a One-Way Circuit Single Roll" section on page 2-50.

2.9.5 Protection Rolling Procedures

To perform protection rolls, follow the procedures in the "2.9.3 Two-Way Circuit Single Roll and Dual Roll Procedures" section on page 2-48 and the "2.9.4 One-Way Circuit Single Roll and Dual Roll Procedures" section on page 2-50.

Note Before performing a protection roll, either from one protection group to another or within the same protection group, the protection group must already be provisioned.

Table 2-10 shows what kind of protection rolls are supported from one domain to another. An X indicates the roll is allowed. A dash indicates that the roll is not allowed.

Table 2-10 Supported Protection Rolls

	Roll To Domain				
Roll From Domain	**BLSR**	**PCA**	**1+1**	**Path Protection**	**Unprotected**
BLSR	X	X	X	—	X
PCA	X	X	X	—	X
1+1	X	X	X	—	X
Path Protection	—	—	—	X	—
Unprotected	X	X	X	—	X

2.10 1:N Low-Density to 1:N High-Density Upgrade

In the Cisco ONS 15454, Cisco ONS 15454 M2, and Cisco ONS 15454 M6 DS1 electrical cards can be upgraded to DS1/E1-56 high-density cards using TL1. This procedure can be performed only when logged in as a Superuser.

Note

- Protect cards must be upgraded before working cards because working cards cannot have more capabilities than their protect card.
- You cannot upgrade electrical cards from low-density to high-density if the low-density electrical cards are installed in Slots 4, 5 or 6 on the A side or 12, 13 or 14 on the B side of the shelf. Only cards in slots 1, 2, 16 and 17 can be upgraded to high-density electrical cards.
- The following limitations apply when upgrading low-density electrical cards to high-density electrical cards:
  - The protect card must be in a protection group.
  - The protect card must not protect any low-density electrical cards on Slots 4, 5, or 6 if on the A-Side of the shelf, or Slots 12, 13, or 14 if on the B-Side of the shelf.

- Perform this procedure on low-density cards that are already in 1:N protection.

Step 1 On the protect card, change the card type from low-density to high-density.

Input format:

CHG-EQPT:[<TID>]:<AID>:<CTAG>::<EQPTTYPE>:[PPMTYPE=PPMTYPE>],[PPMNUM=<PPMNUM>],[PORTNUM=<PORTNUM>],[PORTRATE=<PORTRATE>];

Input example:

CHG-EQPT::SLOT-15:123::DS1-E1-56;

Step 2 Physically remove the low-density protect card and insert the high-density protect card.

Step 3 Switch the traffic from the working card to the protect card.

Input format:

SW-TOPROTN-EQPT:[<TID>]:<AID>:<CTAG>::[<MODE>],[<PROTID>],[<DIRN>];

Input example:

SW-TOPROTN-EQPT::SLOT-16:123::FRCD,SLOT-15,BTH;

Step 4 On the working card, change the card type from low-density to high-density.

Input format:

CHG-EQPT:[<TID>]:<AID>:<CTAG>::<EQPTTYPE>:[PPMTYPE=PPMTYPE>],[PPMNUM=<PPMNUM>],[PORTNUM=<PORTNUM>],[PORTRATE=<PORTRATE>];

Input example:

CHG-EQPT::SLOT-16:123::DS1-E1-56;

Step 5 Physically remove the working low-density card and insert the high-density card.

Step 6 Switch the traffic back onto the working high-density card.

Input format:

SW-TOWKG-EQPT:[<TID>]:<AID>:<CTAG>::[<MODE>],[<DIRN>];

Input example:

SW-TOWKG-EQPT::SLOT-16:123::FRCD,BTH;

Step 7 Repeat these steps to upgrade the other low-density card in the protection group.

2.11 Remote Monitoring-Managed PMs

This section describes the retrieval, threshold setting, threshold crossing alerts (TCAs) and scheduled PM reporting for all the remote monitoring (RMON)-managed PM data in the Cisco ONS 15310-MA, Cisco ONS 15454, Cisco ONS 15454 M2, and Cisco ONS 15454 M6.

The cards that support RMON PMs include: G1K-4, CE-1000-4, ML1000-2/ML100T-12, FC_MR-4, ASAP-4, MXP_MR_2.5G/MXPP_MR_2.5G, and ML-100T-8/CE-100T-8. The PM types for these cards include Ethernet statistic types defined in standard Simple Network Management Protocol (SNMP)/RMON MIBs, and also include other statistic types managed by RMON, for example, the Fibre Channel statistic types.

When creating an RMON threshold, there are two threshold values that need to be specified. The first threshold is the rising threshold and the other is the falling threshold. There are other parameters that need to be specified when creating the RMON threshold, for example, the startup type and the sample type.

Note There can be more than one threshold defined for each RMON statistic type.

The current bucket is not defined by the RMON. RMON-managed PM only shows the history data of the PMs and the data accumulated since the last time the counters are cleared (RAW-DATA).

In the RMON TCA, the accumulation time period is not the predefined PM bucket accumulation time, such as 15-MIN or 1-DAY. It can be any integer (any time greater than 10 seconds) that is defined when creating the RMON threshold.

Note For platform-specific PM information, refer to the Procedure Guide and Reference Manual of that platform.

2.11.1 RTRV-PM-<MOD2>

The RTRV-PM-<MOD2> command retrieves the RMON-managed PMs.

The TL1 modifiers FSTE/GIGE/POS are used to retrieve the RMON-managed Ethernet PMs if the Ethernet port is an FSTE/GIGE/POS port type. The FC modifier retrieves the RMON-managed Fibre Channel PMs.

There are three accumulation time periods for RMON statistics: 1-MIN, 1-HR, and RAW-DATA. For RMON-managed PMs, only history PM buckets and RAW-DATA are supported and there is no current bucket defined for RMON-managed PMs. When RAW-DATA is specified in the input of RTRV-PM, the date and time specified in the input will be ignored. The MONDATE and MONTIME in the output will be the last time the counters were cleared. RAW-DATA will be the default TMPER value for RMON-managed PM retrieval.

Because RMON PM only supports the history data if the accumulation time period is 1-MIN, 15-MIN, 1-HR, or 1-DAY, you must specify the correct history PM bucket for the RTRV-PM command to succeed.

When retrieving PM, if an unsupported MONYYPR is specified, an error message will be returned.

Currently there is no support of LOCN (location) and DIRN (direction) for RMON-managed data statistics.

Input Format

RTRV-PM-<MOD2>:[<TID>]:<AID>:<CTAG>::[<MONTYPE>],[<MONLEV>],[<LOCN>],[<DIRECTION>],[<TMPER>],[<DATE>],[<TIME>];

Input Example

RTRV-PM-GIGE:TID:FAC-2-1:123::ETHERSTATSOCTETS,,,,1-MIN,04-11,12-45;

RTRV-PM-GIGE:TID:FAC-2-1:123::,,,,RAW-DATA;

Output Format

SID DATE TIME
M CTAG COMPLD

"<AID>,[<AIDTYPE>]:<MONTYPE>,<MONVAL>,[<VLDTY>],[<LOCN>],[<DIRECTION>],[<TMPER>],[<MONDAT>],[<MONTM>]"
;

Output Example

TID-000 1998-06-20 14:30:00
M 001 COMPLD
"FAC-2-1,GIGE:etherStatsOctets,21,COMPL,,,1-MIN,04-11,12-45"
;

Table 2-11 shows the error messages associated with the RTRV-PM-<MOD2> command.

Table 2-11 Error Messages for RTRV-PM-<MOD2>

Error Code	Description	Scenario When the Error Message is Sent
IDNV	TMPER Type Not Supported	The TMPER parameter specified is not applicable for the MOD2 type. For example, 1-MIN is not applicable for OC48 PM types.
IDNV	Current Interval Not Supported For RMON PMs	The current interval is specified by default, or is explicitly specified by MONDAT/MONTM, when the TMPER is 1-MIN, 15-MIN, 1-HR, or 1-DAY.

2.11.2 ENT-RMONTH-<MOD2_RMON>

The ENT-RMONTH-<MOD2_RMON> command creates a threshold type (an entry in the RMON alarm table) for an RMON statistic, for the RMON-managed PMs. An event (TCA) is generated and reported when the threshold is crossed in the appropriate direction during the sampled time period.

More than one threshold can be created by using different parameters (rising/falling threshold), for each MONTYPE.

This command applies to G1000, GIGE, FSTE, POS, and FC data objects.

Input Format

ENT-RMONTH-<MOD2_RMON>:[<TID>]:<SRC>:<CTAG>::<MONTYPE>,,,,<INTVL>:RISE=<RISE>,FALL=<FALL>,[SAMPLE=<SAMPLE>],[STARTUP=<STARTUP>][:];

Input Example

The following example creates an entry in the RMON threshold table for the etherStatsOctets statistic type with an interval equal to 100 seconds, rising threshold of 1000, falling threshold of 100, DELTA sampling type, and startup type of RISING-OR-LTING.

ENT-RMONTH-GIGE:CISCO:FAC-2-1:123::ETHERSTATSOCTETS,,,,100:RISE=1000,
FALL=100,SAMPLE=DELTA,STARTUP=RISING-OR-LTING;

Table 2-12 shows the error messages associated with the ENT-RMONTH-<MOD2_RMON> command.

Table 2-12 Error Messages for ENT-RMONTH-<MOD2_RMON>

Error Code	Description	Scenario When the Error Message is Sent
IDNV	Invalid Interval	The input interval value is less than 10.
IDRG	Invalid Threshold Value	The rising/falling threshold is less than 0, or the falling threshold is greater than or equal to rising threshold.
IDNV	Invalid MONTYPE value	The MONTYPE is not applicable to the data type (represented by the MOD2).
IIDT	Cannot Create More RMON Threshold	The number of RMON thresholds created has reached the maximum (256).
IIDT	Duplicate RMON Threshold	There already is a threshold created with the exact same parameters.

2.11.3 DLT-RMONTH-<MOD2_RMON>

The DLT-RMONTH-<MOD2_RMON> command deletes a threshold type (an entry in the RMON alarm table) created for a MONTYPE (RMON statistic type). Because there can be multiple thresholds created for a particular MONTYPE, you must specify all the necessary parameters for the threshold in order to identify the particular threshold to be deleted.

This command applies to G1000, GIGE, FSTE, POS, and FC data objects.

Input Format

DLT-RMONTH-<MOD2>:[<TID>]:<AID>:<CTAG>::<MONTYPE>,,,,<INTVL>:RISE=<RISE>, FALL=<FALL>,[SAMPLE=<SAMPLE>,][STARTUP=<STARTUP>][:];

Input Example

The following example deletes an entry in the RMON threshold table for the etherStatsOctets statistic type, with an interval equal to 100 seconds, rising threshold of 1000, falling threshold of 100, DELTA sampling type, and startup type of BOTH.

DLT-RMONTH-GIGE:CISCO:FAC-2-1:123::ETHERSTATSOCTETS,,,,100:RISE=1000,FALL=100, SAMPLE=DELTA,STARTUP=BOTH;

Table 2-13 shows the error messages associated with the DLT-RMONTH-<MOD2_RMON> command.

Table 2-13 Error Messages for DLT-RMONTH-<MOD2_RMON>

Error Code	Description	Scenario When the Error Message is Sent
IDNV	Invalid Interval	The input interval value is less than 10.
IDRG	Invalid Threshold Value	The rising/falling threshold is less than 0, or the falling threshold is greater than or equal to rising threshold.
IDNV	Invalid MONTYPE value	The MONTYPE is not applicable to the data type (represented by the MOD2).
SROF	RMON Threshold Does Not Exist	The RMON threshold you are trying to delete does not exist.

2.11.4 RTRV-RMONTH-<MOD2_RMON>

The RTRV-RMONTH-<MOD2_RMON> command retrieves the thresholds defined in the RMON alarm table.

Input Format

RTRV-RMONTH-<MOD2>:[<TID>]:<AID>:<CTAG>::[<MONTYPE>]>,,,,
[<INTVL>]:[RISE=<RISE>,][FALL=<FALL>,][SAMPLE=<SAMPLE>,][STARTUP=<STARTUP>];

Input Example

The following example retrieves all the thresholds defined in the RMON threshold table for the etherStatsOctets statistics type.

RTRV-RMONTH-GIGE:TID:FAC-2-1:123::ETHERSTATSOCTETS;

The following example retrieves all the thresholds for the etherStatsOctets statistics type with the DELTA sampling type and RISING startup type defined in the RMON threshold table.

RTRV-RMONTH-GIGE:CISCO:FAC-2-1:123::ETHERSTATSOCTETS:SAMPLE=DELTA,
STARTUP=RISING;

Output Format

```
   SID DATE TIME
M  CTAG COMPLD
   "<AID>,[<AIDTYPE>]:<MONTYPE>,,,,[<INTVL>]:INDEX=<INDEX>,RISE=<RISE>,
   FALL=<FALL>,SAMPLE=<SAMPLE>,STARTUP=<STARTUP>"
;
```

Output Example

```
   TID-000 1998-06-20 14:30:00
M  001  COMPLD
   "FAC-2-1,GIGE:ETHERSTATSOCTETS,,,,100:INDEX=2,RISE=1000,FALL=100,
   SAMPLE=DELTA,STARTUP=RISING"
;
```

Table 2-14 shows the error messages associated with the DLT-RMONTH-<MOD2_RMON> command.

Table 2-14 Error Messages for RTRV-RMONTH-<MOD2_RMON>

Error Code	Description	Scenario When the Error Message is Sent
IDNV	Invalid Interval	The input interval value is less than 10.
IDRG	Invalid Threshold Value	The rising/falling threshold is less than 0, or the falling threshold is greater than or equal to rising threshold.
IDNV	Invalid MONTYPE value	The MONTYPE is not applicable to the data type (represented by the MOD2).
SROF	RMON Threshold Does Not Exist	The RMON threshold you are trying to delete does not exist.

2.11.5 REPT EVT <MOD2ALM> for Threshold Crossing Events

The REPT EVT <MOD2ALM> autonomous message reports the threshold crossing event for the RMON statistics. The high threshold (HT) designator is generated when crossing the RISING threshold. The low threshold (LT) is generated when crossing the FALLING threshold.

The table index for thresholds in the RMON alarm table is enclosed in the text of the TCA description. This table index also appears in the output of the RTRV-RMONTH command. You can retrieve additional information regarding the threshold that generates the TCA by issuing the RTRV-RMONTH command and comparing the output with corresponding table index.

Output Format

```
   SID DATE TIME
M  CTAG COMPLD

"<AID>:<CONDTYPE>,[<CONDEFF>],[<OCRDAT>],[<OCRTM>],[<LOCN>],[<DIRN>],[<MONV
AL>], [<THLEV>],[<TMPER>]:[<DESC>],[<AIDDET>]"
;
```

Output Example

```
   VA454-23 2000-02-20 08:47:03
A  512.512 REPT EVT G1000
   "FAC-2-1,G1000:T-ETHERSTATSOCTETS-HT,TC,09-30,23-59-59,,,1003,
   1000,:\"RMON THRESHOLD CROSSING ALARM # 1 \",G1000-4"
;
```

2.11.6 INIT-REG-<MOD2>

This command initializes the PM registers.

This command applies to G1K-4, GIGE, FSTE, and FC data objects.

Only RAW-DATA is allowed to be specified for TMPER because no history data will be cleared for RMON-managed PMs by INIT-REG-<MOD2>.

2.11.7 SCHED-PMREPT-<MOD2>

This command schedules/reschedules the NE to report the performance monitoring data.

The three accumulation time periods form RMON statistics are: 1-MIN, 1-HR, and RAW-DATA.

2.11.8 RTRV-PMSCHED-<MOD2>

This command retrieves the RMON statistics reporting schedule that was set for the NE by the SCHED-PMREPT-<MOD2> command.

The LOCN parameter is optional in the output of RTRV-PMSCHED-<MOD2>, and no LOCN information will be given in the output of RTRV-PMSCHED for RMON PM schedule.

2.11.9 REPT PM <MOD2>

Reports autonomous monitoring statistics as a result of the schedule created by SCHED-PMREPT-<MOD2>.

The LOCN parameter is optional in the output of REPT PM <MOD2> message, and no LOCN information will be given in the output of REPT PM <MOD2>.

2.11.10 REPT DBCHG

Reports any changes on the NE that result from issuing the following commands:

- ENT-RMONTH-<MOD2>
- DLT-RMONTH-<MOD2>

Also reports when an RMON PM schedule is created or deleted through the SCHED-PMREPT-<MO2> command.

2.11.11 MONTYPE and CONDEF Defined for TCA

The names of Ethernet and Fibre Channel MONTYPEs are defined exactly as they are defined in the corresponding SNMP MIB statistics group. For example, etherStatsUndersizePkts will be used as the name for the same RMON statistics defined in request for comment (RFC)1757.

Unlike the PM parameters of other SONET entities (such as STS path and OCn), there are two CONDEFs defined for the TCAs of each RMON-managed statistics type: Ethernet or Fibre Channel MONTYPE. One CONDEF is for the rising threshold, and the other is for the falling threshold. For example, there are two CONDEFs for the etherStatsUndersizePkts statistics type: T-etherStatsUndersizePkts-HT for the rising threshold, and T-etherStatsUndersizePkts-LT for the falling threshold.

Note For platform-specific PM information, refer to the Procedure Guide and Reference Manual of that platform.

2.11.12 Enumerated Types

2.11.12.1 TMPER

Table 2-15 shows the possible TMPER values.

Table 2-15 TMPER Type

Values	Description
1-DAY	Performance Parameter Accumulation Interval Length - Every 24 Hours. For SONET PM data (line/session/path), only 1 day of history data is available. For RMON managed data statistics, 7 days of history data are available.
15-MIN	Performance Parameter Accumulation Interval Length - Every 15 Minutes. 32 15-MIN buckets of history data are available for this accumulation interval length.
1-MIN	Performance Parameter Accumulation Interval Length - Every 1 minute. Only applicable to RMON statistics. 60 minutes of history data are available for this accumulation interval length.
1-HR	Performance Parameter Accumulation Interval Length - Every 1 Hours. Only applicable to RMON statistics. 24 hours of history data are available for this accumulation interval length.
RAW-DATA	The data shown is accumulated starting from the last time the counters are cleared. This is only applicable to RMON-managed PMs.

2.11.12.2 SAMPLE_TYPE

SAMPLE_TYPE (Table 2-16) describes how the data will be calculated during the sampling period.

Table 2-16 SAMPLE_TYPE

Value	Description
ABSOLUTE	Comparing directly.
DELTA	Comparing with the current value of the selected variable subtracted by the last sample.

2.11.12.3 STARTUP_TYPE

STARTUP_TYPE (Table 2-17) indicates whether an event will be generated when the first valid sample is crossing the rising or falling threshold.

Table 2-17 STARTUP_TYPE

Value	Description
RISING	Generate the event when the sample is greater than or equal to the rising threshold.
FALLING	Generate the event when the sample is smaller than or equal to the falling threshold.
RISING-OR-LTING	Generate the event when the sample is crossing the rising or falling threshold.

2.11.13 Notes for DWDM Card Types

The PM for client port and/or optical channel (OCH) can include both the RMON-managed PM and the SONET PM when the client payload is provisioned as 1GFC, 2GFC, 10GFC, 1GFICON, 2GFICON, GIGE, or 10GIGE for the following cards:

- MXP_2.5G_10G
- TXP_MR_10G
- TXP_MR_2.5G
- TXP_MR_10E
- MXP_MR_2.5G

2.11.13.1 Client Port of DWDM Cards

When the client port of a dense wavelength division multiplexing (DWDM) card is provisioned as 1GFC, 2GFC, 10GFC, 1GFICON, 2GFICON, GIGE, or 10GIGE, the applicable PM for the client port includes both the RMON-managed PM and the SONET PM. Therefore, the behavior of the RTRV-PM-<MOD2>, INIT-REG-<MOD2>, and SCHED-PMREPT-<MOD2> commands is different from the Ethernet or Fibre Channel port of the other cards where only RMON PM is applicable. The differences include:

- LOCN and DIRN parameters are applicable to the RTRV-PM-<MOD2>, INIT-REG-<MOD2>, and SCHED-PMREPT-<MOD2> commands because they are applicable to the SONET optics PM. When the LOCN or DIRN parameter is specified, it only applies to the SONET optics PM.
- Because 1-MIN, 1-HR, or RAW-DATA are not applicable to the SONET optics PM, no SONET optics PM would be returned in the output of RTRV-PM. If RAW-DATA is specified in the input of the INIT-REG command, no SONET optics PM counter will be cleared.
- When the accumulation time period is specified as 15-MIN or 1-DAY and the PM history bucket is specified as 0 (current bucket), only the SONET optics PM will be returned in the output of the RTRV-PM command. No RMON-managed PM will be included in the output of the RTRV-PM command because the RMON PM does not have current bucket.
- A SONET optics PM MONTYPE cannot be specified in the input of the INIT-REG command. Only the SONET optics PM counters will be cleared. When the ALL MONTYPE is specified, both the RMON and the SONET optics PM counters will be cleared.
- The commands used to manage RMON thresholds (ENT-RMONTH, DLT-RMONTH, and RTRV-RMONTH) are only applicable to the RMON PM of the client port. The SONET optics PM thresholds of the client port are still managed by the SET-TH and RTRV-TH commands. For example, if the client port type of an MXP_MR_2.5G card is provisioned as GIGE, the following command would be used to create an RMON threshold:

  ENT-RMONTH-GIGE::FAC-2-1-1:1::IFINOTETS,,,,1000:RISE=1000,FALL=900;

  In the same client port, the following command would be used to set the SONET the optics PM threshold:

  SET-TH-GIGE::FAC-2-1-1:1LBCL-MIN,0.2;

2.11.13.2 OCH Port of DWDM Cards

The optical channel (OCH) port of the TXP_MR_10G and TXP_MR_10E cards include the RMON-managed 8B10B PM as well as the other SONET PMs, when their client port is provisioned as GIGE, 10GIGE, 1GFC, 2GFC, or 10GFC.

The RTRV-PM-OCH, INIT-REG-OCH, SCHED-PMREPT-OCH, and REPT PM OCH commands have behaviors similar to those mentioned in the "2.11.13.1 Client Port of DWDM Cards" section on page 2-61.

2.12 Rules for Framing Type Autoprovisioning in CTC Versus TL1

The DS3, DS3E, DS3XM, DS3i, and DS1 cards can autosense framing and set the format accordingly; however, this framing autosense feature can only be set using CTC. Use CTC to set the frame format (FMT) attribute on DS3, DS3E, DS3XM, DS3i, and DS1 cards to autoprovision. The FMT field will blank out for a few seconds while the card is determining the framing mode received by that particular port. The FMT field is set accordingly to unframed, M23, or CBit. If the card is not present (preprovisioned), setting the FMT field to autoprovision will result in the FMT field defaulting to unframed.

The TL1 interface does not support the autoprovision option for the DS3, DS3E, DS3XM, DS3i, and DS1 cards; it only supports unframed, M23, or CBit. If autoprovision is selected from CTC and at the same time the TL1 command RTRV-T3 is issued, the TL1 output will indicate the FMT field as unframed during the time period that the card (if present) is autosensing the frame format. If the card is not present (preprovisioned), the response of the RTRV-T3 command (after CTC sets the FMT to autoprovision) will indicate the FMT field as unframed.

2.13 Provisioning Rules for Transponder and Muxponder Cards

This section provides provisioning rules associated with the following cards and their pluggable port modules (PPMs):

- MXP_2.5G_10G
- TXP_MR_10G
- TXP_MR_2.5G
- TXPP_MR_2.5G
- MXP_2.5G_10E
- TXP_MR_10E
- MXP_MR_2.5G
- MXPP_MR_2.5G
- GE_XP
- 10GE_XP
- GE_XPE
- 10GE_XPE
- OTU2_XP
- ADM_10G

2.13.1 PPM Provisioning Rules

To provision PPMs, use the **ENT-EQPT** command.

Example 2-32 provisions the first PPM.

Example 2-32 Provision the first PPM on Slot 2

ENT-EQPT::PPM-2-1:100::PPM-1PORT;

To delete PPM provisioning, use the DLT-EQPT command.

2.13.2 Payload Provisioning Rules

The following rules apply when provisioning a payload:

- PPM must first be provisioned.
- When changing the payload data type:
  - All ports being edited must be in the Out-of-Service and Management, Disabled (OOS-MA,DSBLD) state because this change is service affecting.
  - All ports being edited must not have any DCC terminations.
  - All ports being edited must not be part of any timing source.
  - The section trace mode of all ports being edited must be OFF.
  - For all regeneration and retiming (2R) payload types, trunk ports must not have GCC termination or optical transport network/forward error correction (OTN/FEC) enabled.
  - The payload cannot be changed if any ports being edited are part of a Y-cable protection group.
  - The payload cannot be changed if any of the ADM-10G and OTU2_XP ports being edited are part of the APS (Automatic Protection Switching) protection group.
  - Only the TXP, GE_XP, 10GE_XP, GE_XPE, 10GE_XPE, and OTU2_XP cards can be used for the 10GIGE payload. Termination mode must be set to TRANSPARENT-AIS or TRANSPARENT-SQUELCH (TRANSPARENT-SQUELCH is only supported on TXP_MR_10E).
- To set the payload to a speed other than OC-3, OC-12, OC-48, or OC-192, the termination mode must be set to TRANSPARENT-AIS or TRANSPARENT-SQUELCH (TRANSPARENT-SQUELCH is only supported on TXP_MR_10E). For Fibre Channel cards and all 2R payload types, the termination mode is not applicable and must be set to TRANSPARENT-AIS or TRANSPARENT-SQUELCH.
- Changing the payload while in a regeneration group requires unprovisioning the regeneration group, unprovisioning the payload, reprovisioning the payload, and reprovisioning the regeneration group.

To provision the payload, use the following commands:

- **ENT-(OCn, nGIGE, nGFC, 2R)**
- **DLT-(OCn, nGIGE, nGFC, 2R)**
- **ED-(OCn, nGIGE, nGFC, 2R)**

2.13.3 OC-N Payload Provisioning Parameters

SONET payloads are supported by DWDM cards according to Table 2-18. These payloads are configurable only for the Section and Line layers. STS layers cannot be provisioned or retrieved.

Table 2-18 Payload/Card Mode Support

Card Type	Payload	Card Mode
TXP_MR_10G	OC192	DWDM-LINE
	10GIGE	DWDM-SECTION DWDM-TRANS-AIS With REGEN group: DWDM-TRANS-AIS
MXP_2.5G_10G	OC48	DWDM-LINE DWDM-SECTION DWDM-TRANS-AIS
TXP_MR_2.5G and TXPP_MR_2.5G	1GIGE, 1GF, 1GFICON, 2GFICON, ESCON, ISC1, ISC3, ETRCLO, DV6000, HDTV, D1VIDEO	With REGEN group: DWDM-TRANS-AIS Must be DWDM-TRANS-AIS. Requires the DWRAP and FEC disabled on the network/OCH ports.
	OC3, OC12, OC48	DWDM-LINE DWDM-SECTION DWDM-TRANS-AIS
TXP_MR_10E	OC192	DWDM-LINE DWDM-SECTION DWDM-TRANS-AIS DWDM-TRANS-SSQUELCH
	10GIGE, 10GFC	DWDM-TRANS-AIS DWDM-TRANS-SQUELCH With REGEN group: DWDM-TRANS-AIS DWDM-TRANS-SQUELCH
MXP_2.5G_10E	OC48	DWDM-SECTION DWDM-TRANS-AIS DWDM-TRANS-SQUELCH
MXP_MR_2.5G and MXPP_MR_2.5G	Port-1: 1GFC, 1GFICON, GIGE Port-2: 1GFC, 2GFC, 1GFICON, 2GFICON, GIGE[1]	FCGE[2]
GE_XP and GE_XPE	GIGE, 10GIGE	GEXP-10x1Gx2-MXP GEXP-20x1G-MXP GEXP-L2ETH
10GE_XP and 10GE_XPE	GIGE, 10GIGE	10GEXP-TXP 10GEXP-L2ETH

Table 2-18 Payload/Card Mode Support (continued)

Card Type	Payload	Card Mode
OTU2_XP	OC192, 10GIGE	DWDM-TRANS-AIS DWDM-TRANS-SQUELCH DWDM-SECTION DWDM-LINE
ADM_10G	OC3, OC12, OC48, GIGE	—

1. If 2GFC or 2GFICON is on Port-2, then Port-1 must be unprovisioned. If Port-1 is provisioned, then Port-2 cannot contain 2GFC or 2GFICON because of bandwidth limitations. Ports 3 through 8 are not available. ESCON payload is not supported.
2. ESCON and mixed card modes are not supported.

The configuration parameters for OC-N ports can be retrieved/edited using the ED-<OCN_TYPE> and RTRV-<OCN_TYPE> commands. The following conditions apply when using the ED-<OCN_TYPE> and RTRV-<OCN_TYPE> commands:

- DCC parameters are used to enable and disable SDCC functionality.
- Line DCC (LDCC) parameters are used to enable and disable LDCC functionality.
- SYNMSG and SENDDUS synchronization parameters are applicable only to cards supporting synchronization: MXP-2.5G-10G, TXP-MR-10E, MXP-2.5G-10E, OTU2_XP, and ADM-10G.
- Signal fail can be provisioned using the SFBER parameter.
- Signal degrade can be provisioned using the SDBER parameter.
- Soak time and administrative/service state parameters can be provisioned using SOAK, SOAKLEFT, PST, SST, and CMDMDE parameters.
- The SONET/SDH selection can be provisioned using the MODE parameter.
- The name of the facility can be provisioned using the NAME parameter.
- The J0 Section Trace parameters can be provisioned using the EXPTRC, TRC, INCTRC, TRCMODE, and TRCFORMAT parameters.

2.13.4 Termination Mode Provisioning Rules

The following rules apply when provisioning the termination mode:

- It is a card-level operation.
- Termination mode is only applicable to the OC-3, OC-12, OC-48, and OC-192 payload types.
- Changing termination mode requires the following:
  - All ports must be in the Out of Service (OOS) state because this change is traffic-affecting.
  - All ports must not have DCC terminations (GCC is not applicable).
  - The J0 Section Trace Mode on all ports must be OFF.
  - The trunk port must not be part of any timing source.
  - If any port is Y-cable protected, these rules also apply to the peer slot.
- Section and Line termination modes are supported for the OC-3, OC-12, OC-48, and OC-192 payloads.

- You cannot change the termination mode if the port is part of a Y-cable protection or regeneration group.
- Termination mode provisioning does not apply to MXP_MR_2.5G, MXPP_MR_2.5G, and ADM-10G cards.

To set the termination mode, use the following commands:

- **ENT-EQPT**
- **ED-EQPT**

Example 2-33 sets the termination mode of the card in Slot 1 to DWDM-LINE.

Example 2-33 Set the Termination Mode

```
ED-EQPT::SLOT-1:116:::CARDMODE=DWDM-LINE
```

2.13.5 Wavelength Provisioning Rules

The following rules apply when provisioning the wavelength:

- Change the trunk wavelength of all the trunk ports to OOS state because this change is service-affecting.
- Set the wavelength to the first tunable wavelength, which will cause the first wavelength from the card manufacturing data to be used as the operational wavelength.
- If the provisioned wavelength is set to the first tunable wavelength, any removal of an operational card and subsequent replacement with a card for a different wavelength will not cause a mismatch alarm to be raised.
- To receive the mismatch alarm notification, you need to explicitly provision the wavelength and not use the first tunable wavelength.

To set the card-level wavelength, use the following commands:

- **ENT-EQPT**
- **ED-EQPT**

Example 2-34 sets the card-level wavelength of the card in Slot 1 to 150.33.

Example 2-34 Set the Card-Level Wavelength

ED-EQPT:VA454-22:SLOT-1:116:::PWL=1530.33;

2.13.6 Regeneration Group Provisioning Rules

The following rules apply when provisioning the regeneration group:

- Both the TXPP and TXP versions of the transponder card can be used in a regeneration group.
- When the TXPP card is used as a regeneration group, the LOCKOUT_OF_PROTECTION, inhibit switching command must be issued on the working trunk port.
- The inhibit switching command cannot be unlocked until the regeneration group is unprovisioned for the TXPP.
- Regeneration group provisioning is denied if there is a FORCE or MANUAL switching command already provisioned on the trunk ports for the TXPP.

- A regeneration group enables the continuation of the client signal across multiple spans.
- The peer-slot must not be itself.
- The peer-slot must be provisioned or preprovisioned.
- The peer-slot must not be part of another regeneration group.
- The peer-slot must not be part of a Y-cable protection group.
- Both cards must have the same card type.
- Both cards must have the same payload type and data rate.
- Both cards must have the same ITU-T G.709 OTN status.
- Both cards must have the same FEC status.
- Termination mode must be set to TRANSPARENT-AIS or TRANSPARENT-SQUELCH mode.

To set the card-level regeneration group, use the following commands:

- **ED-EQPT**
- **ENT-EQPT**

Example 2-35 sets a card-level regeneration group for Slot 2.

Example 2-35 Set Card-Level Regeneration Group

```
ED-EQPT::SLOT-2:CTAG:::PROTID=SLOT-2,NAME=REGENGROUPNAME;
```

2.13.7 DCC/GCC Provisioning Rules

The following rules apply when provisioning DCC and GCC:

- The DCC can be provisioned on the client port of a TXP or MXP card.
- 2R payload types do not support GCC.
- To provision a DCC, the payload data type must be set to OC-3, OC-12, OC-48, or OC-192.
- To provision a DCC, the termination mode must be set to Line or Section terminated (if the card supports provisionable termination mode).
- The DCC can be provisioned on the trunk line provided that ITU-T G.709 is provisionable and the ITU-T G.709 OTN status is turned off:
  - To provision a GCC on the trunk port, ITU-T G.709 should be enabled.
  - To provision a DCC on the trunk port, ITU-T G.709 should be disabled.
- Only the working client port in a Y-cable protection scheme can be provisioned with DCC.
- Only the working trunk port in a splitter protection scheme can be provisioned with DCC or GCC.

To provision DCC, use the **ED-(OCn, nGIGE, NGFC)** command.

Example 2-36 provisions DCC.

Example 2-36 Provision DCC

```
ED-OC192::FAC-1-1-1:100:::COMM=DCC:OOS,AINS;
```

To provision GCC, use the **ED-OCH** command.

Example 2-37 provisions GCC.

Example 2-37 Provision GCC

```
ED-OCH::CHAN-6-2:114::COMM=GCC:OOS,AINS;
```

2.13.8 ITU-T G.709 OTN, FEC, and OTN SDBER/SFBER Provisioning Rules

The following rules apply when provisioning ITU-T G.709 OTN, FEC, and OTN SDBER/SFBER:

- The ITU-T G.709 OTN, FEC, and OTN SDBER/SFBER can only be provisioned on the trunk port.
- 2R (transparent) payload types (HDTV, passthrough) do not support ITU-T G.709 OTN or FEC.
- To enable ITU-T G.709 OTN:
  - All trunk ports must be in the OOS state.
  - All trunk ports must not have any SDCC provisioned.
- To disable ITU-T G.709 OTN:
  - All trunk ports must be in the OOS state.
  - All trunk ports must not have any GCC or active trail trace identification (TTI) mode provisioned.
- FEC status can be enabled only if ITU-T G.709 is enabled.
- To change FEC status, all trunk ports must be in the OOS state.
- Only ITU-T G.709 OTN, FEC status, and the SDBER/SFBER setting on the working trunk port can be changed in the protected version of the TXP card. The value provisioned on the working trunk port will be reflected on the protect trunk port.
- The ITU-T G.709 OTN is only provisionable in non-2R (or unframed) payload type.
- When ITU-T G.709 is turned on, the OTN SFBER value is always set to 1E-5 and no other BER values are provisionable.

To provision ITU-T G.709, FEC, and OTN SDBER/SFBER, use the **ED-OCH** command.

Example 2-38 provisions ITU-T G.709, FEC, and OTN SDBER/SFBER.

Example 2-38 Provision ITU-T G.709, FEC, and OTN SDBER/SFBER

```
ED-OCH::CHAN-6-2:114:::OSDBER=1E-6,DWRAP=Y,FEC=Y,:OOS,AINS;
```

2.13.9 Synchronization Provisioning Rules

The following rules apply when provisioning synchronization:

- The TXP_MR_10G, TXP_MR_2.5G, and TXPP_MR_2.5G cards are through-timed (passthrough) and cannot be used as a timing source. The GE_XP, 10GE_XP, GE_XPE, and 10GE_XPE cards do not support synchronization provisioning.
- The TXP_MR_10E card can be used as a timing reference (only on the client port, not the trunk port).
- A MXP_MR_2.5G, MXPP_MR_2.5G, OTU2_XP, or ADM-10G card trunk port can be used as a timing source.
- Only MXP ports can be used for a timing source. A trunk port is only allowed as a timing reference if ITU-T G.709 is off and the termination mode is Line or Section.

- All client ports of the ADM-10G cards are available for timing source when configured as SONET. GIGE payload cannot be used for timing source. Interlink port cannot be used for synchronization.
- All client ports of the MXP cards are available for timing source irrespective of termination mode.

To set port-level synchronization attributes, use the following commands:

- **ENT-OCn**
- **ED-OCn**
- **ED-OCH**

Example 2-39 sets port-level synchronization attributes.

Example 2-39 Set Port-Level Synchronization Attributes

```
ED-OC48::FAC-1-1-1:CTAG:::SYNCMSG=Y,SENDDUS=N:;
ED-OCH::CHAN-6-2:114:::SYNCMSG=N,SENDDUS=Y;:
:
```

2.13.10 Section Trace Provisioning (J0) Rules

The following rules apply when provisioning section trace (J0):

- The client and trunk ports support section trace only if the payload is OC-3, OC-12, OC-48, or OC-192.
- The client and the trunk ports support section trace only in Line or Section terminated mode.
- In Line termination mode, the supported trace modes are MANUAL and MANUAL_NO_AIS.
- In Section termination mode, only the MANUAL_NO_AIS trace mode is supported.
- The section trace supports 1-byte or 16-byte length trace format.
- The AUTO and AUTO-NO-AIS trace modes are not supported.
- No trace mode is applicable for 2R (unframed) payload types, for example, DV-6000, HDTV, and ESCON.
- The section trace received string should appear when the card is in TRANSPARENT-AIS or TRANSPARENT-SQUELCH termination mode and the payload is OC-3, OC-12, OC-48, or OC-192.
- When the client port is configured in a Y-cable or APS (Automatic Protection Switching) protection group, the received string is always retrieved from the active client port.
- If the line is Y-cable or APS protected, trace can only be provisioned on the working port. However, the provisioning will be duplicated between the two ports, that is, both ports will contain the same values. This rule applies to the following parameters: Mode, Format, Send String, and Expected String.
- The MXP_2.5G_10E card is used for client test connection on client ports. For the trunk port, the trail trace identification (TTI) is used.
- The TXP_MR_10E card is used to test connections on client trunk ports.
- On MXP_MR_2.5G/MXPP_MR_2.5G cards, the trunk port section trace can be provisioned following the rules for line-terminated SONET equipment.
- Section trace provisioning is not supported on GE_XP, 10GE_XP, GE_XPE, 10GE_XPE cards.

For section trace provisioning of client ports provisioned for OCn payload, use the ED-OCn command.

Example 2-40 provisions section trace for client ports.

Example 2-40 Section trace provisioning of client ports

```
ED-OC48::FAC-6-1-1:10:::EXPTRC="AAA",TRC="AAA",TRCMODE=MAN,
TRCFORMAT=16-BYTE;
```

For section trace provisioning of trunk/OCH DWDM ports, use the ED-TRC-OCH command.

Example 2-41 provisions section trace for client ports.

Example 2-41 Section Trace Provisioning of Trunk/OCH DWDM Ports

```
ED-TRC-OCH::CHAN-6-2:10:::EXPTRC="AAA",TRC="AAA",TRCMODE=MAN,
TRCLEVEL-J0,TRCFORMAT=64-BYTE;
```

2.13.11 Trail Trace Identification Provisioning Rules

The following rules apply when provisioning trail trace identification (TTI):

- For the TXPP_MR_2.5G card, TTI can be provisioned only on the working trunk port. However, the provisioning will be duplicated between the two ports. Both ports will contain the same values. This rule applies to the following parameters: Mode, Format, Send String, and Expected String.
- The TTI level trace supports only the 64-byte length trace format.
- The TTI level trace supports only the MANUAL and MANUAL_NO_AIS trace modes.
- The TTI received string is always retrieved from the active trunk port.
- The TTI level trace can be provisioned for Section and Path monitoring.
- MXP_MR_2.5G and MXPP_MR_2.5G cards do not support TTI.

To provision port-level trace, use the **ED-TRC-OCH** command.

Example 2-42provisions port-level trace.

Example 2-42 Provision Port-Level Trace

```
ED-TRC-OCH::CHAN-6-2:10:::EXPTRC="AAA",TRC="AAA",TRCMODE=MAN,
TRCLEVEL=TTI-PM,TRCFORMAT=64-BYTE;
```

2.13.12 PM (Performance Monitoring) and Alarm Threshold Provisioning Rules

The following rules apply when provisioning PM parameters and alarm thresholds:

- When the framing type is unframed, for example, HDTV and DV6000, only optics threshold provisioning and PM are applicable. Support for optics threshold provisioning and PM depends on the ESCON SFP type.
- Optics PM supports only Near End, 15MIN, and 1DAY interval buckets.
- When the framing type is Fibre Channel or Ethernet (for example, 1GFC, 1G Ethernet):
  - (TXP_MR_2.5G/TXPP_MR_2.5G, MXP_2.5G_10G, and TXP_MR_10G cards only) Only 8B10B threshold provisioning and PM are available.
  - 2G Fibre Channel does not support 8B10B threshold provisioning and PM.

- When the framing type is GIGE/10GIGE, all monitored PM parameter terminology will follow the current chassis type.
- (TXP_MR_2.5G/TXPP_MR_2.5G, MXP_2.5G_10G, and TXP_MR_10G cards only) 8B10B applies to both transmit (Tx) and receive (Rx) directions.
- 8B10B PM supports only Near End, 15MIN, and 1DAY interval buckets.
- The 8B10B layer is not used for MXP_2.5G_10E and TXP_MR_10E cards.
- When the framing type is SONET/SDH, all monitored PM parameter terminology follows the current chassis type.
- The OTN thresholds are only applicable if ITU-T G.709 OTN is enabled.
- The FEC thresholds are only applicable if ITU-T G.709 and FEC are enabled.
- If the line is configured in a Y-cable, APS protection, or splitter protection group, only the working line thresholds can be provisioned. The working line thresholds will be reflected on the protect line thresholds. This rule applies for all threshold types including ITU-T G.709 OTN and FEC thresholds.
- Payload PM can be independently retrieved for the working and protect ports.

To set port-level thresholds, use the **SET-TH-(OCn, nGIGE, nGFC, OCH)** command.

Example 2-43 sets port-level thresholds.

Example 2-43 Set Port-Level Thresholds

```
SET-TH-OC48::FAC-1-1-1:123::CVL,12,NEND,,15-MIN;
SET-TH-OCH::CHAN-6-1:123::ES-PM,12,NEND,,15-MIN;
```

To retrieve port-level thresholds, use the **RTRV-PM-(OCn, nGIGE, nGFC, OCH)** command.

Example 2-44 retrieves port-level thresholds.

Example 2-44 Retrieve Port-Level Thresholds

```
RTRV-PM-OC48::FAC-1-1-1:123::CVL,10-UP,NEND,BTH,15-MIN,04-11,12-45;
RTRV-PM-OCH::CHAN-6-1:123::ES-PM,10-UP,NEND, BTH,15-MIN,04-11,12-45:
```

2.13.13 Y-Cable Protection Group Provisioning Rules

The following rules apply when provisioning a Y-cable protection group:

- A Y-cable protection group can be created between the client ports of two unprotected TXPs and OTU2_XP cards.
- While in Y-cable protection, a TXP card cannot be part of a regeneration group.
- Only the working client port can be provisioned with SDCC.
- Y-cable cannot be provisioned for a protect version of the TXP_MR_2.5G card.
- Y-cable protection group is not supported on the ADM-10G card.
- Only the working ports (not the protect) can be provisioned with DCC and timing reference.

To provision Y-cable protection groups, use the following commands:

- ENT-FFP-(OCn, nGIGE, nGFC)
- DLT-FFP-(OCn, nGIGE, nGFC)
- ED-FFP-(OCn, nGIGE, nGFC)

Example 2-45 provisions Y-Cable Protection Groups.

Example 2-45 Provision Y-Cable Protection Groups

```
ENT-FFP-OC48::FAC-1-1-1,FAC-2-1-1:100:::PROTTYPE=Y-CABLE,
PROTID=DC-METRO-1,RVRTV=Y,RVTM=1.0,PSDIRN=BI:
ENT-FFP-10GIGE::FAC-1-1-1,FAC-2-1-1:100:::PROTTYPE=Y-CABLE,
PROTID=DC-METRO-2,RVRTV=Y,RVTM-1.0,PSDIRN=BI;
```

2.13.14 Splitter Protection Group Provisioning Rules

The following rules apply when provisioning a splitter protection group:

Note Splitter protection group provisioning rules apply only to the protect version of the TXP and OTU2_XP cards.

- Splitter protection groups cannot be created or deleted.
- A splitter protection group is created automatically when a protect TXP card is provisioned.
- The only editable attributes are: Revertive, Revertivetime, and Transponder mode.

To provision a splitter protection group, use the **ED-FFP-OCH** command.

Example 2-46 provisions a splitter protection group:

Example 2-46 Provisioning Splitter Protection Group Attributes:

```
ED-FFP-OCH::CHAN-2-1:100:::PROTID=DC-METRO3,RVRTV=Y,
RVTM=5.0,PSDIRN=BI;
```

2.13.15 Loopback Provisioning Rules

The following rules apply when provisioning loopbacks:

- Loopbacks can be provisioned on the client and trunk ports.
- Both terminal and facility loopback types can be provisioned.
- Loopback is not applicable when the framing type is UNFRAMED (HDTV, DV6000).
- For the protect TXP card, the following loopback rules apply to the trunk ports:
  - Only one loopback can be provisioned at the trunk ports at any given time.
  - Loopback is allowed only if the sibling trunk port is OOS-MT.
  - Provisioning a loopback on a trunk port will trigger the inhibit switching command LOCKOUT_OF_PROTECTION or LOCKOUT_OF_WORKING, depending on whether the working or the protect is placed in a loopback.
  - When a loopback is provisioned on a trunk port, both of the trunk ports will transmit the signal of the loopback port signal.
  - A loopback will be denied if there is a FORCE or MANUAL switching command in place on the trunk ports.
  - You cannot remove the inhibit switching command issued as a result of the loopback. This command will be removed only when the loopback is removed.

Use the **OPR-LPBK-OCH** command to provision loopbacks.

Example 2-47 is an example of operating a loopback.

Example 2-47 Operating a Loopback

```
OPR-LPBK-OCH::CHAN-2-1:1::,,,TERMINAL;
```

2.13.16 Automatic Laser Shutdown Provisioning Rules

The following rules apply when provisioning automatic laser shutdown (ALS):

- ALS can be provisioned on the client and trunk ports. For an ADM-10G card, ALS can be provisioned on interlink ports as well.
- If the trunk port is configured in a splitter protection group, only the working trunk port can be provisioned for ALS. However, provisioning on the working trunk port is reflected on the protect port.
- For an OTU2-XP card, ALS can be provisioned on the trunk ports. If the trunk port is configured in an APS protection group, only the working trunk port can be provisioned for ALS. However, provisioning on the working trunk port is reflected on the protect port.
- For the protected TXP card, ALS mode will only take effect when both ports receive a loss of signal (LOS).

To provision ALS, use the following commands:

- **ED-ALS**
- **ED-ALS-(OCn, nGIGE, nGFC, OTS, OMS, OCH)**

Example 2-48 provisions ALS.

Example 2-48 Provision ALS

```
ED-ALS::FAC-1-1-1:100:::ALSMODE=Y,ALSRCINT=130,ALSRCPW=35.1,RLASER=Y;
ED-ALS-OC192::FAC-1-1-1:100:::ALSMODE=Y,ALSRCINT=130,ALSRCPW=35.1,
RLASER=Y;
```

2.13.17 Ethernet Provisioning Rules

Ethernet provisioning is applicable only when the card is configured in the GEXP-L2ETH or 10GEXP-L2ETH mode.

2.13.17.1 Bandwidth Profile Provisioning Rules

The following rules apply when provisioning Bandwidth profile:

- Bandwidth Profile (BWP) database (DB) is applicable to the entire node.
- Any row of the BWP represents a set of VLAN profile attributes.
- Each BWP is identified by a unique number in the range of 1 to 10000.
- BWP 0 is reserved for default profile. Since it contains the default manufacturing data, only retrieve (RTRV) command is applicable.
- NAME, CIR, CBS, PBS, PIR, and CFMSTATE parameters can be configured.

To provision BWP, use the following commands:

- **ENT-BWP-ETH**
- **DLT-BWP-ETH**
- **ED-BWP-ETH**
- **RTRV-BWP-ETH**

Example 2-49 provisions BWP.

Example 2-49 Provision BWP

```
ENT-BWP-ETH:ROCKS:BWP-75:123:::NAME="MyBWP75",CIR=10,CBS=1M,PBS=1M,PIR=20,CFMSTATE=Y;
DLT-BWP-ETH:ROCKS:BWP-75:123;
ED-BWP-ETH:ROCKS:BWP-75:123:::NAME="MyBWP75",CIR=10,CBS=1M,PBS=1M,PIR=25,CFMSTATE=N;
RTRV-BWP-ETH:ROCKS:BWP-75:123;
```

When a BWP is created using the ENT-BWP-ETH command, it can be used in the ED-VLAN-ETH command to set up a relationship between the ETH port, VLAN, and BWP parameters.
If BWP field is omitted the first time the ENT-VLAN-ETH command is executed, then BWP-0 default value is assumed. When a BWP is already associated with the ETH Port-VLAN couple, to detach the Profile and restore the default value, a BWP=0 is requested using the ED-VLAN-ETH command.

TL1 examples of BWP attach, retrieve, or detach are:

```
ED-VLAN-ETH:ROCKS:ETH-1-1-1:123::100:BWP=34;
RTRV-VLAN-ETH:ROCKS:ETH-1-1-1:123::100:;
ED-VLAN-ETH:ROCKS:ETH-1-1-1:123::100:BWP=0;
```

2.13.17.2 VLAN Provisioning Rules

The following rules apply when provisioning the VLAN:

- The VLAN database (DB) is applicable to the entire node.
- Any row of the database represents a VLAN.
- The VLAN DB can be in the range of 1 to 4069. VLAN 0 is reserved for untagged VLAN.
- Name and Protected parameters can be configured.
- There is a hardware limitation on the maximum number of VLANs on which the CIR (Committed Information Rate), CBS (Committed Burst Size), EBS (Excess Burst Size), EIR (Excess Information Rate), and Ingress rate limit is set:
  - For GE_XP and 10GE_XP cards, Ingress rate limit is set on 128 (maximum) VLANs per board.
  - For GE_XPE and 10GE_XPE cards, Ingress rate limit is set on 256 (maximum) VLANs per board.
- A VLAN can be created (ENT), deleted (DLT), modified (ED), and retrieved (RTRV).

To provision VLAN, use the following commands:

- **ENT-VLAN**
- **DLT-VLAN**
- **ED-VLAN**
- **RTRV-VLAN**

Example 2-50 provisions VLAN.

Example 2-50 Provision VLAN

```
ENT-VLAN::VLAN-100:123::NAME="My VLAN",PROTN=N;
DLT-VLAN::VLAN-100:123;
ENT-VLAN::VLAN-100:123::NAME="Your VLAN",PROTN=Y;
RTRV-VLAN::VLAN-100:123
```

2.13.17.3 Link Integrity Rule

Link Integrity must be provisioned on a specific VLAN setting, that is, CFMSTATE=Y, in the bandwidth profile used by the VLAN.

To activate link integrity, use the **ED-BWP-ETH** command.

Example 2-51 activates link integrity.

Example 2-51 Activate Link Integrity

```
ED-BWP-ETH:ROCKS:BWP-56:1:::NAME="MyBWP56",CIR=10,CBS=1M,PBS=1M,PIR=20,CFMSTATE=Y
```

The VLAN-AIS action depends on the AISACTION parameter set on the ETH port. The possible values are AIS-SQUELCH and AIS-NONE.

To set and retrieve the AISACTION value use the following commands:

- **ED-L2-ETH**
- **RTRV-L2-ETH**

Example 2-52 sets and retrieves AISACTION parameter

Example 2-52 Set and Retrieve AISACTION Parameter

```
ED-L2-ETH::ETH-5-3-2-1:502:::AISACTION=AIS-SQUELCH;
RTRV-L2-ETH:TID:ETH-5-3-2-1:CTAG;
```

Since VLAN-AIS alarm on a ETH port is a summarization of multiple possible VLAN-X-AIS, the RTRV-VLAN-ETH command can be used to retrieve specific VLAN-X-AIS status on a single port as shown in the following examples:

```
RTRV-VLAN-ETH:TID:ETH-1-1-1:CTAG::110;
RTRV-VLAN-ETH:TID:ETH-1-1-1:CTAG;
```

Link Integrity can be activated on a limited number of VLANs per board:

- For GE_XP and 10GE_XP cards, link integrity is enabled on 128 (maximum) VLANs.
- For GE_XPE and 10GE_XPE cards, the link integrity feature is enabled on 256 (maximum) VLANs.

2.13.17.4 L2 Provisioning Rules

An L2 Ethernet port is present for every 22 ports of the GE-XP card, and for every 4 ports of the 10GE-XP card.

The following rules apply when provisioning L2:

- An L2 Ethernet port is accessed by the ETH modifier.
- The access identifier (AID) of an L2 Ethernet port is same as the supporting facility, with ETH prefix instead of FAC.

- The following parameters can be edited:
  - PST, SST, CMDMDE, and so on—administrative or service state parameters.
  - NIMODE (UNI,NNI)—client ports default to UNI and trunk ports default to NNI.
  - MACLEARNING, INGRESSCOS, ETHERCETYPE (CE type), ETHERSTYPE (Service Provider Type), BPDU, and BRIDGESTATE.
  - ALWMACADDR and INHMACADDR—mutually exclusive parameters.
  - QNQMODE and TRNSPSVLAN—when QNQMODE is SELECTIVE the QNQ-ETH table should be referred for detailed VLAN association; when QNQMODE is TRANSPARENT, TRANSPSVLAN contains VLAN ID of the only service provider's VLAN configured for the port.
  - NAME—name of the facility.

To provision L2, use the following commands:

- **ED-L2-ETH**
- **RTRV-L2-ETH**

```
ED-L2-ETH:CISCO:ETH-1-1-1:123:::NIMODE=NNI,MACLEARNING=Y,INGRESSCOS=7,
ETHERCETYPE=8100,ETHERSTYPE=8100,
ALWMACADDR=[aa-bb-cc-dd-ee-ff&zz-yy-ww-tt-ss-rr],BPDU=Y,BRIDGESTATE=DISABLED,
QNQMODE=TRANSPARENT,TRNSPSVLAN=4096,NAME="Ethernet",IGMPROUTER=STATIC,
AISACTION=AIS-SQUELCH
RTRV-L2-ETH:PETALUMA:FAC-1-1:CTAG;
```

2.13.17.4.1 L2 Queue In Queue (QinQ) Provisioning Rules

The following rules apply when provisioning L2 Queue In Queue (QinQ):

- L2 QinQ associates a customer-end VLAN to a service provider VLAN.
- L2 QinQ is valid on port basis only when QNQMODE is SELECTIVE.
- The following association rules apply between the two VLAN types:
  - Add (ADD) the service provider VLAN when the customer-end VLAN (or a range of customer-end VLAN) matches, *or*
  - Translate (XLTE) the customer-end VLAN (or a range of customer-end VLAN) with service provider VLAN when it matches.

    The default rule is ADD.
- The XLTE-ADD and DOUBLE-ADD rules for QinQ settings are not supported by the GE_XP and 10GE_XP cards.
- DOUBLE-ADD and XLTE-ADD are the newly introduced L2 QinQ rules. INTERNALVLAN and INGRESSCOS are the newly added parameters.
- When the DOUBLE-ADD and XLTE-ADD rules are activated, INTERNALVLAN parameter has to be provided.
- When DOUBLE-ADD rule is activated, the C-VLANs identified by FIRSTCEVLANID and LASTCEVLANID parameters will be added by the INTERNALVLAN parameter first and then added by the SVLANID parameter.
- When XLTE-ADD rule is activated, the C-VLANs identified by FIRSTCEVLANID and LASTCEVLANID parameters will be first translated to the INTERNALVLAN parameter and then will be added by the SVLANID parameter.

- The INGRESSCOS parameter is requested only if the INGRESSCOS parameter on the ETH port is set to VLAN operating mode. This this means the INGRESSCOS parameter applied to this port may be different depending on the VLAN and its QinQ setting.
- Only when the Ethernet port Ingress COS value is set to CVLAN, the ENT-QNQ-ETH command can set the ingress value for QinQ.
- Ingress values for QinQ cannot be set when VLAN ranges are configured for QinQ.
- In retrieve command, the VLAN IDs can be optionally specified to filter CVLAN ID (or a range of them) and SVLAN ID. When the VLAN ID is not specified, all the VLAN IDs associated to the Ethernet port are returned.

To provision QinQ, use the following commands:

- **ENT-QNQ-ETH**
- **ED-QNQ-ETH**
- **RTRV-QNQ-ETH**
- **DLT-QNQ-ETH**

Example 2-53 provisions QinQ.

Example 2-53 Provision QinQ

```
ENT-QNQ-ETH::ETH-2-10-1:123::10,10,100:RULE=XLTE;
RTRV-QNQ-ETH::ETH-2-10-1:123;
```

2.13.17.4.2 L2 Selective NNI Provisioning Rules

The L2 Selective NNI Provisioning applies to an L2 Ethernet port configured as NNI. The following rules apply when provisioning L2 Selective NNI:

- Any entry associates a SVLAN to the Ethernet port.
- User can add (ENT), remove (DLT), and retrieve (RTRV) a VLAN associated to the Ethernet port.
- In the RTRV command, the VLAN ID can be optionally specified in order to filter the SVLAN ID. If the VLAN ID is not specified, then all the VLAN IDs associated to the Ethernet port are returned.

To provision NNI, use the following commands:

- ENT-NNI-ETH
- ED-QNQ-ETH
- RTRV-NNI-ETH

Example 2-54 provisions NNI

Example 2-54 Provision NNI

```
ENT-NNI-ETH::ETH-2-10-1:123::10;
RTRV-NNI-ETH::ETH-2-10-1:123::10;
```

2.13.17.5 Internet Group Management Protocol Rules

The Internet Group Management Protocol (IGMP) can be activated on a specific VLAN by setting IGMPENABLE=Y in the ED-VLAN command. Also, IGMPFASTLEAVE=Y can be set in the ED-VLAN command to decrease the delay for forwarding multicast.

To activate IGMP, use the ED-VLAN command.

Example 2-55 activates IGMP.

Example 2-55 Activate IGMP

```
ED-VLAN:ROCKS:VLAN-1-2-84:1:::NAME="VLAN84",PROTN=N,MACLEARNING=N,IGMPENABLE=Y,IGMPFASTLEA
VE=Y,IGMPSUPP=N
```

To indicate which port is connected to the router, set the parameter IGMPROUTER=STATIC in the ED-L2-ETH command.

To set and retrieve IGMP router, use the following commands:

- ED-L2-ETH
- RTRV-L2-ETH

Example 2-56 sets and retrieves IGMP Router.

Example 2-56 Set and Retrieve IGMP Router

```
ED-L2-ETH:CISCO:ETH-1-1-1:123:::IGMPROUTER=STATIC;
RTRV-L2-ETH:TID:ETH-1-1-1:CTAG;
```

The IGMP Snooping feature can be activated on a limited number of VLANs per board:

- For GE_XP and 10GE_XP cards, the IGMP snooping feature is enabled on 256 (maximum) VLANs.
- For GE_XPE and 10GE_XPE cards, the IGMP snooping feature is enabled on 512 (maximum) VLANs.

2.13.17.6 Multicast VLAN Registration Rule

Multicast VLAN Registration (MVR) can be activated using ED-MCAST command.

To set and retrieve MVR, use the following commands:

- ED-MCAST
- RTRV-MCAST

Example 2-57 sets and retrieves MVR.

Example 2-57 Set and Retrieve MVR

```
ED-MCAST:CISCO:SLOT-1-4:321:::MVRSTATE=Y,MVRSVLAN=46,MVRSTARTIP=230.64.72.57,MVRIPRANGE=20
:;
RTRV-MCAST:CISCO:SLOT-1-4:33;
```

2.13.17.7 1+1 Protection Rule

The 1+1 Protection in L2-over-DWDM mode can be activated using the ENT-FFP-GIGE command with a new ONEPLUSONEL2 protection type. The cards must be set in the L2 mode and a double link must be established between the trunk ports.

To establish double link between the trunk ports, use the **ENT-LNK** command.

Example 2-58establishes double link between trunk ports.

Example 2-58 Establish Double Link between Trunk Ports

```
ENT-LNK::CHAN-4-12-21-1,CHAN-4-14-21-1:1482;
ENT-LNK::CHAN-4-14-21-1,CHAN-4-12-21-1:1486;
```

To create 1+1 L2 protection, use the **ENT-FFP-GIGE** command.

Example 2-59 creates 1+1 L2 Protection.

Example 2-59 Create 1+1 L2 Protection

```
ENT-FFP-GIGE::FAC-4-12-1-1,FAC-4-14-1-1:1487:::PROTTYPE=ONEPLUSONEL2;
```

To operate on switch protection, use the OPR-PROTNSW and RLS-PROTNSW-GIGE commands.

The laser status of the standby port in the protection unit can be decided using the PROTACTION parameter set on the ETH port. PROT-SQUELCH and PROT-NONE are the possible values.

To set and retrieve the PROTACTION value, use the following commands:

- **ED-L2-ETH**
- **RTRV-L2-ETH**

Example 2-60 sets and retrieves the PROTACTION value.

Example 2-60 Set and Retrieve the PROTACTION value

```
ED-L2-ETH::ETH-5-3-2-1:506:::PROTACTION=PROT-SQUELCH;
RTRV-L2-ETH:TID:ETH-5-3-2-1:CTAG;
```

2.13.18 Resilient Ethernet Protocol Provisioning Rule

The Resilient Ethernet Protocol (REP) can be configured on the ethernet port of GE_XP or 10GE_XP card. The following rules apply when provisioning the REP:

- You can configure REP only if the card is in ETH-L2 card mode.
- When REP is enabled, the interface is a regular segment port unless it is configured as an edge port.
- If only one port on the card is configured in a segment, the port should be an edge port.
- If two ports on the card belong to the same segment, both ports must be an edge ports or both ports must be a regular segment ports.

Note If one of the port is an Edge with No Neighbor, the other port can be a Regular segment port.

- Each card can have a maximum of 3 segments.
- Each segment can have a maximum of 2 ports (in the same card).

2.13.19 Connectivity Fault Management Provisioning Rules

The following rules apply when provisioning the Connectivity Fault Management (CFM):

- MAC security and CFM is mutually exclusive per card. You can enable CFM only if the MAC security is not enabled and vice versa.
- You cannot disable CFM when Maintenance End Point (MEP) or Maintenance Intermediate Point (MIP) is configured on the interface.
- Maintenance domain profile name length should not exceed more than 43 characters.
- The level of the maintenance domain should be in the range of 0 to 7.
- No two domains can have the same name.
- You cannot modify or delete the maintenance domain profile when the domain is associated with maintenance association (MA) profile.
- You cannot modify or delete the maintenance domain if the domain is associated with the MEP.
- A maximum of 1000 profiles can be created.
- There should not be a duplicate entry for VLAN and MA name on the profile table.
- You cannot delete the MA if it is associated with any domain.
- You can crate MEP or MIP only on the CFM enabled interfaces.
- You cannot detach the VLAN from the interface if the MEP is configured on the port for the VLAN.
- You cannot modify MEP.
- You cannot configure MIP if MEP with higher or same level is already configured on the port with the same VLAN ID.
- You cannot detach the VLAN from the interface if it is associated with any of the MIPs on the interface.
- A maximum of 1000 MEPs can be created per card.
- A maximum of 1500 MIPs can be created per card.

2.13.20 Ethernet in the First Mile Rules

The following rules apply when provisioning the Ethernet in the First Mile (EFM:

- The EFMSTATE parameter should be “enabled” for the facility by ED-FSTE to edit the EFM parameters.
- You cannot enable or disable the remote loopback through the local interface on the remote OAM peer entity if any other type of loopback (facility/terminal) is already configured on the local interface.
- CFM, REP, link integrity, LACP, FAPS, IGMP on SVLAN and L2 1+1 protection are not supported with EFM.

2.13.21 Link Aggregation Control Protocol Rules

The following rules apply when provisioning the Link Aggregation Control Protocol (LACP):

- When the GE_XP card is provisioned in the switch mode (L2 Mode), you can configure the channel group interfaces as follows:
  - MXP: Up to 11 channel group with a maximum of 8 port for each channel group.
  - TXP: Up to 2 Channel group with a maximum of 3 ports for each channel group.

2.13.22 LEX Provisioning Rules

The following rules apply when provisioning the LEX:

- You can provision LEX only on ADM-10G card.
- You can provision LEX provisioning on any of the 8 GigE Ports.
- LEX framing supports 16-bit or 32-bit CRC configuration. The default CRC for LEX framing is CRC-32 bit.

2.13.23 Port State Model Provisioning Rules

Use the following rules when provisioning the port state model:

- The Out of Service, Automatic In-Service (OOS,AINS) port service state is not supported for the 1GigE and 2GigE payload types.
- The working and protect ports can be put in the IS and OOS states independently.
- For the protect TXP card:
  - Setting the protect trunk port to OOS enables the suppression of alarms on that port and will enable the card to be used like an unprotected card, but the card still cannot be used for a Y-cable protection group.
  - Setting the protect trunk port to OOS will not switch off the transmit laser unless both trunk ports are OOS.
  - The protect trunk port cannot be IS if a loopback or a regeneration group is provisioned.

To edit the port state, use the ED-(OCn, nGIGE, nGFC, OCH) command.

Example 2-61 edits port state.

Example 2-61 Edit Port State

```
ED-OC48::FAC-6-1-1:114::::OOS,AINS;
ED-10GIGE::FAC-6-1-1:114::::OOS,AINS;
ED-OCH::CHAN-6-1:114::::IS;
```

2.13.24 SONET-Related Provisioning Rules

When provisioning SONET-related parameters, the SDBER and SFBER can only be provisioned on the working trunk port (OCH) for the protect TXP card. Values set at the working port will be reflected on the trunk port.

To edit SONET trunk port attributes, use the **ED-OCH** command.

Example 2-62 edits SONET Trunk port attributes.

Example 2-62 Edit SONET Trunk Port Attributes

```
ED-OCH::CHAN-6-2:114:::RDIRN=W-E,EXPWLEN=1530.32,VOAATTN=2.5,VOAPWR=7.5,
CALOPWR=0,CHPOWER=2.0,NAME="NYLINE",SFBER=1E-5,SDBER=1E-6,
ALSMODE=MAN,ALSRCINT=60,ALSRCPW=35.1,COMM=DCC,GCCRATE=192K,
OSDBER=1E-6,DWRAP=Y,FEC=Y,MACADDR=OO-OE-AA-BB-CC-DD,SYNCMSG=N,
SENDDUS=Y,RLASER=Y,SOAK=10,OSPF=Y:OOS,AINS;
```

2.13.25 Overhead Circuit Provisioning Rules

The following rules apply when provisioning overhead circuits:

- Local orderwire/express orderwire (LOW/EOW) is possible between the AIC-I, OC-N, and TXP/TXPP cards in any combination in line-terminated mode.
- Creating a F1/D4-D12 user data channel (UDC) is:
  - Not possible between TXP/TXPP and AIC-I cards in the line-terminated mode.
  - Not possible between TXP/TXPP and OCn cards in the line-terminated mode.
  - Possible between OC-N ports.
- All overhead (OH) bytes are passed across client and DWDM ports in the transparent mode.
- SDCC/LDCC tunneling is not possible in the line-terminated mode.
- No end-to-end OH circuit provisioning is possible.
- For MXP_MR_2.5G and MXPP_MR_2.5G cards these rules apply to the trunk port only.

2.13.26 Hardware Limitation Rules

The DWDM cards have the following hardware limitations:

- The ESCON Small Form-factor Pluggable (SFP) does not support any monitoring.
- Optics thresholds and PM are not shown on client ports.
- HI/LO-TXPOWER is not supported for TXP_MR_2.5G and TXPP_MR_2.5G cards.

CHAPTER 3

TL1 Errors

Note The terms "Unidirectional Path Switched Ring" and "UPSR" may appear in Cisco literature. These terms do not refer to using Cisco ONS 15xxx products in a unidirectional path switched ring configuration. Rather, these terms, as well as "Path Protected Mesh Network" and "PPMN," refer generally to Cisco's path protection feature, which may be used in any topological network configuration. Cisco does not recommend using its path protection feature in any particular topological network configuration.

This chapter provides TL1 error information supported by the Cisco ONS 15310-MA, Cisco ONS 15454, Cisco ONS 15454 M2, and Cisco ONS 15454 M6. For alarm information, refer to the platform-specific procedure guide, troubleshooting guide, and reference manual.

3.1 Errors

Errors can be generated by any command or command response message. Table 3-1 through Table 3-65 list errors alphabetically by error code. The format of an error message is as follows:

```
   SID DATE TIME
M CTAG DENY
   <ERRCDE>
    /* <ERRMSG> */
;
```

Table 3-1 ENEQ Errors

ENEQ Error Messages
At Least One Equipment Is Not Plugged
Communication Failed
Control Not Provisioned
Cost Not Found
EnvControl IF Is Not Found
Environmental Control Interface Not Found
Equipment Is Deleted
Equipment Must Be Present
Equipment Not Found

Table 3-1 ENEQ Errors (continued)

ENEQ Error Messages
Equipment Not Present
Equipment Not Provisioned
IP Address Not Found
IP Mask Not Found
Internal Communication Error
Next Hop Not Found
No standby present
No standby provisioned
Not Equipped
Sensor IF Is Not Found
Sensor Interface Not Found
Standby not in valid state, please wait
TID Not Found

Table 3-2 IBEX Errors

IBEX Error Messages
Extra Datablock
Extra parameters
Invalid AID Block. Extra Datablock
Invalid Payload Block. Extra Datablock

Table 3-3 ICNV Errors

ICNV Error Messages
AIS on LOF Not Supported
AISV on AIS Not Supported
Admin SSM Not Supported
Cannot Change Threshold Values On Protect Port
Cannot Enable IPV6 Without Provisioning IPV6 Address
Cannot Provision IPV6 Parameters While IPV6 Is Disabled
Cannot Set DCC When G709 Is Enabled
Cannot set Timer value if FTP server is not enabled
Cross Connect Not Supported By XC Mode
Equipment Does Not Match Request
Equipment In Use
Impedance Not Supported With Current Configuration

Table 3-3 ICNV Errors (continued)

ICNV Error Messages
Inhfelpbk Not Supported
Invalid Command
Invalid VLAN Remapping
Operation Not Supported By This Card
Operation Not Supported On This Shelf
PDIP Generation Not Supported
PDIP Not Supported
PM Threshold Type Not Supported
PM Type Not Supported
Payload Does Not Match Request
Performance Monitoring Type Not Supported
Protection Type Not Supported in SONET Media
SaBit Not Supported With Current Configuration
Senddus Not Supported
Syncmap Not Supported
Syncmsg Not Supported
Threshold Type Not Supported
Trace Not Supported On Protect Trunk Port
Unidirectional Not Supported
VT Map Not Supported
XC MODE Not Supported

Table 3-4 IDMS Errors

IDMS Error Messages
Data Missing
Loopback Type Missing
Missing Internal Data

Table 3-5 IDNC Errors

IDNC Error Messages
Invalid Data
Invalid PST Value
Invalid SST Value
PRI source cannot be INTERNAL when SEC source is not INTERNAL
PRI source cannot be INTERNAL when THIRD is not INTERNAL

Table 3-5 IDNC Errors (continued)

IDNC Error Messages
Primary Source Cannot Be INTERNAL When Secondary Source Is Not INTERNAL
Primary Source Cannot Be INTERNAL When Third Source Is Not INTERNAL
Primary Source Cannot Be NONE When Secondary Source Is Not NONE
Primary Source Cannot Be NONE When Third Source Is Not NONE
SEC source cannot be INTERNAL when THIRD is not INTERNAL
SSM not supported on SDH
Secondary Source Cannot Be INTERNAL When Third Source Is Not INTERNAL
Secondary Source Cannot Be NONE When Third Source Is Not NONE
Third source must be INTERNAL

Table 3-6 IDNV Errors

IDNV Error Messages
2F-BLSR Architecture Does Not Permit Manual/Forced Span Switching
ADM Peer Group Name Exceeds Maximum Length
AIS On Terminal Loopback Not Supported
AISONLPBK Not Supported
AMPLMODE Not Supported
AUTO ALS Mode Not Allowed With Digital Wrapper Disabled
AUTO Trace Mode Not Allowed
Alarm Message Must Be Enclosed Within a Pair of Quotes
Alarm Message Required for MISC
Alarm Type Exceeds Maximum Length Allowed
At least an XC10G XC card is needed for this equipment type
BERT Diagnostics Limited To VT Cross connections
BWP Name Exceeds Maximum Length
CALOPWR Not Supported
CALTILT Not Supported
CHPOWER Not Supported
CKTID Exceeds Maximum Length
CMDMDE Only Applicable when Creating/Deleting Protection Group
Calibration Power Not Allowed
Cannot Access DCC
Cannot Change Protection Type
Cannot Change XC Mode
Cannot Delete Dynamic TDC Entry

Table 3-6 IDNV Errors (continued)

IDNV Error Messages
Cannot Edit NAME When ADM Peer Group Not Present
Cannot Edit NAME When Regeneration Group Not Present
Cannot Modify Circuit Size While Active Equipment
Cannot turn off proxy server or firewall while in secure mode
Card Does Not Support Synchronization/Timing Parameters
Card Mode Incompatible With Configured Payload Type
Command Not Valid On Protect Card
Configuration Does Not Support AUTO ALS Mode
Current Interval Not Supported For RMON PMs
DCC Not Supported In Transparent Term Mode
DCC is in use
DS1 Mode Not Supported
Data Rate Already Provisioned
Description Too Long
Description cannot be more than 32 characters
Distance Extension Not Enabled
EXPGAIN Parameter Not Supported By Amplifier Facility
Edit FMT on an Invalid Card
Edit FMT with an Invalid Data
Edit Line Code Failed
Edit Line Code on an Invalid Card
Equipment Does Not Support ADM Peer Group
Equipment Does Not Support EXPWLEN
Equipment Does Not Support FCS
Equipment Does Not Support Fast Ring Protection Role
Equipment Does Not Support Fast Ring Protection State
Equipment Does Not Support PROTID
Equipment Does Not Support PRTYPE
Equipment Does Not Support Payload Type
Equipment Does Not Support RDIRN
Equipment Does Not Support RVRTV
Equipment Does Not Support RVTM
Equipment Does Not Support Regeneration Group
Equipment Does Not Support SUPERBLKS
Equipment Incompatible For Regeneration Group
Flow Control Value Not Supported

Table 3-6 IDNV Errors (continued)

IDNV Error Messages
Frame Format Contains Invalid Data
Frame Format Not Supported On Equipment
GCC Not Supported On CLNT Port
GFP Buffer Out Of Range
High Threshold Should Be Lower Than Extreme High
Incompatible Equipment Type For Protection
Incompatible Equipment Type
Incompatible New Equipment Type
Incompatible Protect Slot For Protection
Incorrect Raman Setup Configuration
Input, Data Not Valid
Interval Out Of Range
Invalid AID For PCA Cross-Connection
Invalid Alarm Message
Invalid Buffer Type
Invalid Card Mode For Equipment Type
Invalid Committed Rate
Invalid Community
Invalid Data For 2F-BLSR
Invalid Data Rate
Invalid Drop Path
Invalid Enable Value
Invalid Equipment Type
Invalid ESH Timer
Invalid Ethernet Frame Size
Invalid Expected Path Trace Message
Invalid Fast Ring Protection Role
Invalid Fast Ring Protection State
Invalid Holdoff Timer Value
Invalid IIH Timer
Invalid Interval
Invalid ISH Timer
Invalid L1 Buf Size
Invalid L1prog Value
Invalid L1tdc Value
Invalid L2 Buf Size

Table 3-6 IDNV Errors (continued)

IDNV Error Messages
Invalid L2prog Value
Invalid L2tdc Value
Invalid LDB Value
Invalid LDBEntry Value
Invalid LDBflush Value
Invalid LanSupp Value
Invalid Level Value
Invalid Log Name
Invalid MODE
Invalid MONLEV Value
Invalid MONTYPE Value
Invalid MTU Size
Invalid MAC Address
Invalid NI Mode
Invalid Next Hop
Invalid Notification Code
Invalid NSAP Value
Invalid PDU4timer Value
Invalid Pdu4onstart Value
Invalid Pduorigin Value
Invalid PM Interval
Invalid PPM Port
Invalid Port Mode For Facility
Invalid Port Number
Invalid Protect Group Identifier
Invalid PROTID
Invalid QNQ Mode
Invalid Recovery Pulse Width
Invalid Reference
Invalid Regeneration Group AID
Invalid Regeneration Group Configuration
Invalid Report Interval
Invalid ROLE
Invalid RibType Value
Invalid Side Role Specified
Invalid Start Time

Table 3-6 IDNV Errors (continued)

IDNV Error Messages
Invalid Static Route Destination
Invalid Switch Command
Invalid Switch Type For BLSR
Invalid TAP Number
Invalid Tarp Data
Invalid Tarp1 Value
Invalid Tarp2 Value
Invalid Tarp3 Value
Invalid Tarp4 Value
Invalid TXCOUNT Or RXCOUNT
Invalid TXCOUNT
Invalid Threshold Value Ordering
Invalid Time Offset
Invalid Timer Value
Invalid Trace Level
Invalid User Name
Invalid VCAT Group Name
Invalid area ID, format is nnn.nnn.nnn.nnn
J0 Section Trace Not Supported In Transparent Term Mode
Keyword All Not Allowed
Line Code Not Supported
Link Credit Out Of Range
Link Recovery And Distance Extension are Mutually Exclusive
Low Threshold Should Be Greater Than Extreme Low
MAN TRCMODE Not Allowed with NULL EXPTRC
Maximum Number Of Protected VLAN Reached
Maximum Number Of Routes Reached
Maximum Number Of VLAN Reached
Multiple AIDs Not Allowed
Multiple PROTID Not valid
Multiple Protection Group Card Slot Identifiers Not Allowed
Multiple References Not Allowed
Must Provide PROTID for Adding Working Modules
NEWSHELFID Required When Changing SHELFROLE To SC
Next Hop Conflicts Default Router
Node Has Default GRE Tunnel

Table 3-6 IDNV Errors (continued)

IDNV Error Messages
Null Userid Or Range In Userid List Not Allowed
Number Of Reports Is Negative
OSRI Not Supported
Only One Trunk Required For Card Mode
PPM Does Not Exist
PPM Type Parameter Not Supported By This Card
PRIVLVL Not Allowed When PAGE = 0
PRIVLVL Not Allowed Without PAGE, PCND, or TMOUT
PRIVLVL Required With PAGE, PCND, Or TMOUT
Parameter Not Supported By Payload Type
Parameter Not Supported By This Optical Node Type
Parameter Not Supported On Protect Trunk Port
Payload Mapping Type Incompatible With G.709 Settings
Payload Type Does Not Support AUTO ALS Mode
Payload Type Does Not Support DCC
Payload Type Does Not Support IS-AINS State
Payload Type Does Not Support OTN/FEC
Payload Type Not Supported
Peer Card Not Present
Peerid Must Be Different From Aid
Port Name Exceeds Maximum Length
Port Unsupported in Card Mode
Power Setpoint Adjust Failed
Protect Card Does Not Support Protection Type
Protect Slot Not Provisioned
Protection Group Card Slot Identifier Field Required
Protection Group Does Not Exist
Protection Group Name Cannot Be Null
Protection Group Name Exceeds Maximum Length
QNQ Entry Not Provisioned
REFTILT Not Supported
RMON Threshold Not Supported
Rate Capacity Exceeded
Regeneration Group Name Exceeds Maximum Length
Requested CRSTYPE Not Supported
Retime Not Supported

Table 3-6 IDNV Errors (continued)

IDNV Error Messages
Ring Lockout BLSR Switching Is Not Supported
SDCC is in use
SHELFROLE Field Must Be SC With NEWSHELFID
Shelf Role Invalid For Equipment Type
Span Lockout of Working on BLSR Switching Is Not Supported
Squelch Not Allowed With Current Setting
Static Route Cannot Be 255.255.255.255
Static Route Cannot Be Same As Class A Broadcast Address
Static Route Cannot Be Same As Class B Broadcast Address
Static Route Cannot Be Same As Class C Broadcast Address
Static Route Cannot Be Same As Default Router Mask
Static Route Cannot Be Same As Internal Network
Static Route Cannot Be Same As Node Broadcast Address
Static Route Cannot Be Same As Node IP
Static Route Cannot Be Same As Node Subnet
Static Route Cannot Be Same As Old Class E Address
Static Route Cannot be Same As Local Net
Switch Type Is Not Allowed On 1+1
TID Name Exceeds Maximum Length
TMPER Type Not Supported
Tap Out Of Range
Term Mode Does Not Support Synchronization/Timing Parameters
Threshold Increment Invalid
Threshold Value Out Of Range
Trace Level Not Supported By Client Port
Trace Level Required
Trace Not Supported In Transparent Term Mode
Transmitted Path Trace Message not supported
Transport Mode Invalid For Equipment Type
Unsupported Or Incompatible Termination Mode
Unsupported Protection Option
VLAN Name Exceeds Maximum Length
VLAN Out Of Range
VOA Not Supported
VOA Out Of Range

Table 3-6 IDNV Errors (continued)

IDNV Error Messages
Value Or Threshold Read Only
Value Out Of Range

Table 3-7 IDRG Errors

IDRG Error Messages
DST Not Supported For The Time Zone
Difference Value Range Error
Invalid DURAL Value
Invalid GFPBUF Value
Invalid MXINV Value
Invalid MXINV or DURAL Value
Invalid PAGE Value
Invalid PAGE or PCND Value
Invalid PCND Value
Invalid PDIF Value
Invalid PINT Value
Invalid PJMON Value
Invalid POLD Value
Invalid TMOUT Value
Invalid Threshold Value
Invalid Time Zone
Invalid Trap Destination
Invalid Trap Port
Invalid UOUT Value
Invalid Watermark Value
PJMON Out Of Range

Table 3-8 IIAC Errors

IIAC Error Messages
AID Does Not Match with Requested BLSR Path Type
AID PARSE ERROR
ALL AID Not Allowed
ALL, Ranging and Grouping Are Not Supported for Hard Reset
ALL, Ranging and Grouping Are Not Supported
AID validation failed

Table 3-8 IIAC Errors (continued)

IIAC Error Messages
BERT Diagnostic Cross connection Source Must Equal Destination
BLSR East and West On Same Slot Not Allowed
BLSR Time Slot Mismatch
Bad Ring Id
CCT=1WAY Not Allowed For The Card
Cannot Create Schedule On Protect Card
Cannot Access One Plus One Protect Line
Cannot Make Changes To Protect Card
Cross-Connection Cannot Overlap PCA Boundary
Cross-Connection Cannot Use GIGE Ports When In Transponder Mode
Cross-connection PathWidth Not Supported by Card
DS1 Out of Range
EQPT Prot AID parse failed
Equipment Can Not Be Provisioned On Low Speed Slot
Equipment Does Not Match Request
Equipment Does Not Support This Type Of Cross-connection
Equipment Type Is Same As Provisioned Equipment
Expected Trace Not Supported On This Card Type
Expected Trace String Exceeds Max Length (62)
Expected Trace String Exceeds Maximum Length
FAC parse failed
Incoming Trace Not Supported On This Card Type
Incorrect Card Type
Input, Invalid Access
Invalid AID
Invalid Cross-connection Name
Invalid Cross-connection Path Number
Invalid DRI Node Type
Invalid DRI Topology
Invalid DS1 AID
Invalid FROM AID
Invalid G1000 Facility Port
Invalid Month Or Day
Invalid Node Side
Invalid NodeId
Invalid Operation On Drop AID

Table 3-8 IIAC Errors (continued)

IIAC Error Messages
Invalid PJMON Value
Invalid PM Direction parameter
Invalid Protect AID or Working AID
Invalid Protect AID
Invalid RFROM AID
Invalid RFROMEND AID
Invalid RFROMSTART AID
Invalid RTO AID
Invalid RTOSTART AID
Invalid Reference
Invalid RingID
Invalid Roll From And/Or Roll To AID
Invalid Source AID
Invalid Source/Destination AID Count For Cross-Connection Type
Invalid TAP
Invalid TO AID
Invalid TPORT AID
Invalid Time
Invalid VCG Member Number
Invalid Year
Invalid fac-n-m input
J1 Trace Not Supported On This Card
List AID Not Allowed For ALL AID
List Or All AID Not Supported
Loopback type mismatch
LpbkType Does Not Match
Multiple AIDs Not Allowed With All AID
Multiple AIDs Not Allowed
Multiple AIDs Not Supported
Multiple Destination AID Exceeds Limit
Multiple Destinations Not Supported By Cross-Connection
Multiple Source AID Exceeds Limit
Multiple TAP AIDs Not Supported
Multiple AIDs Not Allowed
No TPORT With ONE-PORT-BI TRANS Mode
No TPORT With Removing TRANS Mode

Table 3-8 IIAC Errors (continued)

IIAC Error Messages
Not Allowed On 1+1 Protect Line
Not Allowed On BLSR Protect Line
Not Allowed On Protect Line
Optional AIDs Are Not Supported
Ranging and Grouping Are Not Supported for Soft Reset
RingID Does Not Match with AID Number
TPORT Must Use The Same Slot As The Aid
TPORT Supports Only A Single AID
Trace Format Not Supported On This Card Type
Trace Mode Not Supported On This Card Type
Trace Not Supported For Current Configuration
Trace String Exceeds Maximum Length
Transmit Trace Not Supported On This Card Type
Path Protection Cross-Connections Not Allowed For The Facility Of Data Card
Use Of TPORT Argument Requires Use Of TRANS

Table 3-9 IICM Errors

IICM Error Messages
Command not implemented yet...
Command not supported in this release
Input, Invalid Command
Input, Invalid MOD1
Input, Invalid MOD2
Input, Invalid VERB
Memory Allocation Error

Table 3-10 IICT Error

IICT Error Message
Invalid Correlation Tag

Table 3-11 IIDT Errors

IIDT Error Messages
'%xx' Encoding Error In URL Parsing
0 Sec Revertive Time Not Supported

Table 3-11 IIDT Errors (continued)

IIDT Error Messages
2F-BLSR Does Not Support SRVRTV/SRVTM/EASTPROT/WESTPROT Parameters
AUTO trace mode not supported
CMDMDE Must Be FRCD
Can Not Delete A Schedule Which Does Not Exist
Cannot Activate To Older Software
Cannot Add And Remove Drops Together
Cannot Create More RMON Threshold
Cannot Edit OSPF When Both SDCC and LDCC are Enabled
Cannot Revert From R2 To R1
Cannot Revert To Newer Software
Cannot Revert While In Permanent Secure Mode
Cannot Revert While In Secure Mode
Command Already In Progress
DEST Incompatible With RFR Type
DEST Incompatible With SWDL Type
DEST Required For RFBU Type
Duplicate BLSR Working/Protect Facilities
Duplicate Performance Monitoring Schedule
Duplicate RMON Threshold
Duplicate Schedule
Error Adding New Schedule
FRCD mode not supported
FTTD Host Cannot Be IP Address
FTTD Is Not Supported. Only Direct File Transfers Are Supported
FTTD URL Missing
Facility Already in OSC Group
File Name Missing In URL
Flash Manager Not Active
Hostname Missing In URL
IOS Config File Too Big
Invalid 2 Fiber Blsr Parameter
Invalid Area Address
Invalid Area Address Length
Invalid Area Chars
Invalid BLSR Mode
Invalid BLSR Protect Facility

Table 3-11 IIDT Errors (continued)

IIDT Error Messages
Invalid BLSR Working Facility
Invalid Data Parameter
Invalid East Protect Port
Invalid East Working Port
Invalid FTTD Host
Invalid NSAP Character
Invalid NSAP Length
Invalid NSAP Selector
Invalid NSAP
Invalid OSC Group Facility
Invalid Phase Number
Invalid Port In URL
Invalid Revertive Time
Invalid Router Number
Invalid Shelf Id 1 For SC
Invalid Software Switch Type
Invalid State Transition Request
Invalid State Value
Invalid Type Value In FTP URL. Only 'a', 'i', or 'd' Is Allowed.
Invalid West Protect Port
Invalid West Working Port
Invalid type= Syntax In FTP URL
Loopback type not supported
Mandatory FTP URL Not Provided
Maximum Performance Monitoring Schedule Limit Reached
Memory Out Of Range
Missing/Invalid Destination
Missing/Invalid Source
NSAP FTTD Hosts Unsupported
No TID matches FTTD hostname
Non-IP Hostname In FTP URL
Non-IP Hostname or Invalid TID In FTP URL
Null Outputs In URL Parsing
Only IS PST Is Supported
Only MAINT STATE Supported
Only NORM CMD_MODE Is Supported

Table 3-11 IIDT Errors (continued)

IIDT Error Messages
Only OOS PST Is Supported
Only OVWRT of YES is Allowed For Uploads
Only Port 21 Is Supported
Only SWDL Is Supported For The xfertype Argument
Only Type 'a' Is Supported In The COPY-IOSCFG FTP URL
Only Type 'i' Is Supported In The COPY-RFILE FTP URL
OSPF Cannot Be Enabled On OSI Alone SDCC
Password Missing In URL
Performance Monitoring Schedule Does Not Exist
Port Missing In URL
RFBU Type Required With RFILE-LOG Aid
Reach Limits Of MAX Schedules Allowed. Cannot Add More
SRC Incompatible With RFBU Type
SRC Required For RFR Type
SRC Required For SWDL Type
SWDL Incompatible With RFILE-COMPDB Aid
SWDL Incompatible With RFILE-PKG Aid
Software Activate/Revert Failed
Software Not Available For Switch
Terminal Loopback is not supported
The URL Contains Unsafe Characters. Please Encode
Unknown Error Processing FTP URL
Unsupported Locn Value
Username Missing In URL
ftp:// Missing In FTP URL
fttd:// Missing In FTTD URL

Table 3-12 IIFM Errors

IIFM Error Messages
Invalid AID Block. Invalid Data Format
Invalid Alarm Type - Must Conform To TL1 Rules
Invalid Data Format
Invalid Password
Invalid Payload Block. Invalid Data Format
Invalid User ID

Table 3-13 IIPG Errors

IIPG Error Messages
Configuration Requires Transparent Termination Mode
Equipment Payload Type Incompatible For Regeneration Group
Payload Type Requires Squelch Card Mode
Payload Type Requires Transparent Termination Mode
Transparent Termination Mode Required For Regeneration Group

Table 3-14 IISP Errors

IISP Error Messages
Input, Garbage
Invalid AID Block. Extraneous ',' Found

Table 3-15 IITA Errors

IITA Error Messages
GNE: Input, Invalid Target Identifier
Input, Invalid Target Identifier

Table 3-16 INUP Errors

INUP Error Messages
EXTRNG Configuration Is Not Supported
General Block Unsupported
Missing mandatory field
NODEID Configuration Is Not Supported
RNGID Configuration Is Not Supported
RNGMAPAUTO Configuration Is Not Supported
RNGWTR Configuration Is Not Supported

Table 3-17 IPEX Errors

IPEX Error Messages
Duplicate N/V field
Invalid Payload Block. Extra Parameters

Table 3-18 IPMS Errors

IPMS Error Messages
Invalid AID Block. Missing Mandatory Field
Invalid Payload Block. Missing Mandatory Field
Invalid syntax
Missing mandatory field
Parameter Missing

Table 3-19 IPNC Errors

IPNC Error Messages
Cannot Change Existing Protection Type
Cross-connect Doesn't Have Path Protection Path Selector
Description Too Long
Expected Duplex Not Supported
Expected Speed Not Supported
Invalid Auto Negotiate Value
Invalid Encapsulation Type
Invalid Flow Control Value
Invalid Maximum Frame Size
Invalid Oprnominal Value
Invalid Parameter
Invalid Trans Value
Parameter Not Valid
Parameters Are Not Consistent
Parameters Not Compatible
Selective auto Negotiate Cannot be enabled

Table 3-20 IPNV Errors

IPNV Error Messages
AID or Condition Must Be Specified
Bad IP Configuration Parameter
Bad Parameter
Bad Reference
Cannot Set Expected Path Trace For Source Path
Cannot Set Expected Path Trace In Auto Mode
Cannot Set Outgoing Path Trace For Drop Path

Table 3-20 IPNV Errors (continued)

IPNV Error Messages
Cross-Connection Does Not Have Path Protection Path Selector
DRITYPE Not Supported For Connection Type
Empty parameter
Exercise Is Not Allowed On Protected Facility
Expected Trace String Exceeds Max Length (62)
Facility Does Not Support Montype
Far End Loopback Type Not Supported In Current Framing Format
Far End Performance Monitoring Values Not Supported
Holdoff Timer Not Supported For Non-DRI Cross-Connections
INT Not Valid For BITS-OUT
INVALID SAMPLE TYPE
Internal-Ip Lookup Failed
Internal-Network Nodes Lookup Failed
Invalid BITS Framing
Invalid BITS Rate
Invalid Clock Source
Invalid Condition Type
Invalid DRITYPE
Invalid Default Router Address
Invalid IIOP Port number
Invalid IP Address
Invalid IP Configuration Parameter
Invalid IP Mask
Invalid IP Port Number
Invalid IPV6 Prefix Length
Invalid Link Termination Port
Invalid MONLEV Value
Invalid OSPF Cost
Invalid PM register
Invalid Parameter
Invalid Payload Block. Empty Parameter
Invalid Report Interval
Invalid SNTP Host Address
Invalid Start Time
Invalid Switch Command For Synchronization
Invalid Switch Type

Table 3-20 IPNV Errors (continued)

IPNV Error Messages
Invalid Threshold Value
Invalid Why Parameter
New Source Must Be Specified
Node Name Exceeds Maximum Length
Number Of Reports Is Negative
Optical Performance Monitoring Not Supported For This Card Type
PM Not Supported
Parameter Not Valid
Path is not associated with Path Protection Path Selector
Payload Does Not Support Optics Montypes
Primary Reference Incompatible With Timing Mode
Protection Type Does Not Support Reversion Mode
Protocol Does Not Support This State
RMON PM History Not Supported
Reference Type Not Supported
SPNWTR Parameter Not Supported
STARTUP TYPE MUST BE RISING FOR ABSOLUTE SAMPLE TYPE
Secondary Reference Incompatible With Timing Mode
Synchronization Source Already Defined For Protection Group
Synchronization Source Already Defined For The Slot
TL1 Can Not Set Its Own Access Level
TMGREF Parameter Not Supported
Third Reference Incompatible With Timing Mode
Time Period Not Applicable
Timing Mode Not Compatible

Table 3-21 NO Errors

NO Error Messages
No Applicable PM Data
No Error

Table 3-22 PICC Errors

PICC Error Messages
AID Required
AID does not match this session UID

Table 3-22 PICC Errors (continued)

PICC Error Messages
Bad Password Toggling - New Password Same As A Prior Password
Can't logout if user is not logged in
Can't change own security level
Can't login
Command Not Available to this User Level
IP Address Display Is Suppressed
Invalid User Access Privilege Value
Invalid User Identifier - Must Conform To TL1 Rules
Invalid User Password - Must Conform To Provisioned Password Rules
Invalid User Password - Must Conform To TL1 Rules
Logout failed
New Password Too Similar To Old Password
Password Cannot Be Changed Before Minimum Wait Time Expires.
Password Must Be Changed Before Continuing
Unexpected Default Case
Unknown CORBA Exception (Internal Error)
Unknown User
User Access Privilege Required
User Already Exists
User Identifier Exceeds Maximum Length Allowed
User Not Authorized
User Password Required

Table 3-23 PIMA Errors

PIMA Error Message
Memory Out Of Range

Table 3-24 PIUC Errors

PIUC Error Messages
Cannot Delete The Logged In User
Cannot Remove The Last Superuser
Unauthorized change of PID
Unauthorized
User Currently Logged Into Another Session
User Is Not Superuser

Table 3-24 PIUC Errors (continued)

PIUC Error Messages
User Not Allowed To Change User Access Privilege
User Not Allowed To Change User Password
User Not Allowed To Disable/Enable Self
User Not Allowed To Terminate Self
User Not Logged In

Table 3-25 PLNA Error

PLNA Error Message
Login Not Active

Table 3-26 RALB Errors

RALB Error Messages
GNE: All ENE Connections in Use
Requested DCC In Use

Table 3-27 RANB Error

RANB Error Message
GNE: No Response from ENE - IENE

Table 3-28 RNBY Errors

RNBY Error Message
Software upgrade in progress

Table 3-29 RRNG Errors

RRNG Error Messages
I/O Slot Out Of Range
Invalid Slot Number For SDH Electrical Cards
Invalid Slot Number

Table 3-30 RTBY Errors

RTBY Error Messages
Connection In Service
Side In Service
TAP Already In Use
TAP Number In Use

Table 3-31 RTEN Errors

RTEN Error Messages
Cannot Access VT
Cannot Change Access Mode
Cannot Set Access Mode
Invalid Access Mode
Invalid STS TAP Number
Invalid TAP AID
Invalid TAP Mode
Invalid TAP Number
Invalid VT Path TAP Number
Requested TAP Does Not Exist
Requested Tap Busy
TAP Not Found

Table 3-32 SAAL Error

SAAL Error Message
Already Allowed

Table 3-33 SAAS Error

SAAS Error Message
Equipment Already Provisioned

Table 3-34 SADC Errors

SADC Error Messages
Already Disconnected
GNE: ENE is down
TAP Not Connected

Table 3-35 SADS Error

SADS Error Message
Loopback Applied On Cross-connection

Table 3-36 SAIN Errors

SAIN Error Messages
Already Inhibited
Already Locked On
Already Locked Out

Table 3-37 SAIS Errors

SAIS Error Messages
Connection In Service
Port Already In Service

Table 3-38 SAMS Errors

SAMS Error Messages
Already In Clear Maintenance State
Already In Force Maintenance State
Already In Lockout Maintenance State
Already In Manual Maintenance State

Table 3-39 SAOP Errors

SAOP Error Messages
Control Already Operated
Control Already Released
Control Operated In Mntry

Table 3-40 SAOS Errors

SAOS Error Messages
Port Already in IS-AINS
Port Already In OOS-MT
Port Already Out Of Service

Table 3-41 SAPR Errors

SAPR Error Messages
Cannot Provision Regeneration Group When A Protection Group Is Present
Card Already In A Regeneration Group
Card Has Y Cable Protection
Entity Already In A Regeneration Group
Peer Card Already In A Regeneration Group
Peer Card Has Y Cable Protection
Peer Entity Already In A Regeneration Group
Peer Entity Has Y Cable Protection

Table 3-42 SARB Errors

SARB Error Messages
GNE: All Gateways in Use
System Memory Exhausted. Retry A Few Seconds Later

Table 3-43 SCAT Errors

SCAT Error Messages
Connection Already In Loopback
Connection Already In Test Access
Connection Is Tapped
End Point Is Already Connected
STS Is Already Used
Test Access Busy
VT Is Already Used
Would exceed max number of drops

Table 3-44 SDBE Errors

SDBE Error Messages
AID Parser Failed
Asymmetric VCG Not Supported
Bad Parameter
Cannot Access Alarms
Cannot Access Conditions
Cannot Access Controls
Cannot Access Date/Time

Table 3-44 SDBE Errors (continued)

SDBE Error Messages
Cannot Access Defaults Description
Cannot Access Default VLAN Profile
Cannot Access Environmental Settings
Cannot Access Equipment
Cannot Access Facility
Cannot Access IP Configuration
Cannot Access IP Display Suppression
Cannot Access Interface
Cannot Access Node ID
Cannot Access Node Name
Cannot Access Object
Cannot Access Orderwire
Cannot Access Protection Group
Cannot Access Protection State
Cannot Access SNMP Ip Addr
Cannot Access SNTP Host
Cannot Access STS
Cannot Access Security Mode
Cannot Access Software Version
Cannot Access Synchronization Configuration
Cannot Access Timezone
Cannot Access Trace Information
Cannot Access VT Performance Monitoring Parameters
Cannot Access VT
Cannot Configure Extension Byte For Current Configuration
Cannot Configure SYNC
Cannot Create 1+1 Protection Group
Cannot Edit STS
Cannot Get Line Information
Cannot Get Synchronization Configuration
Cannot Set Date When Using SNTP
Cannot Set Date
Cannot Set IP Configuration
Cannot Set Node Name
Cannot Set Pointer Justification Monitoring Parameter (PJMON)
Cannot Set SNTP Host Configuration

Table 3-44 SDBE Errors (continued)

SDBE Error Messages
Cannot Set Timezone
Cannot Soft Reset System
Card Type Not Supported
DLT prg Failed
Delete Protection Group Failed
Equipment Not Found
Ethernet Port Not Provisioned
Facility Does Not Exist
Facility Does Not Match Request
Facility Does Not Support Mac Address
Facility Is Not Provisioned
Facility Not Provisioned
File Transfer In Progress
Get Sonet Line Info Failed
Getting SONET sync configurations
IOS Config Update In Progress
IP Configuration Failed
Incompatible Parameter Values
Incorrect Facility Type
Interface Does Not Exist
Interface Does Not Support Loopback Type
Internal Access Failed
Internal Database Error
Invalid Command
Invalid Cross Connect Type For VCG
Invalid DCC
Invalid Mondat Format
Invalid Montm Format
Invalid Performance Monitoring Mode
Invalid Protection Group
Invalid Time Period
Invalid Trace Mode for Card Type
LCAS Not Supported By This Card
Location Value Invalid
Loopback Is Invalid
Loopback Port In Service

Table 3-44 SDBE Errors (continued)

SDBE Error Messages
Loopback type not supported
Mac Address Not Supported By Payload
No such interface
Node Name Configuration Failed
Not a Sonet interface
Object Already In Use
Object Not Provisioned
Object Not Supported
Operation Not Supported On EC1 Interface
Operation not supported by this card
Optical Channel Not Provisioned
Path Width Not Supported
Path loopback already exists
Reach Not Supported With Current Configuration
SNTP Configuration Failed
SSM not supported on SDH
STS Path Not Provisioned
Synchronization Configuration Not Available
Synchronization Status Messaging(SSM) Not Supported On EC1 Interface
Synchronization Status Messaging(SSM) Not Supported On SDH
Synchronization::Sync not available
System Timing Not Applicable For This Platform
Trace Not Applicable On This Card
Used Frame Format Does Not Support Synchronization Status Messaging (SSM)
VLAN Not Provisioned
VLAN Profile Not Provisioned
VT Path Not Provisioned
Wavelength Not Supported With Current Configuration
Wrong Facility Type
Wrong Interface Type
bind failed for Sonet gen
getActiveRefSource failed
getRefSources failed

Table 3-45 SDLD Error

SDLD Error Message
Duplex Unit Locked

Table 3-46 SDNA Errors

SDNA Error Messages
Active TCC Not Ready
Standby TCC Not Ready

Table 3-47 SDNR Error

SDNR Error Message
Data Not Ready

Table 3-48 SNCC Errors

SNCC Error Messages
Cross-connection does not exist
Path Roll Does Not Exist
Replace This Message When A SNCC message is needed

Table 3-49 SNCN Errors

SNCN Error Messages
Bad Quality
Cannot Switch To Bad Reference
Cannot Switch To Inferior Reference Source
Command Not Implemented
Cross-Connection Type Not Supported In TL1
Invalid Clock Source
Requested Direction Not Supported
STS Rate Change Not Supported
Sync Switch Operation Failed, Reference In OOS

Table 3-50 SNNS Error

SNNS Error Message
Reference Not From Optical Card

Table 3-51 SNOS Errors

SNOS Error Messages
Cannot Change Card Wavelength With Port(s) Not In OOS,DSBLD State
Cannot Change Payload With Port(s) Not In OOS State
Cannot Change Payload With Port(s) Not In OOS-MA,DSBLD State
Cannot Change Termination Mode With Port(s) Not In OOS State

Table 3-52 SNPR Errors

SNPR Error Messages
Cannot Get Role Of Port
Get Port Role Failed

Table 3-53 SNVS Errors

SNVS Error Messages
Already Switched To Internal Reference Source
BLSR East Operation Already Set
BLSR West Operation Already Set
CCAT Cross Connect Exists
Cannot Change BITS Configuration With Current State/Status
Cannot Change Configuration When Trunk Ports (or Peer Ports, if any) Are Not In OOS,DSBLD State
Cannot Change Parameter With Current State/Status
Cannot Change Payload For Port Used For Overhead
Cannot Change Payload When Port(s) Are Used As A Clock Source
Cannot Change Port State With Current State/Status
Cannot Change Revertive Behavior When A Protection Switch Is Active
Cannot Change Synchronization Configuration With Current State/Status
Cannot Change Termination Mode When Port(s) Are DCC Enabled
Cannot Change Termination Mode When Port(s) Are Used As a Clock Source
Cannot Change Termination Mode With Trace Enabled
Cannot Change Timing Reference With Current State/Status
Cannot Change or Delete Payload When Port(s) Are DCC Enabled
Cannot Configure Port When J0 Section Trace Enabled
Cannot Delete Port Involved In Loopback
Cannot END An AUTO Roll
Cannot Edit Facility When Not OOS State
Cannot Operate Loopback In Current Cross-connection State

Table 3-53 SNVS Errors (continued)

SNVS Error Messages
Cannot Operate Loopback In Current State
Cannot Provision Regeneration Group When A Protection Switch Operation Is Present
Cannot Provision Regeneration Group When Equipment Has Different FEC Settings
Cannot Provision Regeneration Group When Equipment Has Different G.709 Settings
Connection Already In Roll
Cross-Connect Exists
Facility Not Part Of BLSR
Invalid AINS Soak Time
Invalid Admin State
Invalid BLSR Element
Invalid Clock Source
Invalid Equipment State
Invalid Transponder Provisioning
Loopback Already In Progress
Loopback Not In Progress
No Switch In Progress
No Valid Roll Signal
No loopback in progress
Operation Can Not Be Completed. NE Is In Version UP State
Protection Group Does Not Exist
Protection Unit Active
Provisioning Not Allowed On Protecting Card
Roll Condition Does Not Exist
Roll is not controlled by TL1
Status, Not in Valid State
Unable To Complete Roll
VCG Already Created
Working Unit Already Active
Working Unit Already Standby

Table 3-54 SOSE Error

SOSE Error Message
Unrecognized Message Type

Table 3-55 SPFA Errors

SPFA Error Messages
Cannot Get Current Card Status
Protection Unit Failed Or Missing
Status, Protection Unit Failed or Missing

Table 3-56 SPLD Errors

SPLD Error Messages
Cannot Create 1+1 Protection Group
Cannot Delete Equipment
Equipment In Use
FTP Task Is Busy
Facility Is Busy
Protection Unit Locked

Table 3-57 SRAC Errors

SRAC Error Messages
Invalid Connection Type
Requested Access Configuration is Invalid

Table 3-58 SRCN Errors

SRCN Error Messages
Already In Requested Mode
Area already exists on lan interface
Cannot use backbone area, lan active
Protection Group Already Exists
Requested Condition Already Exists

Table 3-59 SROF Errors

SROF Error Messages
1+1 Protection Group Not Found
1WAYMON not supported
2F BLSR Pool Not Available
4F BLSR EastProtect Pool Is Not Available
4F BLSR Pool Not Available

Table 3-59 SROF Errors (continued)

SROF Error Messages
4F BLSR WestProtect Pool Is Not Available
ADM Peer Group Does Not Exist
ADM Peer Group Is Provisioned
AID Does Not Match With Requested Roll Type
AID Listing Not Allowed
ALL Rolls Failed
ALS Mode Does Not Allow Laser Restart
APC Not Applicable
APC System Is Busy
APC System Is Not Enabled
Active Flash Not Ready
Alarm Type Not Found
Alarm type In Use
All DCCs In Use
All Link Terminations On Port Must Terminate On Same Remote Node
All Rolls Failed to Cancel
All Rolls Failed to Complete
All Rolls Failed to Edit
Bandwidth Not Available
BFDL Mode Requires ESF Framing
BLSR In Use
BLSR Pool Not Available
BLSR Protect STS Path List Is Empty
BLSR Spans Are Not Locked
Bridge And Roll Not Supported On Roll From And/Or Roll To
Cannot Create 1plus1 L2 Protection
Cannot Create Splitter Protection
CKTID Does Not Match
CMDMDE Must Be FRCD To Create Protection Group With Pre-provisioned Cards
Can Not Get IOS Config Source Origin
Cannot Access 1+1 Line
Cannot Access 1+1 Protected Line
Cannot Access 2 Fiber BLSR
Cannot Access 4 Fiber BLSR East Protection
Cannot Access 4 Fiber BLSR West Protection
Cannot Access 4F BLSR

Table 3-59 SROF Errors (continued)

SROF Error Messages
Cannot Access Alarm Log
Cannot Access Audit Log
Cannot Access BLSR 2-Wire Line
Cannot Access BLSR
Cannot Access Cross-Connection
Cannot Access DCC
Cannot Access Facility
Cannot Access PM Mode
Cannot Access Performance Monitoring Statistics
Cannot Access Protected Equipment
Cannot Access Protection Group Information
Cannot Access Protection Group Name
Cannot Access Protection Group Reversion Information
Cannot Access Reversion Information
Cannot Access STS
Cannot Access TAP
Cannot Access TL1 Craft Session
Cannot Access Unprotected Line
Cannot Access VT
Cannot Add Equipment
Cannot Change Card Mode In SWDL State
Cannot Change Configuration With Port Having Connection
Cannot Change Entity In A Protection Group
Cannot Change Equipment Type
Cannot Change Ethernet IP With DHCP Provisioned
Cannot Change Ethernet IP With OSPF Provisioned
Cannot Change Parameter When User Switch Exists
Cannot Change G.709 Setting On This Card
Cannot Change G.709 Setting With Port Having Connection
Cannot Change Payload When Regeneration Group Exist
Cannot Change Threshold Values On Protect Card
Cannot Change Timing Reference When User Switch Exists
Cannot Change XTC Protection Group
Cannot Clear Performance Monitoring Statistics On Protect Card
Cannot Configure SYNC
Cannot Create Cross-Connection Between Incompatible Interfaces

Table 3-59 SROF Errors (continued)

SROF Error Messages
Cannot Create OCHNC With Invalid DWDM Network Type
Cannot Create Protection Group
Cannot Create TAP On Last VT
Cannot Create TAP
Cannot Create Y-cable Protection
Cannot Delete CCAT Cross-Connection In Forced Mode
Cannot Delete Cross-Connection
Cannot Delete Last Drop
Cannot Delete Link Termination Having Active Circuit
Cannot Delete Protected Equipment
Cannot Delete Protection Group
Cannot Delete System Defined Alarm Type
Cannot Delete VCAT Group When Members Are In Group
Cannot Delete VCAT Group
Cannot Delete VCAT Member When It Is In Group
Cannot Delete VCG Member In Current State
Cannot Disable DWRAP With FEC Enabled
Cannot Disable DWRAP With GCC Enabled
Cannot Disable DWRAP. Orderwire Circuit Exists
Cannot Disable DWRAP. Y-Cable Protection Exists
Cannot Edit Ethernet IP
Cannot Edit STS
Cannot Enable DWRAP With DCC Enabled
Cannot Enable FEC When G.709 Is Disabled
Cannot Enable FEC With DWRAP Disabled
Cannot Modify Protect Card
Cannot Operate Terminal Loopback With AISONLPBK Enabled
Cannot Perform ACO
Cannot Provision Equipment
Cannot Provision Filler Equipment
Cannot Provision Protection Equipment
Cannot Retrieve Performance Monitoring Statistics From Protect Card
Cannot Retrieve Threshold Values From Protect Card
Cannot Roll Hairpin Connection
Cannot Set ALS Mode
Cannot Set Bidirectional Protection Group

Table 3-59 SROF Errors (continued)

SROF Error Messages
Cannot Set DCC When Digital Wrapper Is Enabled
Cannot Set GCC When DWRAP Is Disabled
Cannot Set GCCRATE With GCC Disabled
Cannot Set GFP Buffer With AutoThresholdGfpBuf On
Cannot Set Linkcredits With AutoDetection On
Cannot Set Loopback In Current Mode
Cannot Set NodeID
Cannot Set Payload Type
Cannot Set Protection Group Name
Cannot Set RETIME, Port In Use
Cannot Set ROLE When WDM Is Disabled
Cannot Set RingID
Cannot Set Span Revertive Mode Unless 4-Fiber Ring
Cannot Set Span Revertive Time In Non-revertive Mode
Cannot Set Span Revertive Time Unless 4-Fiber Ring
Cannot Set Termination Mode
Cannot Set Wave Length
Cannot Setup Connection With Port In OOS-MT
Cannot Switch For Specified Connection Type
Cannot Switch For Specified Path
Cannot Update AISONLPBK When Loopback In Progress
Cannot Update Synchronization Reference List
Cannot force 1way destination roll
Cannot modify cross-connect right now
Card Mode Provisioning Failed
Clear PM Not Supported
Command Not Supported
Connection In Loopback
Connection In Roll
Connection In Test Access
Connection In Topology Upgrade
Connection Is Already In Roll
Connection Type Error
Control Channel In Use
Could Not Delete Protection
Could not provision area

Table 3-59 SROF Errors (continued)

SROF Error Messages
Cross-Connection Creation Failed
Cross-Connection Does Not Exist
Cross-connection Was Not Found
Cross-connection deletion failed
DCC Does Not Exist
DCC In Use
DCC Not In Use
DCC Termination Is Required to Set OSPF
DWRAP Not Enabled
Data Link Using TE Link
Data Not Available
Database Is Busy
Distance Extension And Directional Mode Are Not Compatible
Duplicate Alarm Type Create Attempted
Duplicate Area address
Duplicate FTP Server Create Attempted
Duplicate IP Address Route
Duplicate MAT
Duplicate Remote Link Termination Information
Duplicate Remote TE Link
Duplicate Tunnel Create Attempted
Duplicate VLAN Create Attempted
East And West Ports Must Have Dcc Terminations
Element Not Found
Element not available
End Facilities Are Using Different Wavelength
End Facilities Do Not Have An Internal Path
Equipment Does Not Match Request
Equipment Does Not Support 8B10B Montypes
Equipment Does Not Support Cross-connection Loopback
Equipment Is Double Slot Sized
Equipment Provisioning Failed
Ethernet IP And Default Router IP Subnets Are Different
Exceed Max Matrix Port Allowed For VT1 Path
Exceed Max Matrix Port Allowed For VT2 Path
Expected Trace Size Exceeds Trace Format Limit

Table 3-59 SROF Errors (continued)

SROF Error Messages
FTP Server Not Found
Facilities Are Not On Boundary
Facilities Belong To Different Node Sides
Facilities Must Be On Different Node Sides
Facility Does Not Support Laser Restart
Facility Has Unknown Node Side
Facility Not Part Of Appropriate BLSR
Facility Not Protected
Fail To Add RTO
Flash Is Busy
Force To Primary Not Allowed
Frame Format Not Applicable With Current Configuration
Generation 1 Does Not Support Given Quality Of RES
Generic IOS config upload failure message
Get IOR Failed
Has Valid Roll Signal Already
Hello Dead Less Than 3X Hello
Hello Dead Max Less Than Max
Hello Dead Max Less Than Min
Hello Dead Max Too Large
Hello Dead Min Less Than Min
Hello Dead Min Too Small
Hello Dead Out Of Range
Hello Max Less Than Min
Hello Max Too Large
Hello Min Too Small
Hello Out Of Range
Host Not In IP Address Format
IPPM Not Supported By Equipment Type
Impedance Not Applicable With Current Configuration
Insufficient Contiguous Bandwidth
Insufficient Path Width For Cross-Connection
Insufficient Path Width For Test Access
Insufficient Path Width on Roll Destination
Interlink Port Does Not Exist
Internal Bind Error

Table 3-59 SROF Errors (continued)

SROF Error Messages
Internal Database Error
Internal Exercise Failure
Internal Facility Type Failure
Invalid AID
Invalid ALS Recovery Interval
Invalid ALS Recovery Pulse Width
Invalid BLSR DRI Drop
Invalid Broadcast Remote IP Address
Invalid Class A Remote IP Address
Invalid Class B Remote IP Address
Invalid Class C Remote IP Address
Invalid Control Type (CONTTYPE) For AID
Invalid Cross-Connect Type For VCG
Invalid Cross-Connection Path
Invalid Cross-Connection Type (CRSTYPE)
Invalid Cross-Connection Type For Drops
Invalid Drop Path
Invalid Local Node ID
Invalid Local Port
Invalid Loopback Provision
Invalid Operation For Connection Type
Invalid Operation For Specified Path
Invalid Path
Invalid Payload For LMP Data Link
Invalid Protection Group
Invalid Protection Switch Operation
Invalid Provisioning For Current Configuration
Invalid RMODE
Invalid Reference Source for Timing
Invalid Remote Data Link ID
Invalid Remote Network Element
Invalid Remote TE Link ID
Invalid SYNC entity
Invalid State When Loopback Present
Invalid Subnet Mask
Invalid Synchronization Source

Table 3-59 SROF Errors (continued)

SROF Error Messages
Invalid Path Protection Path
Invalid Username/Password
Invalid WDMANS PPMESH Parameter
Invalid type for this Cross-connection
Is Not 1+1 Element Type
J0 Section Trace Level Not Supported By 10GE Payload Type
LMP Data Link Using Port
Laser Was Not Shutdown.Cannot Restart Laser
Line Code Not Applicable With Current Configuration
Link Does Not Exist
Link Termination Does Not Exist
Link Termination Id Already In Use
Local And Remote IP Addresses the Same
Location Incompatible With Loopback Type
Loopback Not Allowed On Drop Path
Loopback Type Does Not Match
MAA List Full, PAA Can Not Be Removed
MAT Entry Does Not Exist
MAT Table MaxLimit Exceeded
MIC Cards Cannot Be Reset
Maximum Control Controls Provisioned
Maximum DIAG Crossconnect Limit Reached
Maximum Data Links For TE Link Provisioned
Maximum Data Links Provisioned
Maximum Drop Limit Reached
Maximum FTP server Creation Limit Exceeded
Maximum Link Terminations On Port Reached
Maximum Subnet Already Exist
Maximum TE Links Provisioned
Maximum Tunnel Creation Limit Exceeded
Maximum User Limit Reached
Maximum UserDefined Alarm Type Limit
Maximum VT Cross Connection Limit Reached
Multi-Shelf Mode Not Supported On This Equipment
Multi-Shelf Mode Not Supported On This Platform
Multi-Shelf disable not allowed

Table 3-59 SROF Errors (continued)

SROF Error Messages
No Path To Regulate
No Start-Up IOS Config
No clock and data copy information from Line cards and SSXC cards
Node::General not available
Node::NetworkConfig not available
Non Revertive Mode Does Not Allow to Set RVTM
Not Compatible With Protect
Not Enough Path Width For TACC
Number of Drops Exceed Allowable
OCH Client Connection Already Exist
OCH Client Connection Does Not Exist
OCHNC Connection Does Not Exist
One Plus One Line pool not available
Operate Alarm Cutoff Failed
Operation Not Supported By XC Card
Operation Not Supported On Port
Operation Not Supported
Operation not Valid for Connection Type
Operation not Valid for Path Specified
OspfTopology::OSPFTopo not available
PM Not Supported For Specified Path
Parameter Not Supported When DWRAP Is Enabled
Path Already In Use
Path Specified Is Not Valid
Path Used For Test Access
Payload Provisioning Failed
Payload Type Does Not Support Trace
Peer Equipment Attributes Do Not Match
Peer Equipment Type Does Not Match
Peer Facility Has Loopback
Peer Facility Is IS
Peer Facility Not In OOS-MT
Peer Payload Type Does Not Match
Peer Termination Mode Does Not Match
Platform Does Not Support Given AIS Threshold Value
Platform Does Not Support Given Frame-Format Value

Table 3-59 SROF Errors (continued)

SROF Error Messages
Platform Does Not Support Given Line Code Value
Platform Does Not Support Given Quality Of RES
Pool Does Not Exist
Pool not available
Port In Use
Port Mode Configuration Not Supported
Port Type Already Provisioned
Port Type Mismatch
Port Type Not Provisioned
Protect Port Active
Protection Group Busy
Protection Group Does Not Exist
Protection Switch In Progress
Protection Switching Failed
Protection Type Mismatch
Protection Type Not Compatible With Facility
Provisioning Rules Failed
Quality Of Clock Reference Not Applicable For This Platform Or Selected System Timing
RMON Threshold Does Not Exist
ROLL TO Path Is Already In The Cross-connection
Regeneration Group Already Exist
Regeneration Group Does Not Exist
Remote IP Address Cannot Be Class D Or E
Remote IP Address Cannot Equal The Node IP Address
Remote IP Address Cannot Equal The Node Mask
Remote IP Address Has Invalid Host Portion
Remote IP Address Is All Ones
Remote IP Address On Internal Net
Remote IP Address On Local Net
Requested Operation Failed
Requested Tap Busy
Revertive Mode Not Supported
Ring Reversion Failed
Roll Failed
Roll To Path Not Aligned

Table 3-59 SROF Errors (continued)

SROF Error Messages
SDBER Out Of Range
SDCC creation failed
SFBER Out Of Range
SSet PRG Reversion Failed
STS Does Not Exist
STS Does Not Have TAP
STS Path Width Does Not Match
STS Rates Do Not Match
SaBit Not Applicable With Current Configuration
Section Termination Mode Not Supported
Security::General not available
Set PRG Bidirectional Failed
Set PRG Name Failed
Side Not Applicable To WDMANS Application
Slot Does Not Support New Equipment Type
Software Activation Failed
Software Download Failed
Software Error
Software Reversion Failed
Span Reversion Failed
Specified Operation Is Not Valid
Standby Flash Not Ready
Sync Reference List Update Failed
Synchronization Status Messaging (SSM) Not Supported In Current Configuration
Synchronization/Timing Parameters Not Supported With DWRAP Enabled
TAP connected
TARP Origination Is Disabled
TCC Type Does Not Support Given Framing Type
TE Link In Use
TE Link Using Control Channel
TID exists in TADRMAP
TL1 Cannot Roll Connections In A Port Group
TTI Trace Not Allowed With G709 Disabled
Tap Not Provisioned
Test Access Active
Test Access Not Supported On Card

Table 3-59 SROF Errors (continued)

SROF Error Messages
The Maximum number of TID-Address pairs has been reached
This Timer Not Applicable to Standard 1+1
Trace Format Not Supported By J0 Section Trace
Trace Format Not Supported By TTI Section Trace
Trace Format Unsupported
Trace Message Size Exceeds Trace Format Limit
Trace Mode Incompatible With Termination Mode
Trace Mode Not Supported
Trap Destination Already Exists
Trap Destination Does Not Exist
Trap Table Full
Tunnel Not Found
Path Protection Needed To Change Revertive Behavior
Path Protection Selector Not Allowed On Non-Optical Ports
Unable To Cancel Roll
Unknown Internal Error
Unprotected Line pool not available
Unprovisioning Rules Failed
Unsupported BLSR STS Path Operation
Unsupported Command Type
Unsupported Element Type
VCG Does Not Exist
VLAN Already In Use
VLAN Not Applicable
VLAN Profile Not Applicable
VT Cross-Connection Does Not Exist
VT Does Not Exist
VT Does Not Have TAP
VT Path Width Does Not Match
WDMANS Not Regulated
WDMANS System Is Busy
Wavelength Value Not Supported
Working/Peer Card In Use
Wrong Interface Type
XC Card Does Not Support VT Cross-Connection
XC Card Not Present

Table 3-59 SROF Errors (continued)

SROF Error Messages
XCVXL Card Not Present
Y-Cable Protection Does Not Exist

Table 3-60 SRQN Errors

SRQN Error Messages
1 Disabled #
1 Enabled#
Admssm Not Allowed When SSM Enabled
Area Address Does Not Exist
Area Address is PAA Can Not Be Removed
BLSR Creation Failed
BLSR Deletion Failed
BLSR Does Not Exist
BLSR Editing Failed
Cannot Be Disbaled Until Router
Cannot Be Enabled Until Router
Cannot Create Automatic Links
Cannot Edit ADMSSM On Protect Port
Cannot Edit HIWRMK While Port Is In Transponder Mode
Cannot Edit LOWRMK While Port Is In Transponder Mode
Cannot Edit MFS While Port Is In Transponder Mode
Cannot Edit SENDDUS On Protect Port
Cannot Edit SYNCMSG On Protect Port
DCC Not Allowed In SDH Mode
DCC Not Allowed On Protect Port
DCC not enabled
Data Access Request Failed
Invalid Mode For Current Configuration
Invalid Request
Maximum Limit For MAA Addition Reached
OSC Group Already Exists
OSC Group Does Not Exist
Path loopback already exists
Protect Card Does Not Support Electrical Protection
Protect Card Does Not Support Protection Type

Table 3-60 SRQN Errors (continued)

SRQN Error Messages
Router Cannot Be Enabled IN ES MODE
Router Not Enabled
SDH Not Allowed On Protect Port
SDH Not Allowed With DCC
SDH Not Allowed With SENDDUS
SDH Not Allowed With SYNCMSG
SDH Not Allowed
SECURITY CANNOT BE CHANGED
SENDDUS Not Allowed With SDH Mode
STS Cross-Connection Does Not Exist
SYNCMSG Not Allowed With SDH Mode
Sync Status Messaging(SSM) Not Allowed With SDH Mode
TCC CANNOT SUPPORT FRONT-END PORT
VT Cross-Connection Does Not Exist

Table 3-61 SRTN Error

SRTN Error Message
TAP Not Found

Table 3-62 SSRD Errors

SSRD Error Messages
Manual Switch Cannot Override Forced Switch
Switch Request Denied

Table 3-63 SSRE Errors

SSRE Error Messages
GNE: ENE Connection Closed
GNE: System Resources Exceeded - FD
GNE: System Resources Exceeded - Lock
GNE: System Resources Exceeded - Thread
Memory Resources Exceeded
Memory resource denial

Table 3-64 SWFA Errors

SWFA Error Messages
Status, Working Unit Failed or Missing
Working Unit Failed Or Missing

Table 3-65 SWLD Error

SWLD Error Message
Working Unit Locked

3.2 Echo

In order to improve Telnet functionality for automated systems, the echo function has been turned off in ONS 15454 Release 3.0 and later. This change is transparent to users running standard UNIX-compliant Telnet clients; however, PC users might need to change their client setup to enable “local echo.” This is normally accomplished by a drop-down list or a preference attribute.

To test the local echo on your PC client, use the RTRV-HDR command. If you receive a response but no data, set the local echo to ON. Cisco recommends that you close any windows containing sensitive information after exiting a TL1 session.

INDEX

Numerics

A

B

C

D

E

F

G

I

K

L

M

N

O

P

Q

R

S

T

U

Y