Cisco ONS 15302 Installation and Operations Guide

Release 2.0
January 2005

Corporate 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: 408 526-4100

Text Part Number: OL-3580-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

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

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

Modifying the equipment without Cisco's written authorization may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

• Turn the television or radio antenna until the interference stops.

• Move the equipment to one side or the other of the television or radio.

• Move the equipment farther away from the television or radio.

• Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco ONS15302 Installation and Operations Guide

About This Guide

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

This section provides the following information:

Document Objectives

This chapter explains the function of the Cisco ONS 15302 system. It also contains the information how to install a Cisco ONS 15302 system.

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

This Cisco ONS15302 Installation and Operations Guide is organized in the following chapters:

- Chapter 1, “Safety Summary,” provides required and recommended safety practices for working with electrical equipment and electro-optical equipment.
- Chapter 2, “Product Overview,” provides the functionality and the feature of the ONS 15302.
- Chapter 3, “Pre-Installation Procedures,” provides information concerning pre-installation equipment storage and handling, site verification of equipment, site preparation, and equipment unpacking.
- Chapter 4, “Installation,”provides specific installation procedures.
- Chapter 5, “Troubleshooting,” provides troubleshooting information.
- Chapter 6, “Technical Specifications,” provides detailed information about the system.
- Chapter 7, “ONSCLI Command Line Interface,” provides the functionality and the syntax of the ONSCLI.
- Chapter 8, “ONSCLI Command Hiearchy,” provides all commands in graphical version and describes the available commands and the parameters of the ONSCLI.
- Chapter 9, “Managed Objects,” provides parameters related to each managed object

Related Documentation

Refer to the following standards documentation referenced in this publication:

- ANSI X3T12 TP-PMD
- EIA RS-232
- EN 300 386
- EN 50081-1
- EN 50082-1
- EN 50082-2
- EN 55022
- EN 55024
- EN 60825
- EN 60950
- EN 61000-3-2
- EN 61000-3-3
- EN 61000-4-2
- EN 61000-4-3
- EN 61000-4-4
- EN 61000-4-5
- EN 61000-4-6
- EN 61000-4-11
- EN/IEC 60950
- ETS 300 011
- ETS 300 019

- ETS 300 019-2-3 Class 3.2
- ETS 300 019-2-2 Class 2.2
- ETS 300 019-2-1 Class 1.1
- ETS 300 126
- ETS 300 132-2
- ETS 300 233
- ETS 300 246
- ETS 300 247
- ETS 300253
- ETS 300 418
- ETS 300 419
- ETS 300 461-1
- ETSI EN 300 019-2-3 Class 3.2
- IEC 61000-4-2
- IEC 61000-4-3
- IEC 61000-4-4
- IEC 61000-4-6
- IEC 793-2
- IEEE 802.1q
- IEEE 802.1d
- IEEE 802.2
- IEEE 802.3
- ISO/IEC8877
- ITU-T G.651
- ITU-T G.652
- ITU-T G.701
- ITU-T G.702
- ITU-T G.703
- ITU-T G.704
- ITU-T G.706
- ITU-T G.707
- ITU-T G.783
- ITU-T G.813
- ITU-T G.823
- ITU-T G.825
- ITU-T G.832
- ITU-T G.957
- ITU-T G.958

- ITU-T V.11
- ITU-T X.150

Document Conventions

This publication uses the following conventions:

Convention	Application
boldface	Commands and keywords in body text.
italic	Command input that is supplied by the user.
[ ]	Keywords or arguments that appear within square brackets are optional.
{ x | x | x }	A choice of keywords (represented by x) appears in braces separated by vertical bars. The user must select one.
Ctrl	The control key. For example, where Ctrl + D is written, hold down the Control key while pressing the D key.
`screen font`	Examples of information displayed on the screen.
`boldface screen font`	Examples of information that the user must enter.
< >	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

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 15xxx systems. It also includes translations of the safety warnings that appear in the ONS 15xxx system documentation.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation DVD

Cisco documentation and additional literature are available in a Documentation DVD package, which may have shipped with your product. The Documentation DVD is updated regularly and may be more current than printed documentation. The Documentation DVD package is available as a single unit.

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/

Cisco Marketplace:

http://www.cisco.com/go/marketplace/

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.

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

  http://www.cisco.com/en/US/partner/ordering/

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com
- Nonemergencies—psirt@cisco.com

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support Website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID

or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

Safety Summary

This chapter provides safety considerations for operating the Cisco ONS 15302 system.

1.1 Critical Safety Warnings

Warning **Do not perform cabling on an electrically-live system. Ensure that all power is removed from the shelf before continuing with this procedure. Actual wire gauge should be determined based on local engineering standards and practices.**

Warning **Before connecting 48 V power to the ONS 15302, remove the fuses from both the A and B sides of the power distribution panel (PDP). Failure to do so can cause serious injury or death. Actual wire gauge should be determined based on local engineering standards and practices.**

Warning **Before connecting 230 V power to the ONS 15302, remove the fuse from the 230 V power supply. Failure to do so can cause serious injury or death. Actual wire gauge should be determined based on local engineering standards and practices.**

Warning **Before installing the ONS 15302, remove the fuses from both the A and B sides of the PDP. Failure to do so can cause serious injury or death.**

Warning **Touching electrical connectors or other exposed electrical circuitry inside the ONS 15302, when they are energized can cause serious injury or death.**

1.2 General Safety Precautions

General safety precautions are not related to any specific procedures and do not appear elsewhere in this publication. Personnel must understand and apply the following precautions during installation and testing of the ONS 15302 system.

- Know standard electrical safety and electrical wiring and connection practices.

- Be familiar with cardio-pulmonary resuscitation (CPR). Obtain this information through the appropriate national authority (such as the Red Cross or the local equivalent). This knowledge is imperative for personnel working with or near voltages with levels capable of causing injury or death.

1.3 Recommended Safety Precautions

The following precautions are recommended when working on the ONS 15302 system:

- Keep your work area tidy and free of obstructing objects at all times.
- Do not wear loose clothing, jewelry, or other items that could be caught in the components during installation or use.
- Use the equipment only in accordance with the electrical power rating.
- Do not work alone if hazardous conditions may exist in your workplace.
- Install the ONS 15302 components in compliance with the following local and national electrical codes:
  - In the United States: National Fire Protection Association (NFPA) 70; US National Electrical Code
  - In Canada: Canadian Electrical Code, part I, CSA C22.1
  - Elsewhere: International Electrotechnical Commission (IEC) 364, part 1-7
- Properly ground the equipment.
- Connect only a DC power source that complies with the safety extra-low voltage (SELV) requirements in UL1950, CSA 950, EN 60950, and IEC950 to an ONS 15302 DC power supply input.
- Install DC power supplies used in restricted access areas in accordance with Articles 110-16, 110-17, and 110-18 of the National Electric Code, ANSI/NFPA 70.
- Terminate all laser outputs properly before connecting laser inputs.
- Disconnect the input end of an optical fiber jumper cable before disconnecting the output end.
- Handle glass fiber with care. Glass fiber can be broken if mishandled. Using broken fiber can result in permanent equipment damage.
- Protect skin from exposed glass fiber. It can penetrate the skin.
- Limit the number of personnel that have access to lightwave transmission systems. Personnel should be authorized and properly trained if access to laser emissions is required.
- Limit the use of laser test equipment to authorized, trained personnel during installation and service. This precaution includes using optical loss test (OLT) set, optical spectrum analyzer, and optical time domain reflectometer (OTDR) equipment.
- Exclude any unauthorized personnel from the immediate laser radiation area during service and installation when there is a possibility that the system may become energized. Consider the immediate service area to be a temporary laser-controlled area.
- The ONS 15302 system functions in the 1270 – 1335 nm window, which is considered invisible radiation. You cannot see the laser light being emitted by a fiber, a pigtail, or a bulkhead connector. Use appropriate eye protection during fiber-optic system installation or maintenance whenever there is potential for laser radiation exposure, as recommended by the company's health and safety procedures. Observe this precaution whether warning labels have been posted.

1.4 Safety Symbols and Labels

The ONS 15302 equipment is clearly printed with warning about the equipment radiation level. Read and understand all warning notes before working with the equipment.

The ONS 15302 has a warning note located left from the optical connector. The warning note consists of warning text CLASS 1 LASER PRODUCT.

1.5 Electrostatic Discharge Cautions

Some ONS 15302 components are classified as Class 0 ESD-sensitive devices. Adhere to the following rules:

- Observe standard precautions for handling ESD-sensitive devices.
- Assume that all solid-state electronic devices are ESD-sensitive.
- Ensure that you are grounded with a grounded wriststrap or equivalent while working with ESD-sensitive devices.
- Transport, store, and handle ESD-sensitive devices in static-safe environments.

1.6 Translated Warnings

The following sections describes the translated warnings.

1.6.1 DC Power Disconnection Warning

Warning **Before performing any of the following procedures, ensure that power is removed from the DC circuit.**

Waarschuwing **Voordat u een van de onderstaande procedures uitvoert, dient u te controleren of de stroom naar het gelijkstroom circuit uitgeschakeld is.**

Varoitus **Varmista, että tasavirtapiirissä ei ole virtaa ennen seuraavien toimenpiteiden suorittamista.**

Attention **Avant de pratiquer l'une quelconque des procédures ci-dessous, vérifier que le circuit en courant continu n'est plus sous tension.**

Warnung **Vor Ausführung der folgenden Vorgänge ist sicherzustellen, daß die Gleichstromschaltung keinen Strom erhält.**

Figyelem! **Mielõtt a következõ eljárások bármelyikét végrehajtaná, feltétlenül szakítsa meg az egyenáramú áramkör tápellátását.**

Avvertenza **Prima di svolgere una qualsiasi delle procedure seguenti, verificare che il circuito CC non sia alimentato.**

Advarsel **Før noen av disse prosedyrene utføres, kontroller at strømmen er frakoblet likestrømkretsen.**

Aviso **Antes de executar um dos seguintes procedimentos, certifique-se que desligou a fonte de alimentação de energia do circuito de corrente contínua.**

¡Advertencia! **Antes de proceder con los siguientes pasos, comprobar que la alimentación del circuito de corriente continua (CC) esté cortada (OFF).**

Varning! **Innan du utför någon av följande procedurer måste du kontrollera att strömförsörjningen till likströmskretsen är bruten.**

Предупреждение Перед выполнением любых описанных ниже действий убедитесь, что цепь питания постоянным током отключена.

警告 在进行下述任一操作过程之前，要确保将电源从直流电路上断开。

警告 次の手順を開始する前に、DC回路から電源が切断されていることを確認してください。

1.6.2 Main Disconnecting Device

Warning **The plug-socket combination must be accessible at all times, because it serves as the main disconnecting device.**

Waarschuwing **De combinatie van de stekker en het elektrisch contactpunt moet te allen tijde toegankelijk zijn omdat deze het hoofdmechanisme vormt voor verbreking van de aansluiting.**

Varoitus **Pistoke/liitinkohta toimii pääkatkaisumekanismina. Pääsy siihen on pidettävä aina esteettömänä.**

Attention **La combinaison de prise de courant doit être accessible à tout moment parce qu'elle fait office de système principal de déconnexion.**

Warnung **Der Netzkabelanschluß am Gerät muß jederzeit zugänglich sein, weil er als primäre Ausschaltvorrichtung dient.**

Figyelem! **A dugaszolóaljzat és a dugasz együttesének mindig hozzáférhetõnek kell lennie, mivel ez szolgál fõmegszakítóként.**

Avvertenza **Il gruppo spina-presa deve essere sempre accessibile, poiché viene utilizzato come dispositivo di scollegamento principale.**

Advarsel **Kombinasjonen støpsel/uttak må alltid være tilgjengelig ettersom den fungerer som hovedfrakoplingsenhet.**

Aviso **A combinação ficha-tomada deverá ser sempre acessível, porque funciona como interruptor principal.**

¡Advertencia! **El conjunto de clavija y toma ha de encontrarse siempre accesible ya que hace las veces de dispositivo de desconexión principal.**

Varning! **Man måste alltid kunna komma åt stickproppen i uttaget, eftersom denna koppling utgör den huvudsakliga frånkopplingsanordningen.**

Предупреждение Штепсельная розетка всегда должна быть доступна, поскольку она служит основным устройством отключения.

警告 插销和插座必须便于随时插拔，因为它是主要断电设备。

警告 主要な切断装置となるので、プラグとソケットは常に手が届く場所に置く必要があります。

1.6.3 Laser Radiation Warning

Warning **Invisible laser radiation may be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments.**

Waarschuwing **Losgekoppelde of losgeraakte glasvezels of aansluitingen kunnen onzichtbare laserstraling produceren. Kijk niet rechtstreeks in de straling en gebruik geen optische instrumenten rond deze glasvezels of aansluitingen.**

Varoitus **Irrotetuista kuiduista tai liittimistä voi tulla näkymätöntä lasersäteilyä. Älä tuijota säteitä tai katso niitä suoraan optisilla välineillä.**

Attention **Les fibres ou connecteurs débranchés risquent d'émettre des rayonnements laser invisibles à l'œil. Ne regardez jamais directement les faisceaux laser à l'œil nu, ni d'ailleurs avec des instruments optiques.**

Warnung **Unterbrochene Fasern oder Steckerverbindungen können unsichtbare Laserstrahlung abgeben. Blicken Sie weder mit bloßem Auge noch mit optischen Instrumenten direkt in Laserstrahlen.**

Figyelem! **A nem csatlakoztatott üvegszálak és csatlakozók láthatatlan lézersugárzást bocsáthatnak ki. Ne nézzen bele a sugárba, és ne nézze közvetlenül, optikai berendezések segítségével!**

Avvertenza **Le fibre ottiche ed i relativi connettori possono emettere radiazioni laser. I fasci di luce non devono mai essere osservati direttamente o attraverso strumenti ottici.**

Advarsel **Det kan forekomme usynlig laserstråling fra fiber eller kontakter som er frakoblet. Stirr ikke direkte inn i strålene eller se på dem direkte gjennom et optisk instrument.**

Aviso **Radiação laser invisível pode ser emitida de conectores ou fibras desconectadas. Não olhe diretamente para os feixes ou com instrumentos ópticos.**

¡Advertencia! **Es posible que las fibras desconectadas emitan radiación láser invisible. No fije la vista en los rayos ni examine éstos con instrumentos ópticos.**

Varning! **Osynlig laserstrålning kan avges från frånkopplade fibrer eller kontaktdon. Rikta inte blicken in i strålar och titta aldrig direkt på dem med hjälp av optiska instrument.**

Предупреждение Отключенные световоды и разъемы могут испускать невидимое лазерное излучение. Не допускайте попадания лазерного луча в глаза и не смотрите на него через оптические приборы.

警告 断开的光纤或接头有可能发出不可见的激光辐射。请勿直视光束或直接用光学仪器观看光束。

警告 光ファイバ ケーブルまたはコネクタを取り外した状態では、目に見えないレーザー光が放射されていることがあります。光線をのぞきこんだり、光学機器を使用して光線を直接見たりしないでください。

1.6.4 Unterminated Fiber Warning

Warning **Invisible laser radiation may be emitted from the end of the unterminated fiber cable or connector. Do not view directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm may pose an eye hazard.**

Waarschuwing **Er kunnen onzichtbare laserstralen worden uitgezonden vanuit het uiteinde van de onafgebroken vezelkabel of connector. Niet in de straal kijken of deze rechtstreeks bekijken met optische instrumenten. Als u de laseruitvoer met bepaalde optische instrumenten bekijkt (zoals bijv. een oogloep, vergrootgras of microscoop) binnen een afstand van 100 mm kan dit gevaar voor uw ogen opleveren.**

Varoitus **Päättämättömän kuitukaapelin tai -liittimen päästä voi tulla näkymätöntä lasersäteilyä. Älä tuijota sädettä tai katso sitä suoraan optisilla välineillä. Lasersäteen katsominen tietyillä optisilla välineillä (esim. suurennuslasilla tai mikroskoopilla) 10 cm:n päästä tai sitä lähempää voi olla vaarallista silmille.**

Attention **Des émissions de radiations laser invisibles peuvent se produire à l'extrémité d'un câble en fibre ou d'un raccord sans terminaison. Ne pas fixer du regard le rayon ou l'observer directement avec des instruments optiques. L'observation du laser à l'aide certains instruments optiques (loupes et microscopes) à une distance inférieure à 100 mm peut poser des risques pour les yeux.**

Warnung **Eine unsichtbare Laserstrahlung kann vom Ende des nicht angeschlossenen Glasfaserkabels oder Steckers ausgestrahlt werden. Nicht in den Laserstrahl schauen oder diesen mit einem optischen Instrument direkt ansehen. Ein Betrachten des Laserstrahls mit bestimmten optischen Instrumenten, wie z.B. Augenlupen, Vergrößerungsgläsern und Mikroskopen innerhalb eines Abstands von 100 mm kann für das Auge gefährlich sein.**

Figyelem! **A lezáratlan optikai kábelek és a csatlakozók láthatatlan lézerfényt bocsáthatnak ki. Ne nézzen bele a sugárba, és ne nézze közvetlenül, optikai berendezések segítségével! Ha a kibocsátott lézert 100 mm-esnél kisebb távolságból nézi bizonyos optikai eszközökkel (például nagyítóval vagy mikroszkóppal), látáskárosodást szenvedhet.**

Avvertenza **L'estremità del connettore o del cavo ottico senza terminazione può emettere radiazioni laser invisibili. Non fissare il raggio od osservarlo in modo diretto con strumenti ottici. L'osservazione del fascio laser con determinati strumenti ottici (come lupette, lenti di ingrandimento o microscopi) entro una distanza di 100 mm può provocare danni agli occhi.**

Advarsel **Usynlig laserstråling kan emittere fra enden av den ikke-terminerte fiberkabelen eller koblingen. Ikke se inn i strålen og se heller ikke direkte på strålen med optiske instrumenter. Observering av laserutgang med visse optiske instrumenter (for eksempel øyelupe, forstørrelsesglass eller mikroskoper) innenfor en avstand på 100 mm kan være farlig for øynene.**

Aviso **Radiação laser invisível pode ser emitida pela ponta de um conector ou cabo de fibra não terminado. Não olhe fixa ou diretamente para o feixe ou com instrumentos ópticos. Visualizar a emissão do laser com certos instrumentos ópticos (por exemplo, lupas, lentes de aumento ou microscópios) a uma distância de 100 mm pode causar riscos à visão.**

¡Advertencia! **El extremo de un cable o conector de fibra sin terminación puede emitir radiación láser invisible. No se acerque al radio de acción ni lo mire directamente con instrumentos ópticos. La exposición del ojo a una salida de láser con determinados instrumentos ópticos (por ejemplo, lupas y microscopios) a una distancia de 100 mm puede comportar lesiones oculares.**

Varning! **Osynlig laserstrålning kan komma från änden på en oavslutad fiberkabel eller -anslutning. Titta inte rakt in i strålen eller direkt på den med optiska instrument. Att titta på laserstrålen med vissa optiska instrument (t.ex. lupper, förstoringsglas och mikroskop) från ett avstånd på 100 mm kan skada ögonen.**

Предупреждение Световоды и разъемы без заглушек могут испускать невидимое лазерное излучение. Не допускайте попадания лазерного луча в глаза и не смотрите на него через оптические приборы. Нельзя смотреть на источник лазерного излучения через некоторые оптические приборы (например увеличительное стекло, лупу или микроскоп) с расстояния ближе 100 мм: это может привести к травме органов зрения.

警告 无终端接头的光纤缆的末端或接头有可能发出不可见的激光辐射。请勿直视光束或直接用光学仪器观看。在 100 毫米的距离内用某些光学仪器（例如小型放大镜、放大镜和显微镜）观看激光输出有可能伤害眼睛。

警告 終端されていない光ファイバ ケーブルまたはコネクタの開口部からは、目に見えないレーザー光線が放射されていることがあります。光線をのぞきこんだり、光学機器を使用して直接見たりしないでください。ある種の光学機器（ルーペ、拡大鏡、顕微鏡など）を使用して 100 mm 以内の距離からレーザー光線を見ると、目を痛めることがあります。

1.6.5 Class 1 Laser Product Warning

Warning	**Class 1 laser product.**
Waarschuwing	**Klasse-1 laser produkt.**
Varoitus	**Luokan 1 lasertuote.**
Attention	**Produit laser de classe 1.**
Warnung	**Laserprodukt der Klasse 1.**
Figyelem!	**Class 1 besorolású lézeres termék.**
Avvertenza	**Prodotto laser di Classe 1.**
Advarsel	**Laserprodukt av klasse 1.**
Aviso	**Produto laser de classe 1.**
¡Advertencia!	**Producto láser Clase I.**
Varning!	**Laserprodukt av klass 1.**
Предупреждение	Лазерное устройство класса 1.
警告	这是 1 类激光产品。
警告	クラス1レーザー製品です。
주의	1급 레이저 제품.

CHAPTER 2

Product Overview

This section describes the functionality and the features of the Cisco ONS 15302 R2.0.

2.1 Functional Overview

The main R1.0 to R2.0 enhancement is the introduction of GFP/LCAS, which is a Ethernet framing standard to transport Ethernet packets in virtual containers through a SDH network. Additionally this edition introduces a new option for management connectivity, which will simplify design and configuration of a network supplied by Cisco. All features in this release is aligned with new releases of ONS 15305.

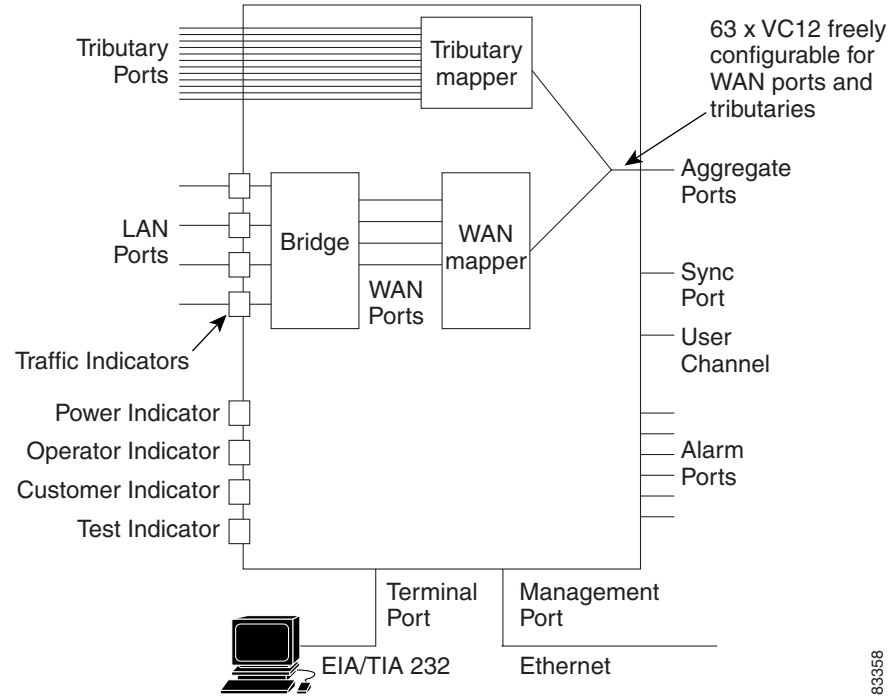
The ONS 15302 is an Integrated Access Device mainly intended for use in fibre optic networks, but can also be supplied as a hardware option with support for electrical STM-1. The ONS 15302 combine IP- and TDM-traffic, by running IP- along with TDM-channels inside an SDH STM-1 frame structure that can be easily carried across the network. The bandwidth of the IP-channel is configurable up to 100 Mb/s true “wire-speed”. The IP part of the ONS 15302 R2.0 consists of a L2/L3 switch.

Each tributary interface (E1) is mapped into a VC-12 container while the WAN traffic can be transported via either nxVC-3 or nxVC12.

The ONS 15302 have room for a plug-in module, which adds more WAN-ports to achieve multiple connections with differentiated bandwidth per customer and/or service.

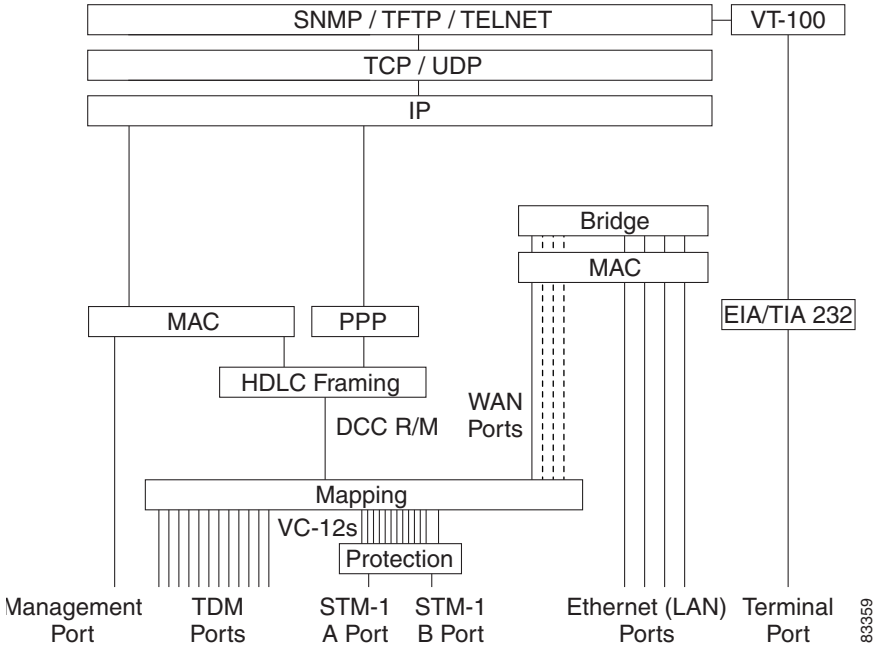
The ONS 15302 management solution is based on an embedded SNMP agent. The CiscoEdgeCraft, a SNMP Craft utility cover any operators' need is supplied with the deliveries of ONS 15302. Minimum required to operate and configure the ONS 15302 is a simple VT100 command line interface (CLI) for direct communication with the embedded SNMP agent.

Figure 2-1 ONS 15302 Functional Overview



From an element management perspective, the ONS 15302 is a multi-protocol machine with several types of interfaces as shown in Figure 2-2.

Figure 2-2 Functional Model for the ONS 15302



2.2 Features

This section describes the features of the Cisco ONS 15302 R2.0

2.2.1 SDH Multiplexing and Mapping

The aggregate interface supports only terminal multiplexer functions, with a mixture of terminated VC-12 and/or VC-3 container as indicated in Figure 2-4.

The internal structure of the ONS15302 is depicted in Figure 2-3. The bridge/router receives an Ethernet frame/IP datagram on one of the ports and decides on which port to send it out. The Ethernet Mapper maps the Ethernet frames into VC-12/VC-3 containers while the Tributary Mapper converts between E1 signals and VC-12s. The SDH Multiplexer is responsible for the multiplexing of VC-12/VC-3 containers into STM-1. The VC-12/VC-3 containers are sent to - and received from - either the Tributary Mapper or the Ethernet Mapper.

Figure 2-3 Multiplexing and Mapping in the ONS 15302

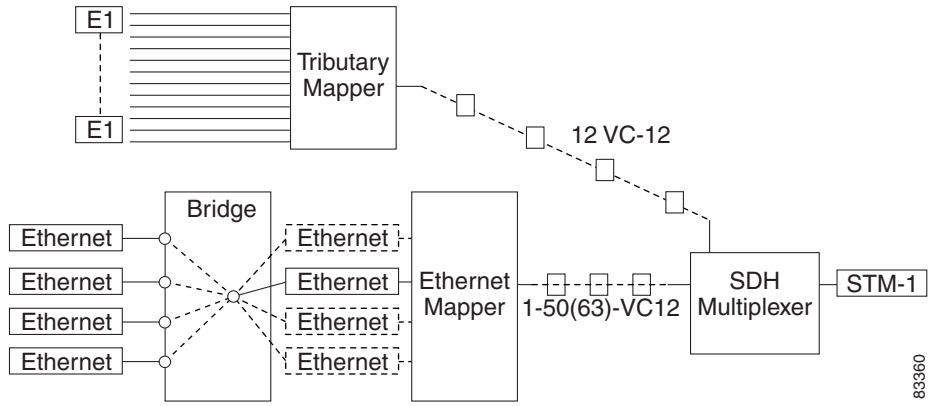
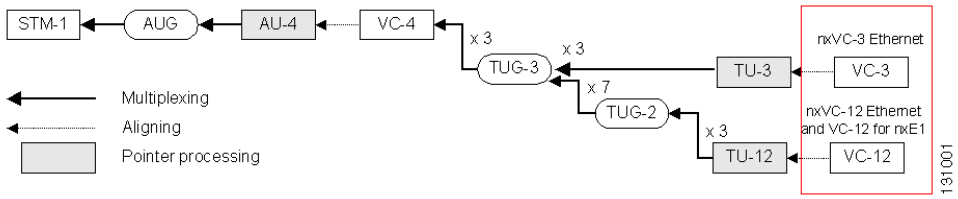


Figure 2-4 Multiplexing Structure in STM-1



The mapping between the tributary interfaces and the WAN port is fully flexible. An example of mapping is shown in Table 2-1.

Table 2-1 Example of a Mapping Scheme for ONS 15302

VC-12 (KLM)	Linked to
1.1.1	TRIBUTARY (1)
2.1.1	TRIBUTARY (2)

Table 2-1 Example of a Mapping Scheme for ONS 15302 (continued)

VC-12 (KLM)	Linked to
3.1.1	TRIBUTARY (3)
1.2.1	TRIBUTARY (4)
2.2.1	TRIBUTARY (5)
3.2.1	TRIBUTARY (6)
1.3.1	TRIBUTARY (7)
2.3.1	TRIBUTARY (8)
3.3.1	WAN-PORT (Only one WAN port is used)
1.4.1	WAN-PORT (Only one WAN port is used)
2.4.1	WAN-PORT (Only one WAN port is used)
... and so forth until...	
3.5.3	WAN-PORT (Only one WAN port is used)
1.6.3	WAN-PORT (Only one WAN port is used)
2.6.3	TRIBUTARY (9)
3.6.3	TRIBUTARY (10)
1.7.3	TRIBUTARY (11)
2.7.3	TRIBUTARY (12)
3.7.3	Unused

The VC-12 containers can be freely allocated to the different WAN ports or the tributary ports.

2.2.2 Protection

The ONS 15302 offers 1+1 linear Multiplex Section Protection (MSP). The protocol used for K1 and K2 (b1-b5) is defined in ITU-T G.841, clause 7.1.4.5.1. The protocol used is 1+1 bi-directional switching compatible with 1:n bi-directional switching.

The operation of the protection switch is configurable as described in Table 2-2.

Table 2-2 Protection Switch Parameters

Parameters	Description	Default Settings
MSP Enabled	• Enabled • Disabled	Disabled
Switching Type	• Unidirectional • Bidirectional	Unidirectional
Operation Type	• Revertive • Non-revertive	Enabled
Wait to restore time	Number of seconds to wait before switching back to the preferred link after it has been restored	300 seconds

Table 2-2 Protection Switch Parameters (continued) (continued)

Parameters	Description	Default Settings
Preferred Link	Identifier of the preferred working link	Always LINK A for ONS 15302 R2.0
Switching Command for active port	• Clear • Lockout of Protection, • Forced Switched to Protection • Forced Switched to Working • Manual Switched to Protection • Manual Switched to Working • Exercise • No-Command	No-Command
Working Link	Identifier of the current working link	—
Local Request	Local request contained in K1 byte	—
Remote Request	Remote request contained in K1 byte	—
PERSISTENCY FILTER ALARM ON	Filtering of transient alarms. Defines the number of seconds an alarm must be on to be registered.	—
PERSISTENCY FILTER ALARM OFF	Filtering of transient alarms. Defines the number of seconds an alarm must be off to be registered.	—
ALARM REPORTING	ENABLED or DISABLED. Set the alarm reporting capability for this object. See Table 2-3	—

Table 2-3 Protection alarm

Alarm ID	Description
MSP	Problem with MSP signalling with another NE across K1/K2 bytes.

2.2.3 Performance Monitoring

The ONS 15302 offers full G.826 performance monitoring at the RS, MS, VC-4, and VC-12 levels in the SDH hierarchy. This includes B1 near end in RSOH section, B2 near and far end in MSOH section, B3 near and far end at VC-4 level and BIP-2 near and far end at VC-12 level.

The ONS 15302 calculates excessive error and degrade signal defects assuming Poisson distribution of errors, according to ITU-T G.826.

The excessive error defect (dEXC) is detected if the equivalent BER exceeds a preset threshold of 10 exp –5, and be cleared if the equivalent BER is better than 10 exp –6, according to ITU-T G.806.

The degraded signal defect (dDEG) is detected if the equivalent BER exceeds a preset threshold of 10 exp –X, where x=6,7,8 or 9. The dDEG is cleared if the equivalent BER is better than 10 exp –(X+1), according to ITU-T G.806.The threshold is individually configurable for the different levels in the SDH hierarchy, from 10 exp –6 to 10 exp –9.

2.2.4 Synchronization

ONS 15302 can synchronize to the following sources:

- An STM-1 interface (working link or backup link)
- The dedicated 2048 kHz sync input (Sync Port)
- A tributary port (PRA mode)
- A local oscillator

Tributary synchronization is only relevant when in PRA mode at the chosen tributary.

The synchronization source is a configurable parameter. If it is impossible to synchronize to the selected source, an alarm will be raised, and the system will automatically switch to free running, that means the local oscillator.

Switchback to the selected source is performed automatically whenever it becomes possible again. The alarm is cleared when the switchback is successful.

The ONS 15302 operates in three different modes:

- Locked
- Holdover
- Free running

The default synchronization source is the local oscillator. The tolerance for this oscillator is +/– 10 ppm. ONS 15302 also provides a 2048 kHz sync output for synchronization of external equipment.

Note The ONS 15302 does not support SSM signaling in the S1 byte. By default transmitted value is “do not use”.

Note SSM signalling in S1 byte support in the ONS 15302 is not relevant since the network element does only support the configuration of one single sync-source at the time. In case of a protected device, i.e. an hardware variant of ONS 15302 with two aggregate interfaces configured in 1+1 MSP protection, the configuration of synchronisation source should be set to sync-source=**active**.

2.3 Ethernet over SDH mapping

This chapter describes the Cisco ONS 15302 Ethernet over SDH mapping.

2.3.1 Mapping modes

The ONS 15302 R2.0 supports two different modes of Ethernet over SDH (EOS) mapping

- Proprietary mapping combined with inverse multiplexing at VC-12 level
- GFP-F mapping, combined with VCAT, at VC-12 and VC-3 level, and LCAS

Note The support of the different EOS modes are dependent on the WAN module inserted. WAN module with ICS 01 supports Proprietary mapping, WAN module with ICS 02 supports Proprietary mapping and GFP-F mapping on a pr. port basis.

2.3.1.1 Proprietary mapping

The ONS 15302 R2.0 provides a proprietary mapping scheme for mapping of Ethernet traffic into a number of VC-12 containers.

The HDLC encapsulated Ethernet frames are mapped into a number of VC-12 containers in a round-robin fashion with an inverse multiplexer function. The mapping process is described in 2.2.1 SDH Multiplexing and Mapping, page 2-3.

A total differential delay of up to 8ms is supported.

The total bandwidth for one WAN channel is 100 Mbps or 50xVC-12 containers. AXXESSIT Proprietary VC-12 mapping scheme for Ethernet take advantage of 2,16 Mbps in each VC-12, which means that 47xVC-12 are sufficient to transport 100Mbps Ethernet.

The VC-12 k.l.m reference assignment for the Ethernet WAN port is fully flexible, and controlled in the same way as a VC-12 cross connect.

The sequence number attached to each VC-12 is used for alarm indication only in case of a sequence mismatch, the sequence number is not used for reordering of the incoming VC-12's. The order of VC's carrying Ethernet traffic between two WAN-ports therefore needs to be obtained.

In case of a failure on one of the VC-12's, the effected VC-12 is removed from the channel, allowing the traffic to flow on the remaining VC-12 connections. RDI is used to indicate a failure to the remote side.

2.3.1.2 Standardised mapping

The ONS 15302 R2.0 supports standardised ways of mapping Ethernet over SDH. The mapping schemes includes mapping protocol, concatenation scheme and control protocols.

2.3.1.2.1 Generic Framing Procedure

ONS 15302 R2.0 supports framed mapped GFP (GFP-F) according to ITU-T 7041.The GFP implementation supports the following functions:

- The implementation only supports GFP null extension header
- Client data frames are supported
- Client management frames are supported
- For control frames, the implementation only supports GFP idle frames insertion and processing, other unspecified control frames are dropped
- Standard GFP scrambling is supported, with the polynomial 1+x43
- The implementation supports the optional data FCS insertion and checking via the PFI bit
- The implementation supports frame sizes from 9 bytes up to 64kbytes (only sizes from 64 bytes to 9k bytes are applicable for this implementation)

GFP Alarm and Event Conditions

The GFP implementation supports the following alarm and event conditions:

- GFP Frame Delineation Loss Event, LFD
- Payload Mismatch, PLM
  - Alarm based on detection of PTI field value in ITU-T G.7041
- User Payload Mismatch, UPM
  - Alarm based on detection of UPI field value in ITU-T G.7041
- Payload FCS Mismatch, PFM.
  - Alarm based on detection of PFI field value in ITU-T G.7041
- Extension Header Mismatch, EXM
  - Alarm based on detection of EXI field value in ITU-T G.7041

GFP Performance Monitoring

The GFP implementation collects the following performance parameters:

- Total number GFP frames transmitted and received
- Total number Client management frames transmitted and received
- Number of bad GFP frames received, based upon payload CRC calculation
- Number of cHEC correted errors
- Number of cHEC uncorrected errors
- Number of tHEC correted errors
- Number of tHEC uncorrectee errors
- Number of Dropped GFP frames Downstream

A degrade alarm is available for the following performance parameters:

- Number of bad GFP frames received, based upon payload CRC calculation, degFCS
- Number of tHEC corrected and uncorrected errors, degtHEC

The deg alarms are handled in a similar way as the SDH degrade alarms.

2.3.1.2.2 Virtual Concatenation (VCAT) and LCAS

The ONS 15302 R2.0 supports virtual concatenation according to ITU-T 707. The VCAT implementation supports the following functions:

- VC-12-nV, where n=1..50
- VC-3-nV, where n=1..3

The VC-x level is individually configurable pr. mapper port, a mix of different VC-x levels in one VCG group is not allowed.

A total differential delay of up to 62ms is supported for the different VCG groups.

ONS 15302 R2.0 supports the LCAS protocol in conjunction with VCAT as defined in ITU-T 7042. The LCAS protocol implemented covers the following functions:

- Automatically temporary removal of a faulty VCAT member
- Automatically insertion of a temporary removed VCAT member when the fault is repaired
- Hitless increase of the VCG capacity by adding a VCG new member
- Hitless decrease of the VCG capacity by removing a current VCG member
- Inter-working with equipment supporting VCAT but not supporting LCAS

VCAT and LCAS configuration modes

The ONS 15302 R2.0 offers two different operation modes for the VCAT and LCAS functionality, the two modes are:

1. VCAT with LCAS enabled
2. VCAT without LCAS enabled

Mode 1

VCAT with LCAS enabled is always uni-directional, which enables the possibility to have different capacity in each direction, but requires a separate cross connect/capacity setup in each direction.

Mode 2

When VCAT is used without LCAS, there is no mechanism for removing of a faulty VC container in a VCG group. To solve this problem the ONS 15302 R2.0 implements, in addition to the standard mode, a proprietary mode.

The following configuration is available in mode 2:

- Default mode, unidirectional connections with the possibility of configuring symmetric capacity as explained in mode 1. Same features as in mode 1 but without LCAS
- SoftLCASBidirectional mode

If SoftLCASBidirectional mode is enabled, the cross connections are uni-directional, but bi-directional. In addition RDI signalling are enabled. A faulty container in a VCG group is removed based upon the VC alarm condition or based upon RDI signalling (similar to the proprietary mapping). This will allow a VCG group to continue operation even if the VCG has a failed member. This configuration mode is proprietary.

VCAT and LCAS Alarm and Event Conditions

The following alarms related to the VCAT and LCAS are reported by default:

Table 2-4 Default alarms - VCAT and LCAS

Alarm	Description
LOM	Vcat, loss of multiframe
SQM	Vcat sequence indicator mismatch
LOA	Lcas loss of alignment for channels with traffic
GIDERR	Lcas Group Id different for active channels
LCASCRC	Lcas CRC error detected
NONLCAS	Lcas non-Lcas source detected
PLCR	Lcas partial loss of capacity receive
TLCR	Lcas total loss of capacity receive
PLCT	Lcas partial loss of capacity transmit
TLCT	Lcas total loss of capacity transmit
FOPR	Lcas failure of protocol
SQNC	Inconsistent SQ numbers

In addition to the above default alarms, the following alarms are available if enabled from the management system:

Table 2-5 Optional alarms - VCAT and LCAS

Alarm	Description
acMstTimeout	Lcas acMst timeout
rsAckTimeout	Lcas RS-ack timeout
eosMultiple	Lcas two or more channels have EOS
eosMissing	Lcas one channel has EOS
sqNonCont	Lcas missing SQ detected in set of channels
sqMultiple	Lcas equal SQ for two or more channels
sqOor	Lcas SQ outside of range

Table 2-5 Optional alarms - VCAT and LCAS (continued)

Alarm	Description
mnd	Lcas member not deskewable
ctrlOor	Lcas undefined Ctrl-word for one or more channels

2.4 Switch Features (Bridging)

The bridge is a transparent multi port remote Ethernet bridge as specified in IEEE 802.3. The Bridge consists of four LAN ports and four WAN port. Each port may have its own MAC address, but in most configurations one MAC address for the whole bridge is sufficient. The four LAN ports support 10/100BaseT Ethernet for UTP cables. Both 10 Mbit/s (Mbps) and 100 Mbit/s (Mbps) are supported with auto negotiation. The LAN ports are compatible with IEEE 802.3.

In addition to standard bridging functionality support, the ONS 15302 also support provider bridge functionality.

2.4.1 L2 Bridging

The bridge supports the following features:

- MAC switching
- Static MAC entries
- Support of up to 32k MAC addresses
- Automatic Learning & Ageing for MAC addresses
- Auto negotiation (speed/duplex)
- Fixed Ethernet Port settings i.e. 10/100 half/full duplex
- MAC Multicast
- Transparent Bridging
- Port-based Virtual LANs (VLANs)
- VLAN by Port and VLAN by Port and Protocol
- IEEE 802.1Q VLAN tagging compliance (VLAN id. 1-4000)
- Head of Line Blocking prevention
- Back pressure and flow control Handling
- IGMP snooping
- Mirroring Port
- IEEE 802.1p priorities (Strict Policy, 4 queues)
- GARP VLAN registration protocol (GVRP)
- MTU Size 6144 bytes

- Rapid spanning tree protocol according to 802.1w

The filtering rate of the bridge is able to operate at full wire speed. The forwarding rate is only limited by the forwarding interface speed, i.e. the selected WAN port speed.

The ONS 15302 R2.0 also support a LAN-WAN port correlation function used in architectures requiring Ethernet protection. The port correlation function, if enabled on a LAN port, reflects the status of the corresponding WAN port on the actual LAN port. This means that if the operational capacity of the WAN port is 0, due to a network error, the corresponding LAN port is disabled, allowing external equipment to very rapidly detect the network error and thereby switch to the other path.

2.4.2 L2 Provider Bridging Functionality

In addition to the standard L2 functionality the following Provider Bridge functionality is supported:

- Tag insertion/removal for Provider bridging/ VLAN tunnelling support
- Protocol tunnelling, offering transparency of the following MAC addresses/protocols:
  - All MAC addresses in the range from 0180C2000000 to 0180C20000FF,except...01, is transported transparently, including the following protocols: RSTP.MSTP.STP,GVRP,GMRP,LACP and 802.1x

The offering of Provider bridging /VLAN tunnelling and protocol tunnelling enables the user to offer transparent Ethernet services in a L2 network with guaranteed security, also called L2 VPN's. The functionality is enabled at the ingress and egress ports in the network.

The Ethertype used for the Tag insertion is 0xFFFF, inter operability with other systems using 0x8100 is obtained by enabling Ethertype swapping on the WAN ports. This functionality is only supported on the new WAN module.

2.4.3 Quality of Service

The QoS features can be used to allocate bandwidth for users or applications at layer 2 and layer 3.

The ONS 15302 performs the following functions:

- Classification:
  - Identifying which packet get which treatment
- Metering
  - Measuring a flow of packets to see if it conforms to desired measurement
- Policing
  - Taking actions on frames according to whether they conform or not

Traffic shaping is not performed by the ONS 15302.

The ONS 15302 allows the operator full control each element of the packet/frame handling.

The QoS implementation supports several profile types, where each profile defines the nature of handling applied to frames belonging to that profile (e.g. amount of BW to be provided). A Classifier is a definition of which parts of the frames contents should be used to decide which frame belongs to which profile (e.g. which header bytes are of interest). Rules within each profile detail for each frame with a specific combination of values in the “interesting” bytes, which actions to take.

The following profiles are possible:

- Reserved Bandwidth allocation (“BW guarantee”) - A specific amount of Bandwidth is reserved for this profile. Traffic will not be allowed to go above this limit.
- Minimum BW guarantee - A specific amount of Bandwidth is reserved for this profile, but traffic may use more than the reserved amount, if available, at the best-effort service class.
- Reserved Bandwidth with Minimum Delay Guarantee - Traffic in this profile has reserved bandwidth, as explained above, and in addition is forwarded with minimum delay (i.e. sent before traffic belonging to one of the above profiles).
- Reserved Bandwidth with Minimum Delay Guarantee per session - Traffic in this profile is composed of a number of Sessions (identified by appropriate classifiers) with each one getting a specified Bandwidth reservation, as defined above, and with traffic for this profile being forwarded with the minimum delay, as explained above.

The two Minimum Delay Guarantee options are only available for Layer 3 (IP) QoS.

The following classifiers are possible:

- For each protocol supported (IP and Bridging) the user should define which header fields are of interest. Each such group of bytes is a classifier.
- Using the Policy MIB the user may specify fields in a general manner, using their offset. Using the Simple MIB, pre-defined possibilities cover the standard header fields of each protocol (e.g. Addresses, Ports, etc.).
  - In IP the predefined fields are: Source/Destination Addresses and ports, Protocol (TCP/UDP), TOS type.
  - For Layer 2 switching, predefined fields are Input Port only

The following rules are possible:

- After classifiers and profiles are defined, they are used to define rules by which frames/packets are assigned to one of the profiles defined, and the actions to be carried out on matching frames/packets.
- Each rule contains a pattern to match (values to match in the fields of interest in the classifier) and action definitions. Actions possible are:
  - Assign to a profile
  - Modifications to frame/packet fields (e.g. re-writing DSCP for IP packets, New VPT for bridged traffic, etc.)
  - Forward, drop, or send to the CPU etc.

2.4.3.1 Limitations

It's important to know that packet priority mechanism is overruled by QoS and packets will not be served according to their priority. The Ethernet ports do not support auto-negotiation in this mode and the port settings must therefore be fixed configured for 10 or 100Mbit/s.

When defining aggregate flow values as part of the bandwidth limitation parameters in the QoS configuration, a non-linear distribution happen where the actual bandwidth differs from what may be expected. This is a result of the algorithm used in the switching chip. A calculated ratio may be provided to translate between the configured parameters and the resulted bandwidth. Bandwidth Guarantee, Minimum Bandwidth Guarantee and Minimum Delay are all aggregate profiles. When configuring the intended rate for one of these profiles the rate to configure depends on the total number of sessions transmitted in the profile's range.

A session means each stream of traffic that is different from the others in a set of classifier fields but still belongs to the same profile. For instance if the user defines IP classification based upon protocol and destination IP address, but configures the rule based only on destination IP address then each additional stream of traffic which goes to the same destination but has a different protocol number will represent an additional session in the profile's range. Two traffic streams that have the same destination IP and the same protocol number represent a single session. The first session will get 1/2 of the configured bandwidth, the second session will get 1/3, third will get 1/4, and so on.

The following table presents different scenarios:

Table 2-6 Scenarios - Intended rate vs. Rate to configure

Number of Sessions in profile	Intended Bandwidth in Kbps.	Rate to configure in Kbps
1	2000	4000
1	4000	8000
1	1000	2000
2	2000	2400
2	4000	4800
2	1000	1200
3	2000	1846
3	6000	5538
3	4000	3692
3	3000	2769

2.5 TDM Features

This section describes the Cisco ONS 15302 TDM features.

2.5.1 Tributary Ports

ONS 15302 provides 12 120 ohm 2.048 MHz Tributary Ports on the customer side. 75 ohm operation is supported by adding an external balun.

Each Tributary Port can be individually configured to run in one of the following modes:

- G.703 Transparent (TRA)
- ISDN Primary Rate Access (PRA)

Note PRA is implemented according to ETS 300011 and ETS 300233. The ONS 15302 can only implement the PRA NTE functions.

2.5.1.1 Transparent Transmission Mode.

In this mode 2.048 Mbit/s plesiochronous data and timing are transferred independently of frame structure. The two directions of transmission are completely independent of each other.

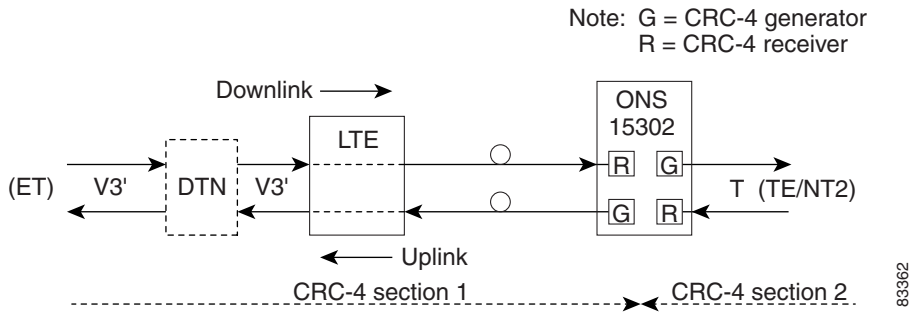
Downstream AIS is generated on loss of signal or loss of optical frame alignment.

2.5.1.2 ISDN Primary Rate Access (PRA) Transmission Mode.

The functional layout compliant to pr. ETS 300 233 is shown below.

DTN	Digital Network
V3' and V3	ISDN Reference Points, Exchange Termination Interface
T	ISDN Reference Point, Customer Interface
Downlink	Signal direction from Exchange Termination (ET)
Uplink	Signal direction to Exchange Termination (ET)

Figure 2-5 ONS 15302 ISDN PRA Configuration



2.5.2 Downlink Transfer

The LTE is transparent to the 2 Mbit/s (Mbps) signal. However, monitoring the G.704 multiframe format is performed for detection of loop back 1 command from the Exchange Termination (TS 0 bit Sa6).

The NTE terminates CRC-4 section 1 by the Receiver (R) circuits, which pass the signal to the Generator (G) circuits with indication of basic frame start. The G circuits generate new TS 0 basic frame and multiframe to CRC-4 section 2, and pass transparently TS1 - TS31 and from TS 0 the RAI bit and the Sa-bits 4 to 8. AIS is generated to the TE on loss of signal and when R circuits have lost alignment to G.704 basic frames.

2.5.3 Uplink

The NTE terminates CRC-4 section 2 in the R circuits, which pass the signal to the G circuits with indication of basic frame start. The G circuits generate new TS 0 basic frame and multiframe to CRC-4 section 1 and pass transparently TS1- TS31 and from TS 0 the RAI bit and the Sa-bits 4,7 and 8.

The G circuits generate substituted frames to the ET on loss of signal or loss of alignment to basic G.704 frames from TE.

The LTE is transparent to the 2 Mbit/s (Mbps) signal.

On loss of optical line signal, the LTE generates an auxiliary pattern AUXP=1010.. to the ET.

2.5.4 Supervision by the Exchange Termination (ET)

The TS 0 bits Sa5 and Sa6 are used for supervision. Bit Sa5 being 0 downlink and 1 uplink, indicates the direction of transmission.

2.5.4.1 ET generated Downlink Sa6 Codes

Normal condition Sa6 = 0000

Loop back 1 command to LTE Sa6 = 1111

Loop back 2 command to NTE Sa6 = 1010

2.5.5 NTE generated Uplink Sa6 Codes

Table 2-7 Time Slot 0 Signalling in PRA Mode

Condition	Uplink report to ExchangeTermination	Comments
Normal Operation	Sa6 = 00XX RAI = 0 Sa5 = 1	XX reports bit errors related to CRC-4 section 2
AIS Received at V3	Sa6 = 1111 RAI = 1 Sa5 = 1	RAI Generated by TE
Loss of SignalV3 (FV3) Loss of line signalor downlink FA (FC5)	Sa6 = 1110 RAI = 1 Sa5 = 1	RAI Generated by TE

Table 2-7 Time Slot 0 Signalling in PRA Mode (continued)

Condition	Uplink report to ExchangeTermination	Comments
Loss of Signal at T (FC4)	Sa6 = 1100 RAI = 0 Sa5 = 1	The NTE generates substituted frames with RAI=0. Reporting of other failure conditions has priority.
Power failure (NTE dying gasp)	Sa6 = 1000 RAI = X Sa5 = 1	Reporting of this failure condition has the highest priority.
Loss of Line Signal at LTE (FC1)	AUXP	Auxiliary alarm indication pattern(1010..) generated by the LTE.
Loop back 1 activated by downlink Sa6=1111	Sa6 = 1111 RAI = 1 Sa5 = 0	The downlink signal is looped back fully transparently in the LTE.
Loop back 2 activated by downlink Sa6=1010	Sa6 = 00XX RAI = 1 Sa5 = 0	The TS1-TS31 and the TS 0 bits RAI, Sa4, 7 and 8 of the downlink signal are looped back by the NTE. Sa5 is changed to 0 by the NTE to indicate loop back condition.

2.5.6 Handling of CRC-4 Errors

CRC-4 errors detected in R circuits downlink and uplink are inserted as E bits to the ET and TE respectively.

If multiframe alignment is not obtained, the NTE reports all E bits 0 error.

Detected bit errors related to CRC-4 section 2 are reported to the ET by use of the two last bits of the Sa6 code in normal operational condition.

Table 2-8 CRC-4 Section 2 Bit

	Events	Sa6
a)	CRC-4 errors detected by the NTE:	0010
b)	CRC-4 errors reported as E-bits from the TE:	0001
	a) + b) or no MF alignment to signal received from the TE:	0011

ITU-T Rec.G.706, ANNEX B is applied to CRC-4 section 2 which means that the NTE stops searching for MF alignment after a given period of time without further actions. Continuous Sa6 = 0011 indicates to the ET that quality information is not available from CRC-4 section 2.

2.6 Test Loops

Two test loops are provided per Tributary Port, one in the customer direction (LL3) and one in the network direction (LL2), (Figure 2-6). One Tributary Port can have only one loop activated at a time. The test loops can be activated, deactivated and monitored by the management system. The loop control logic depends on the tributary mode (TRA or PRA).

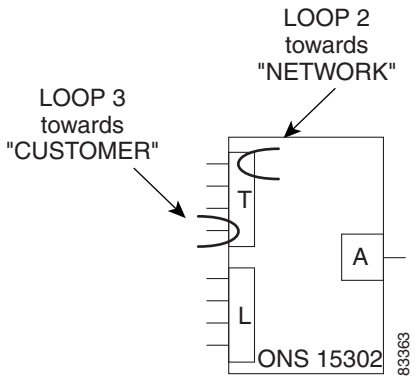
- In TRA mode the management system can operate the loops at any time as long as the port is enabled.
- In PRA mode the loops are supposed to be controlled by some exchange termination equipment (ET) via inband channel 0 control bits. In this mode it is not possible to operate the loops from the ONS 15302 management system.

It is possible to change the tributary mode regardless of the state of the loops. If the mode is changed, the loops will be cleared. The Test LED is on if any tributary loop is activated, regardless of the tributary mode.

To change the tributary mode, the loop must be cleared.

The Test Indicator LED is on if any tributary loop is closed, regardless of the tributary mode. This release does not support any monitor points.

Figure 2-6 Test Loops Schematic View



2.7 Alarm Ports

The ONS 15302 provides facilities to report four auxiliary alarm inputs for associated equipment, for example power unit failure, battery condition, cabinet door etc. These alarms are activated by an external loop between a pair of contacts.

The polarity of the auxiliary alarm input ports is a configurable parameter, this means alarm can be defined either as a loop closed or a loop open condition.

The alarms are reported to the management system. Each alarm input port may have an individual configurable textual description associated with it.

The ONS 15302 provides also support for two alarm output ports (Alarm out 1 and Alarm out 2) used to signal equipment alarms and traffic related alarms. Alarm out 1 and Alarm out 2 reflect the status of the operator LED and the customer LED respectively.

2.8 LED Indicators

The LED indicators are used to visualize the ONS 15302 status:

Table 2-9 LED Functionality on the WAN Module Side

Identity	Color	State On	State Flashing	State Off
PWR (Power)	Green	Presence of power	NA	Power failure
OPER (Operation)	Red	Alarm detected on aggregate interface	NA	No alarm detected on aggregate interface
CUST (Customer)	Red	Alarm detected on tributary or LAN interface	NA	No alarm detected on tributary or LAN interface
TEST (Test)	Yellow		One or more test are activated	
LAN 1	Green	Link is present	Traffic is present	Link down
LAN 2	Green	Link is present	Traffic is present	Link down
LAN 3	Green	Link is present	Traffic is present	Link down
LAN 4	Green	Link is present	Traffic is present	Link down

Table 2-10 LED Functionality on the Connector Array Side

Identity	Position	Color	State On	State Flashing	State Off
PWR (Power)		Green	Presence of power	NA	Power failure
OPER (Operation)		Red	Alarm detected on aggregate interface	NA	No alarm detected on aggregate interface
CUST (Customer)		Red	Alarm detected on tributary or LAN interface	NA	No alarm detected on tributary or LAN interface
TEST (Test)		Yellow		One or more test are activated	
LANn (n-1,2,3,4)	Left	Green	100 MBits/s (Mbps)	NA	NA
LANn (n-1,2,3,4)	Left	Yellow	10 MBits/s (Mbps)	NA	NA
LANn (n-1,2,3,4)	Right	Green	Link OK	Ethernet traffic in operation	Link down

2.9 User Channel

A transparent user channel is provided (F1 byte in RSOH) for transportation of general data. The interface is balanced RS485 and supports synchronous 64 kbit/s or asynchronous 19.2 kbit/s by configuration.

2.10 Automatic System Clock Setting

The ONS 15302 supports time protocol (RFC 868) for automatic date and time adjustment. To utilize this feature a TP server must be available in the network.

Because the time protocol provides UTC (GMT) only, and does not take into account the Day Light Saving Time (summer time), an additional parameter (UTC Delta) allows the user to get the local time. This parameter must be adjusted twice a year to take into account the Day Light Saving Time.

Relevant ONSCLI commands are found in Table 2-11 to Table 2-13.

Table 2-11 Current Device Time

ONSCLI Command	Description	Format
TIME (SYSTEM)	Should be adjusted during first time installation. In case of periods with lacks of power the Time settings will be kept in memory for a period of 48 hours	hh:mm:ss

Table 2-12 Current Device Date

ONSCLI Command	Description	Format
DATE	Should be adjusted during first time installation. In case of periods with lacks of power the Date settings will be kept in memory for a period of 48 hours.	yyyy-mm-dd

Table 2-13 UTC Delta

ONSCLI Command	Description	Format
UTC-DELTA	Used to adjust the GMT time received from the server to the local time, and to possibly take into account the Day-Light Saving Time. Default setting: 0	integer[-720:720min]

Note This parameter is not recommended or required to configure when using the CiscoEdgeCraft as configuration tool since this calculation is best maintained by the management system.

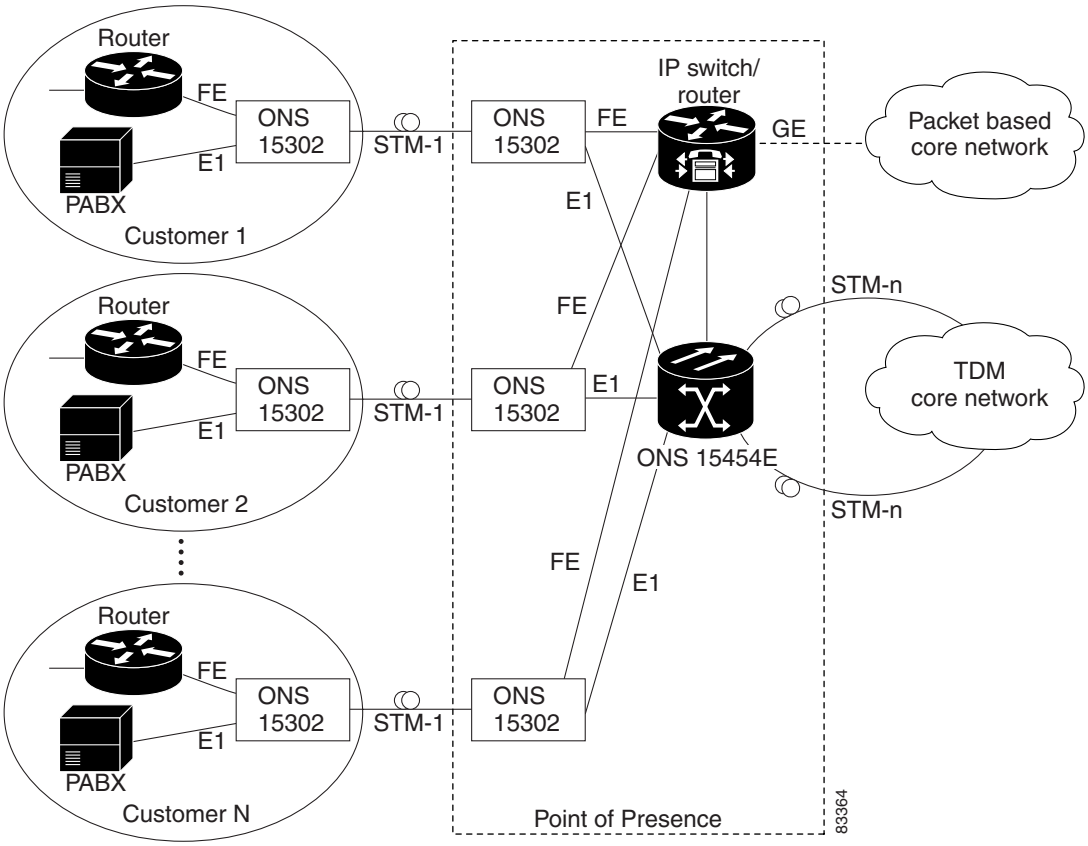
2.11 Applications

The following subsections describes different Cisco ONS 15302 applications.

2.11.1 Back to Back Application

Normally the ONS 15302 at the customer site is connected to an ONS 15302 at the operator point of presence (PoP). A number of these systems can be connected in a star network and the Ethernet traffic is groomed by an Ethernet switch before it is transmitted to the core network. Figure 2-7 shows the layout of a typical system with the ONS 15302 incorporated. The network in this figure does not have a separate Ethernet backbone network, but this could easily be supported.

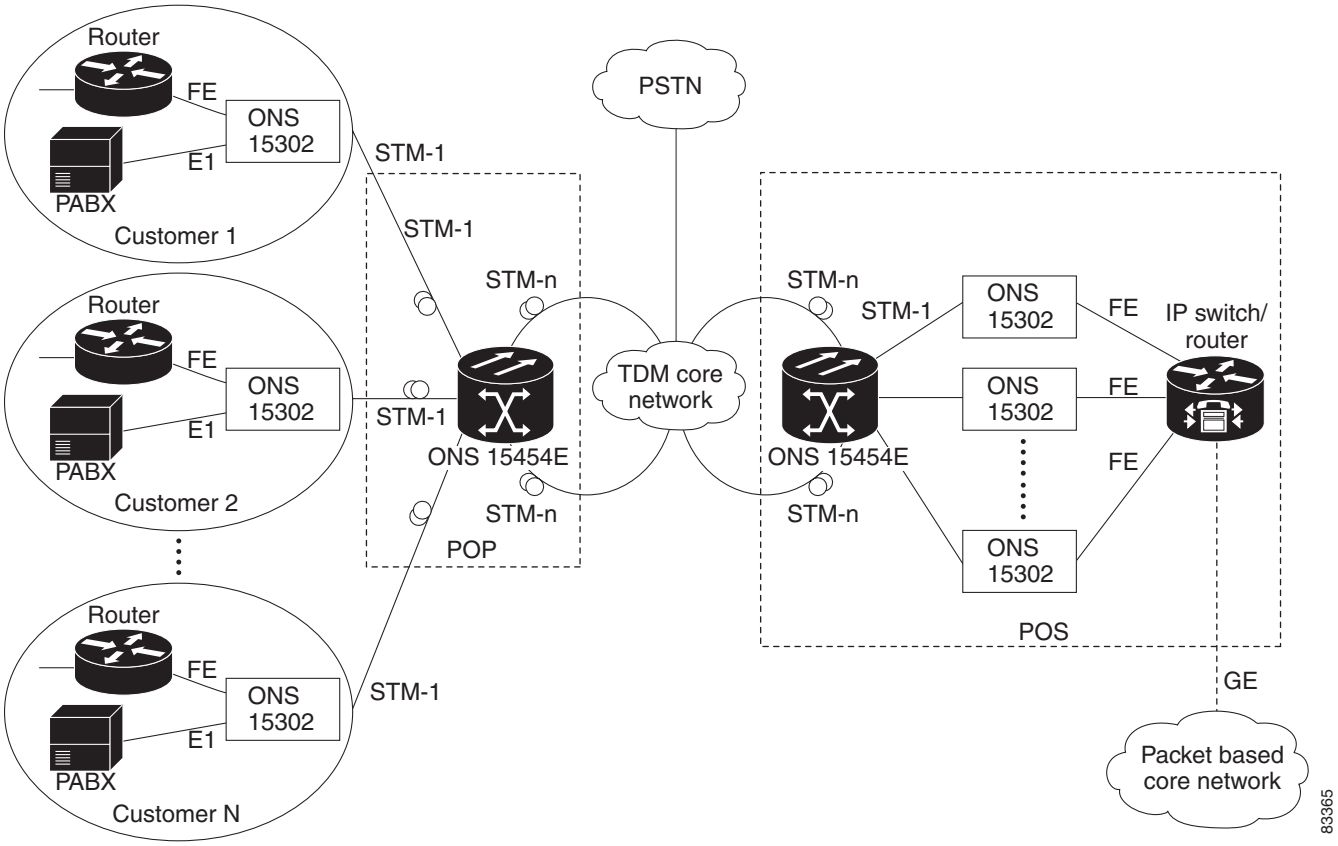
Figure 2-7 Back to Back Configuration across the Access Loop



2.11.2 Remote Back to Back Application

The ONS 15302 can also be directly connected to the SDH transport network if the operator wants to do Ethernet grooming at a different site as shown in the figure below.

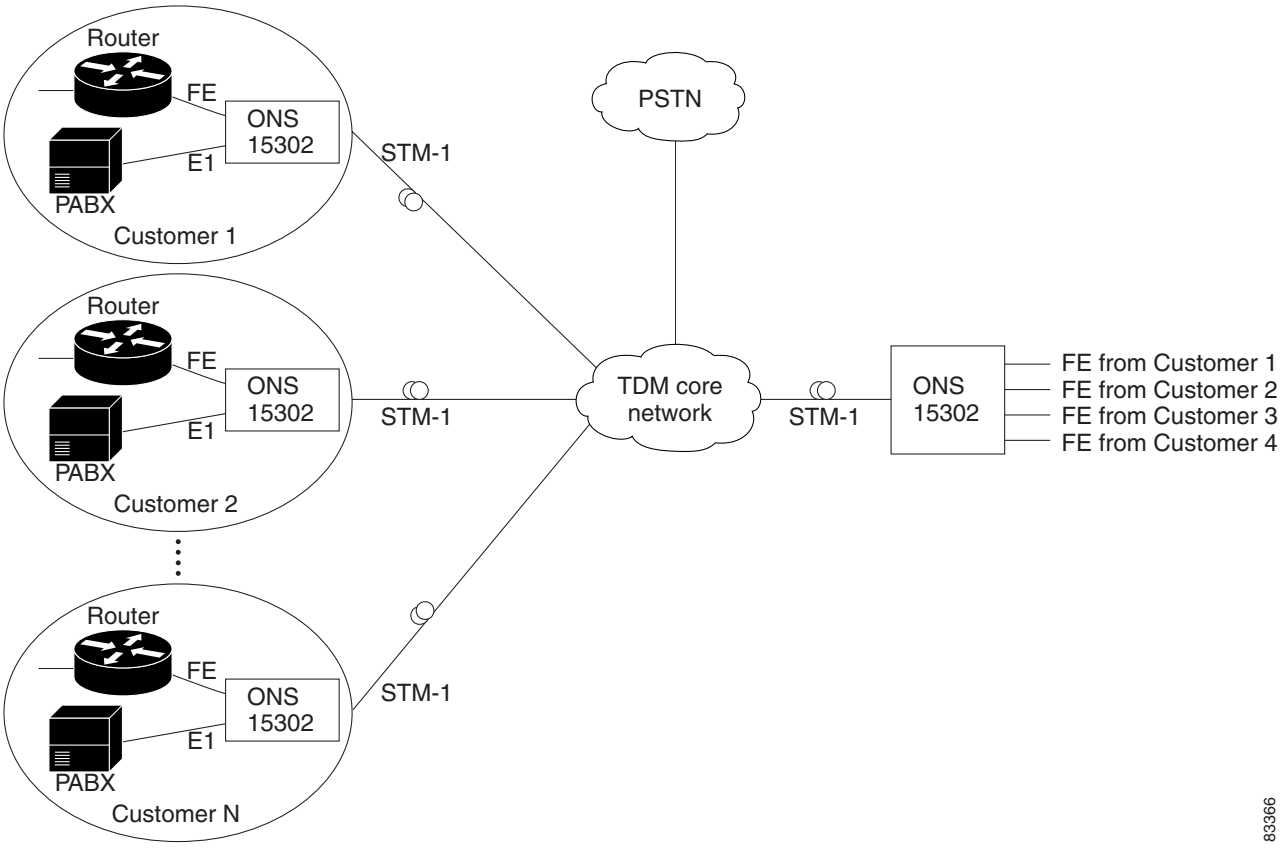
Figure 2-8 Typical System with no Local Grooming in the PoP



2.11.3 Headquarter Office to Branch Office

The ONS 15302 can be connected to four different ONS 15302 units without any additional Ethernet switch Figure 2-9.

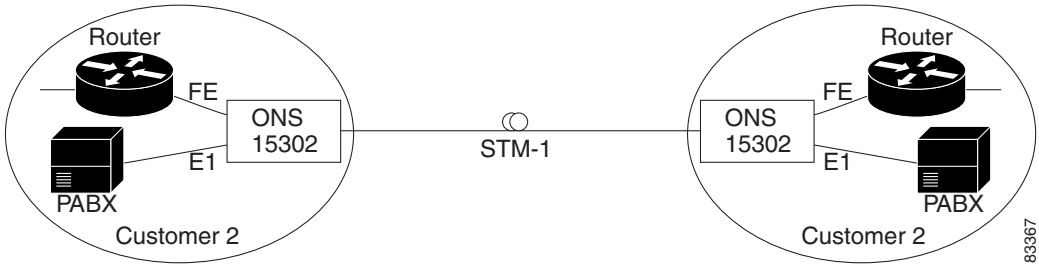
Figure 2-9 Typical System when connected to an ONS 15302



2.11.4 Campus Application

The ONS 15302 can also be connected back to back without any connection to external networks Figure 2-10.

Figure 2-10 Typical Network when used in a Campus Application



2.12 Management

The following main features are supported by the ONS 15302 management system:

- Alarm Handling
- Configuration Management
- Performance Monitoring
- Test Support
- Backup/Restore
- Software Download
- Security

The ONS 15302 management solution is based on an embedded SNMP agent, which can be accessed locally or from a remote management application.

2.12.1 Supported MIBs

In addition to the enterprise specific MIBs, the standard MIBs in the below Table 2-14 are partly supported. Partly supported means that relevant parts of the listed MIBs are implemented and used to manage the associated features in the NEs (Network Elements). Not all parts of the MIBs are used, and there are other features in the NEs not managed through standard MIBs (because covering standard MIBs for the latter features do not exist).

Table 2-14 ONS 15302 MIBs

RFC #	Mnemonic	Title
1213	MIB-II	Management Information Base for Network Management of TCP/IP-based internets: MIB-II
1724	RIP2-MIB	RIP Version 2 MIB Extensions
1471	PPP-LCP-MIB	The Definitions of Managed Objects for the Link Control Protocol of the Point-to-Point Protocol
1473	PPP-IP-NCP-MIB	The Definitions of Managed Objects for the IP Network Control Protocol of the Point-to-Point Protocol
1493	BRIDGE-MIB	Definitions of Managed Objects for Bridges
1757	RMON-MIB	Remote Monitoring (RMON) Management Information Base
1850	OSPF-MIB	OSPF Version 2 Management Information Base
2096	IP-FORWARD-MIB	IP Forwarding Table MIB
2233	IF-MIB	The Interfaces Group MIB using SMIv2
2495	DS1-MIB	Definitions of Managed Objects for the DS1, E1, DS2 and E2 Interface Types
2558	SONET-MIB	Definitions of Managed Objects for the SONET/SDH Interface Type
2665	EtherLike-MIB	Definitions of Managed Objects for the Ethernet-like Interface Types.
2674	P-BRIDGE-MIBQ-BRIDGE-MIB	Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions

Table 2-14 ONS 15302 MIBs (continued)

RFC #	Mnemonic	Title
2932	IPMROUTE-STD-MIB	IPv4 Multicast Routing MIB
2933	IGMP-STD-MIB	Internet Group Management Protocol MIB
2934	PIM-MIB	Protocol Independent Multicast MIB for IPv4

2.12.2 Command Line Interface (ONSCLI)

ONS 15302 supports a serial EIA/TIA 232 interface called ONSCLI. ONSCLI is a line oriented ASCII based management interface, which provides a simple local connection to any VT100 compatible terminal. ONSCLI is protected by a password.

The ONS 15302 also supports the connection of a remote ONSCLI terminal over Telnet/IP.

2.12.2.1 Various ONSCLI Management Access Solutions

ONS 15302 is managed by means of the Optical Network System Command Line Interface (ONSCLI). ONSCLI is an ASCII based VT100 terminal interface. The ONS 15302 can be fully managed by means of the ONSCLI interface.

Figure 2-11 Local Management with ONSCLI

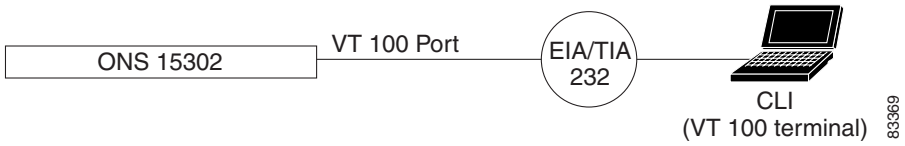
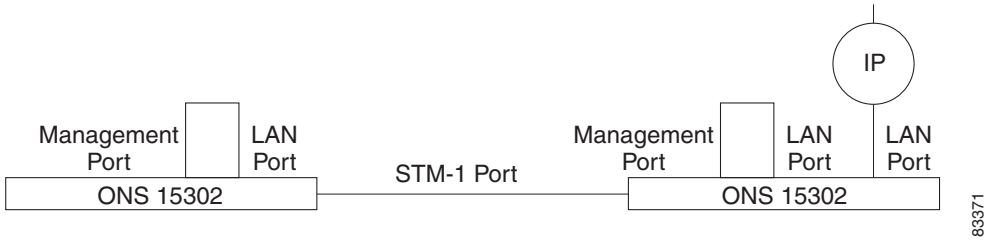


Figure 2-12 Possible Remote Management via In Band Traffic



(Looping remote LAN Port to Management Port. See Inband via one of the LAN Ports, page 2-26 for restrictions).

Note Only one session (local or remote) is allowed at a time.

2.12.3 Management Connectivity

A local Ethernet interface, called the Management Port, is available for connecting to a management DCN. This port is compatible with IEEE 802.3 and supports 10/100BaseT Ethernet for UTP cables.

If an ONS 15302 has no connectivity to the management DCN via the Management Port, mechanisms for transporting management information in the STM-1 DCC channel are provided.

The ONS 15302 management system is based on SNMP and an IP based DCN. However, if an IP based DCN is not available, ONS 15302 provides a mechanism for connecting via IpPPP based DCN.

2.12.3.1 Ways of Connecting to the Management DCN

ONS 15302 can connect to the management DCN in different ways:

Via the dedicated Ethernet Connector (Management Port)

This solution assumes that both ONS 15302s in a pair have local IP- or OSI connectivity.

Via a proprietary HDLC based Protocol in the STM-1 DCC (DCC-R or DCC-M)

This solution assumes that one of the two ONS 15302s in a pair has IP connectivity via the Management Port and that the DCC channel is transparent between the two devices. In this mode, packets received via the Management Port are broadcasted over the DCC HDLC if the MAC address is within the range assigned to Cisco.

Inband via one of the LAN Ports

In this case the Management Port must be physically connected to one of the LAN ports via an external HUB. The management traffic is carried over the Bridge WAN port. If the ONS 15302 device is not managed by the customer itself, the LAN port used for management must belong to a separate VLAN, this means only three ports are left for customer access.

IP Inband

IP inband means that LAN and WAN ports are carrying management traffic together with customer traffic. The configuration is described in 2.14 DCN Configurations Supported, page 2-27.

When using IP inband, the management traffic can be routed or switched (using VLANs). If routed, the routing is carried out in hardware (FFT) if IP routing is enabled. Otherwise, IP forwarding is used, this means software based.

Every ONS 15302 has one and only one IP address allocated to it. ONS 15302 also keeps the IP address of its mate ONS 15302. This simplifies the toggling between two ONS 15302s in a pair. In addition, the flexibility above implies the actual DCN strategy must be decided and configured per device (parameters like DCC enable/disable, IP/HDLC etc.).

All ONS 15302 protocol stack options for implementing the above DCN strategies is illustrated in Figure 2-2.

2.13 DCN Features

The required DCN protocol support is shown in Figure 2-2.

The ONSCLI apply the standards in Table 2-15.

Table 2-15 Protocol Standards

Abbreviation	Standard
Bridge	IEEE 802.1d - Media Access Control Bridges, 1998 Edition Revision (incorporating IEEE 802.1p). The requirements in chapter 0 apply.
MAC / LLC	IEEE 802.x - Information Processing Systems - Local Area Networks
HDLC	ISO 4335 - High level Data Link Control (HDLC) procedures
IP	RFC 791 - Internetwork Protocol
RS-232	EIA/TIA 232
TCP	RFC 793 - Transmission Control Protocol (TCP)
UDP	RFC 768 - User Datagram Protocol (UDP)
PPP	RFC 1661 - The Point to Point Protocol

2.13.1 SDH DCC Channels

Both DCCR (Regenerator Section) and DCCM (Multiplexer Section) channels are supported independently. Note that both channels should not be active on the same port simultaneously, as this will result in looping of the traffic. Activation/deactivation of DCC channels is configurable on a per port basis.The SDH DCC IP/PPP transport mechanism supports only traffic on the DCC-R. The DCC-M is by default turned off, when the IP/PPP/DCC-R mode is enabled.

TELNET

Telnet sessions are possible via all paths of management traffic. Multiple Telnet sessions are not possible.

Security

It is possible to restrict management access to the ONS 15302.

2.14 DCN Configurations Supported

In this context the term DCN (Data Communication Network) is used to denote the network that transports management information between a management station and the NE. This definition of DCN is sometimes referred to as MCN (Management Communication Network). The DCN is usually physically or logically separated from the customer network.

The ONS 15302 management solution is based on SNMP over IP. The main purpose of the DCN implementation is to provide connectivity to the SNMP Agent inside the OSN 15302 via different DCN topologies. The DCN implementation also support transport of management traffic between other Cisco or third party nodes.

Allthough the management application is IP-based, the DCN solution also support OSI-only and mixed IP/OSI-networks at layer 2 and 3. The various options and features related to different DCN topologies are specified throughout this section.

In general, the term OSI in this section is used to denote a CLNP-routed network, ie. it is only used for L3. Higher level OSI-protocols are not considered. At L2 different protocols are supported, including LAP-D. The ONS 15302 OSI-implementation supports CLNP, IS-IS Level 1 and Level 2 and ES-IS.

For the IP In-band L2 topology the management traffic is switched/routed between LAN/WAN ports. When IP-addressing a VLAN IF (id 100000-104000) the management connectivity is obtained at wire-speed along with the user traffic or on a separate WAN-port dedicated for management.

For all other cases, the following applies:

- The DCN traffic is always routed (IP or OSI) between the management interfaces.
- Two different router modes are available for management connectivity.
  - One operates for Numbered mode and the second operates in Un-numbered mode. Both routers are not accessible for DCN purpose simultaneously, and a system mode is introduced to enable desired router.
- Software based DCN routing does not require a routing licence.

Most topologies in the following sections assume standard numbered IP interfaces, ie. every interface connected to the router takes an IP address and a subnet. However, from R2.0 on, a new feature called IP Unnumbered Interfaces is supported. With this feature the device will need only one IP address .

2.14.1 Management Interfaces

The following interfaces may be used to carry management traffic.

2.14.1.1 Management port

The ONS 15302 has a dedicated Ethernet port for management, called the Management Port. This port can be used for local management, e.g. connecting a craft terminal. It can also be used for connecting to a separate external management network. The management port can be turned off to avoid unauthorised local access. The management port cannot be member of a VLAN.

2.14.1.2 LAN ports

The LAN ports are FE Ethernet ports used for connecting customer IP traffic to the OSN 15302. LAN-ports in ONS 15302 are connected to the switch and can be used to carry management traffic.

2.14.1.3 WAN ports

The WAN ports are device internal FE Ethernet ports that can be mapped into one or more virtual containers of an SDH STM-n signal. From a DCN perspective, there are no functional differences between LAN and WAN ports in ONS 15302.

2.14.1.4 DCC channels

The SDH architecture defines data communication channels (DCC) for transport of management traffic in the regenerator section (DCC_R - 192 kbit/s) and in the multiplexer section (DCC_M - 576 kbit/s).

The two SDH-links in ONS 15302 may terminate up to 4 DCC channels (2 DCC_R and/or 4 DCC_M). All DCC channels may be active simultaneously, but this depends on the selected mode. Activation/ deactivation of DCC channels is configurable on a per port basis.

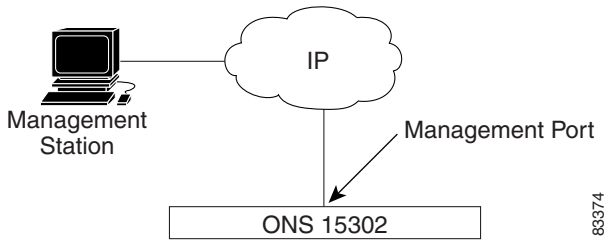
2.14.1.5 Local VT-100 serial port

Also this RS-232 interface is regarded as a management interface, allthough it does not relate to the various DCN topologies described throughout the rest of this section. In ONS15302 full management capability is provided over the ONSCLI.

2.14.2 DCN on Management Port

This configuration is applicable for users connecting an IP based DCN directly to the ONS 15302. For this type of connection, the management port is used, see Figure 2-13.

Figure 2-13 DCN on Management Port

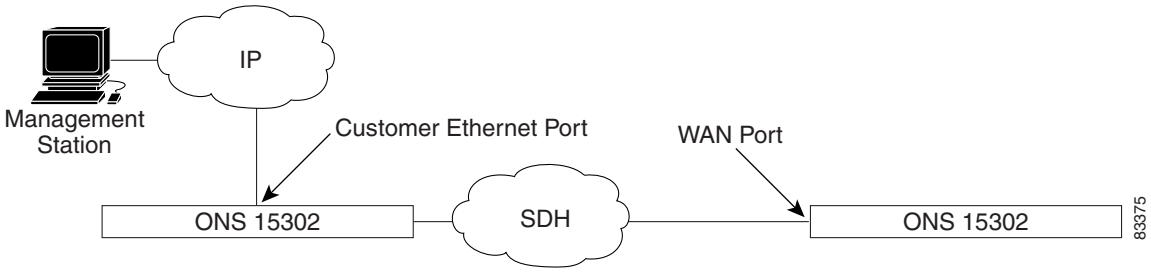


2.14.3 DCN on customer Ethernet Port or WAN Port

This configuration is applicable if the user is connected to one of the customer Ethernet ports, or one of the WAN ports (in band management). IP-Inband means that LAN and WAN ports are carrying management traffic together with customer traffic. This is useful in topologies where (parts of) the SDH-network is owned by a different operator which does not allow a third party to use the DCC capacity. With IP in-band it is possible to build tunnels between islands that have other DCN solutions.

In OSN 15302 all LAN- and WAN-ports are connected to the switch. Any LAN- or WAN-port may be used to carry in-band management traffic, assuming an IP-address is assigned to it, or to the VLAN it belongs to. Between LAN/WAN ports the switching is always at wire-speed. Between LAN/WAN and other management interfaces the traffic is always routed by the CPU. It is possible to split management traffic from user traffic by assigning dedicated LAN/WAN ports to management traffic.

Figure 2-14 DCN on Customer Ethernet Port or WAN Port



2.14.4 PPP/DCC DCN

PPP/DCC means that the management IP-traffic is carried in PPP over the SDH DCC channels according to NSIF-DN-0101-001. The PPP implementation supports RFC1661 (PPP), RFC1662 (PPP in HDLC-like framing) and RFC1332 (IPCP).

Each PPP/DCC channel connects to the IP router individually. Normally this would take one IP subnet per DCC-link, and this is how previous versions of AXX155E would behave.

However, from ONS 15302 R2.0 on a more comprehensive PPP/DCC strategy is supported. This strategy is based on the feature called IP Unnumbered Interfaces, and the rest of this section assumes this option.

The IP Unnumbered concept allows the system to provide IP processing on a serial interface or in general a point-to-point without assigning it an explicit IP address. The IP unnumbered interface borrows the IP address of another interface already configured on the system/router (ie. the Management Port), thereby conserving network and address space, and making the system easier to configure, manage and maintain.

With IP Unnumbered, all nodes connected via PPP-links may be on the same IP subnet. An essential part of the implementation is the DCN ARP Proxy Agent, which makes sure that connectivity between the nodes is obtained without having to provision static routes. The Proxy Agent builds entries for all the DCN IP destinations, and will reply to ARP requests on behalf of them.

IP Unnumbered is regarded as a main mode, and can not be combined with other modes that require numbered interfaces. This implies that this PPP/DCC option can not be combined with IP Inband or OSI.

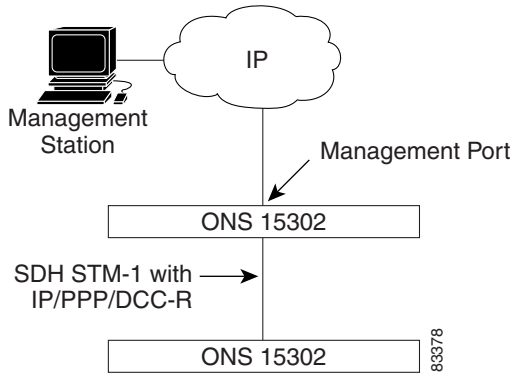
2.14.4.1 Compatibility issues

The ONS 15302 R2.0 is able to provide DCN connectivity with all types of AXXESSIT devices already deployed, including the installed base of ONS 15302 devices with an earlier software revision. Hence, two additional DCN options, are supported; PPP/DCC for numbered interfaces and proprietary IP/DCC communication.

2.14.4.2 PPP/DCC (IP over PPP)

ONS 15302 supports PPP/DCC also on numbered interfaces. This option can not co-exist with the IP unnumbered version of PPP/DCC. However, the numbered variant of PPP/DCC has the advantage that it can be used in combination with all other DCN modes.

Figure 2-15 IP DCN connectivity to a 3rd Party Network Element



Note In the previous ONS 15302 release (R1.0), PPP was only supported over DCC_R. The R2.0 supports both DCC_M and DCC_R.

2.14.4.3 IP/DCC (IP over HDLC)

This configuration is applicable for a user having a subnet of Cisco devices and an IP based DCN connected to the management port of the ONS 15302.

IP/DCC is a non-standard IP broadcast mechanism used for conveying management information on the SDH DCC channels in a network of Cisco devices only. The IP datagrams are encapsulated in HDLC frames before they are sent out on the SDH DCC. Broadcast in this context means that the AXXESSIT devices emulate a shared medium on the SDH DCC channels at the MAC layer. Packets with destination MAC different from the device's MAC are forwarded transparently to the active DCC Tx channel(s).

In order not to saturate the DCC with unnecessary traffic, a filtering mechanism for MAC frames can be enabled. If the filter is enabled, MAC frames received via the management port are broadcasted over DCC only if their destination MAC address is within the range assigned to a Cisco system.

An ONS 15302 configured to broadcast management traffic over the management port and DCC (as described above) can be used to provide IP DCN connectivity to a 3rd party network element via its Management Port, provided than the filter mechanism for MAC frames is disabled.

The IP/DCC option has two special restrictions, imposed by the proprietary pseudo-broadcast mechanism:

- Maximum one DCC per link (M or R)
- The broadcast solution cannot be used in a MSP protection configuration, which involves one, or more radio hops

Figure 2-16 Broadcasting over Management Port and HDLC- DCC

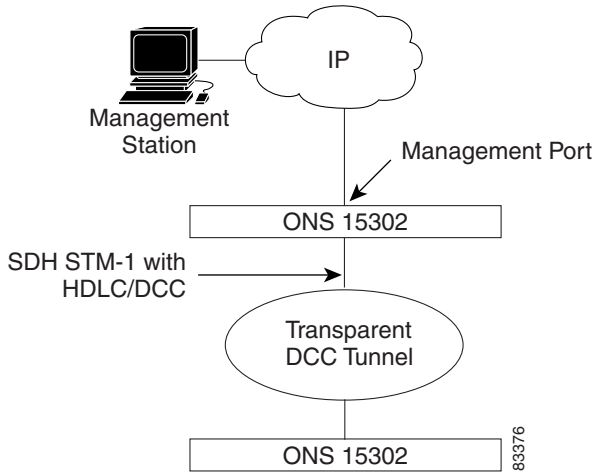
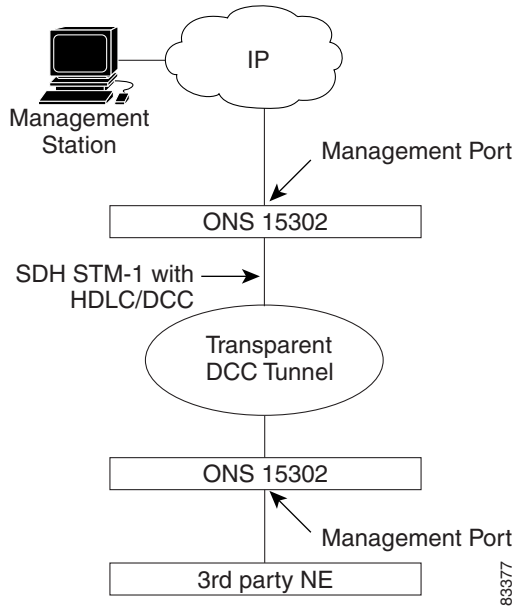


Figure 2-17 IP DCN connectivity to a 3rd Party Network Element



2.14.5 Protection

The two SDH-links in ONS 15302 are protected by means of MSP (1+1 link protection)

For MSP protected links, the DCN behavior depends on the DCN mode:

- If the mode is PPP/DCC (numbered or unnumbered) or IP/DCC (broadcast), the management traffic over DCC follows the user traffic, i.e. traffic is sent over both links (working and protecting), but received only from the active link.
- In all other modes, the two DCC channels will be individual interfaces to the router (CLNP and/or IP), and switch-over will be handled at routing level.

2.14.6 Security

In order to prevent unauthorized access to the SNMP Agent, the following security and traffic control features are supported

2.14.6.1 Management Port On/Off

The Management Port can be turned on and off, thereby preventing unauthorized local access to the management network.

2.14.6.2 SNMPv1 Community

The SNMPv1 packet contains a password (called community string) that must be known by both the manager and the agent. Different community names can be defined for read and read/write access. The community string is, however, transferred un-encrypted.

2.14.6.3 SNMP Manager Identity

This is an enhancement of the SNMPv1 Community feature. Here, the SNMP manager's IP address must be configured in the device subject to management. Only legal combinations of community name and source IP address in SNMP requests are accepted.

2.14.6.4 SNMP Read/Write control

The access rights of the registered management systems can be set to read/write or read only.

2.14.6.5 VLAN (802.1Q)

This security mechanism relates to the IP in-band option only: By configuring a separate VLAN for the management traffic and assigning an IP address to it, the end-users will not be able to access the device or generate traffic into the management VLAN.

2.14.6.6 ONSCLI Access Control

ONSCLI is protected by user name and password. OSNCLI is by default a superuser and can block all remote SNMP users by changing the access rights and passwords. Remote CLI access via Telnet must in addition have a Telnet password.

2.15 ONS 15302 Management

The description of the ONS 15302 management system refers to manageable objects as listed in Table 2-16.

Table 2-16 Managed Object

Object Name	#	Description
Device	1	The ONS 15302 unit itself
Bridge Port	5	The four LAN Ports plus the WAN Port mapped into the STM-1
Tributary Port	4	The 2048 kHz tributary interfaces
Aggregate Port	1(2)	The STM-1 aggregate. Optical or Electrical. Dual ports for MSP (1+1) or single fiber operation.
Auxiliary Port	4	The general purpose auxiliary interfaces
Bridge	1	Common Bridge functionality, like VLAN and Spanning Tree

2.16 Fault Management

The following subsections describes Cisco ONS 15302 fault management.

2.16.1 Alarm Handling

The alarms are related to a managed object as defined in Table 2-16.

The ONS 15302 keeps a record of current and historical alarm events.

The list of current alarms contains the following parameters for each alarm:

- Timestamp
- Alarm Object (for example. Tributary Port 1, Aggregate Port)
- Alarm Identifier
- KLM value if applicable
- Port Affected
- Alarm Description

Port alarms are suppressed if the port itself is disabled. In order to avoid alarm flooding, alarms at different levels are correlated. Lower order alarms are suppressed if a more important alarm at a higher level is active.

In addition to the alarms, the ONS 15302 may generate a number of events. The events are not stored in the current alarm list, but they are appended to the historical alarm list in the same way as the alarms. The historical alarm list contains the same parameters per alarm as the current alarm list, and in addition the following parameter:

- Event Type (RAISED, CLEARED or EVENT)

Both the alarms and the events generate SNMP traps. The traps can be sent to a number of management stations. It is possible to turn SNMP trap sending on or off on a per manager basis. This is the only alarm filtering mechanism provided by the ONS 15302.

Note The bridge port LOSLA alarm is handled slightly different from the rest of the alarms. If a bridge port is unconnected or if it is forced down by the operator, it will cause a LOSLA event, which goes into the historical alarm list like other alarms. These alarms will, however, not cause a red LED to be lit, and they will not be stored in the current alarm list like the other alarms.

Note The LPPLM alarm is only supported for the VC-12 containers used by the tributary ports. It is not supported for the VC-12(s) constituting the WAN port.

Note The MSDEG and LPDEG alarms are based on the near end BER counters over 20 seconds intervals.

Table 2-17 Criterions for Turning Alarms On and Off

Alarm	ON	OFF
MSDEG	> 10 exp –7	< 10 exp –8
LPDEG	> 10 exp –6	< 10 exp –7

2.16.2 Alarm Severity

The Alarm Severity is configurable per alarm object. Default values are assigned automatically as shown in Table 2-19.

2.16.2.1 Alarm Definition

The list below contains all the alarms that are defined for the ONS 15302. For some of the Alarm IDs, the direction (RX or TX) is an integral part of the name. This terminology is used for the direction:

- RX: Downlink (from network to customer)
- TX: Uplink (from customer to network)

Table 2-18 ONS 15302 Alarms

Alarm		Description	Default Severity
ONS15302	HWFAIL	Hardware failure.	Critical
	LOSSY	Loss of external sync.	Minor
	SyncHoldOver	Loss of configured synchronisation source	Major
	TEMP	Too high temperature in the unit i.e. above +45° Celsius	Critical
	FAN	FAN failure.	Major
ALARM	AUX	Dry contact alarm.	Warning

Table 2-18 ONS 15302 Alarms (continued)

Alarm		Description	Default Severity
SDH (STM-1)	LOS	Loss of STM-1 signal.	Critical
	LOF	Loss of frame alignment on the STM-1 signal.	Critical
	TD	Transmit Degrade on laser (Not applicable for electrical interface).	Minor
	TF	Transmit fail on laser (Not applicable for electrical interface).	Critical
RS	TIM	Trace Identifier mismatch (J0-byte).	Critical
	CSF	Communication subsystem failure, DCCR communication failure. (Just applicable for OSI-routing)	Minor
	EXC	Excessive error defect. BER > E-5	Major
	DEG	Degraded signal defect. BER > E-6 - E-9 (default E-6)	Minor
MS	AIS	Alarm Indication signal.	Minor
	EXC	Excessive error defect.	Major
	DEG	Degraded signal defect.	Minor
	RDI	Remote Defect indication.	Minor
	CSF	Communication subsystem failure, DCCM communication failure. (Just applicable for OSI-routing)	Minor
MSP	MSP	Problem with MSP (1+1 protection) signalling with another NE across K1/K2 bytes.	Minor
AU4	LOP	Loss of pointer	Critical
	AIS	Alarm indication signal	Minor
VC4	LOM	Loss of multi-frame alignment	Critical
	UNEQ	Unequipped.	Minor
	TIM	Trace identifier mismatch (J1-byte).	Critical
	PLM	Payload mismatch.	Critical
	EXC	Excessive error defect. BER > E-5	Major
	DEG	Degraded signal defect. BER > E-6 - E-9 (default E-6)	Minor
	RDI	Remote defect indication.	Minor
TU12	AIS	Alarm indication signal.	Minor
	LOP	Loss of pointer.	Critical

Table 2-18 ONS 15302 Alarms (continued)

Alarm		Description	Default Severity
VC12	UNEQ	Unequipped.	Minor
	TIM	Trace identifier mismatch (J2-byte).	Critical
	PLM	Payload mismatch.	Critical
	EXC	Excessive error defect. BER > E-5	Major
	DEG	Degraded signal defect. BER > E-6 - E-9 (default E-6)	Minor
	RDI	Remote defect indication.	Minor
Tributary (E1)	LOSTX	Loss of signal.	Critical
	AISRX	Alarm indication signal network side.	Warning
	LFARX	Loss of frame alignment customer side.	Major
	LFATX	Loss of frame alignment customer side.	Major
	UNASS	Tributary (E1) activated but not mapped to an available VC-12.	Critical
Ethernet WAN-port Proprietary	WANDELAY	Differential VC-12 delay for the WAN port is greater than +/-6,5ms	Critical
	seqFail	Seq wrong channel number p2p, i.e. wrong order of VC-12 allocated to a WAN-port....or one or more VC-12 containers not carrying Ethernet traffic terminated on the WAN-port.	Critical

2.16.3 Alarm Definitions

The different alarms together with their relations to the managed objects are defined in Chapter 9, "Managed Objects,"

2.16.4 Alarm Parameters

Table 2-19 defines the parameters associated with an alarm.

Table 2-19 Alarm Parameters

Parameter	Description
Timestamp	Date/Time of alarm event
Alarm Object	Object subject to alarm situation. Should contain both object type (class) and identification (instance).
Alarm Identifier	Short form alarm description, for example LOS
Alarm Description	Alarm description, for example Loss of signal

Table 2-19 Alarm Parameters (continued)

Parameter	Description
Alarm Severity	According to ITU-T X.733
Event Type	Raised, Cleared or Event. Applicable for alarm log only. Event means alarm with no duration.

The Alarm Severity is configurable per alarm object. Default values are assigned automatically.

2.16.5 Alarm Suppression

Alarms are suppressed if the object subject to alarm is disabled. It is possible to inhibit alarm reporting for a specific managed object. It is possible to inhibit all alarms from one ONS 15302. All SDH and PDH objects have two configurable persistency filters:

- Persistency filter alarm on: alarms must have been on for a certain amount of time before being reported.
- Persistency filter alarm off: alarms must have been off for a certain amount of time before being cleared.

In addition, the STM-1 interfaces follow the alarm suppression, (Table 2-20).

Table 2-20 Alarm Suppression

Object-Id	Alarm-Id	Suppress the following alarms
SDH	LOS	yes
	LOF	yes
RS	TIM	yes
	CSF	no
	EXC	no
	DEG	no
MS	AIS	yes
	CSF	no
	RDI	no
	EXC	no
	DEG	no
MSP	MSP	no
AU4	LOP	yes
	AIS	yes

Table 2-20 Alarm Suppression (continued)

Object-Id	Alarm-Id	Suppress the following alarms
VC-4	UNEQ	yes
	TIM	yes
	EXC	no
	DEG	no
	RDI	no
	PLM	yes
	LOM	yes
TU12	LOP	yes
	AIS	yes
VC-12	UNEQ	yes
	TIM	yes
	EXC	no
	DEG	no
	RDI	no
	PLM	yes
Tributary	AISRX	yes
	LFARX	yes

2.16.5.1 Alarm Suppression for Tributary Tx-Alarms

Table 2-21 Alarm Suppression for Tributary Tx-Alarms

Object-Id	Alarm-Id	Suppress the following alarms
Tributary	LOSTX	yes
LFATX	LFATX	yes

2.16.5.2 VC-4 Alarm Suppression for EXC/DEG

Table 2-22 VC-4 Alarm Suppression for EXC/DEG

Object-Id	Alarm-Id	Suppress the following alarms
VC-4	EXC	yes
	DEG	no

2.16.5.3 RS Alarm Suppression for EXC/DEG

Table 2-23 RS Alarm Suppression for EXC/DEG

Object-Id	Alarm-Id	Suppress the following alarms
RS	EXC	yes
	DEG	no

2.16.5.4 MS Alarm Suppression for EXC/DEG

Table 2-24 MS Alarm Suppression for EXC/DEG

Object-Id	Alarm-Id	Suppress the following alarms
MS	EXC	yes
	DEG	no

2.16.5.5 VC-12 Alarm Suppression for EXC/DEG

Table 2-25 VC-12 Alarm Suppression for EXC/DEG

Object-Id	Alarm-Id	Suppress the following alarms
VC-12	EXC	yes
	DEG	no

2.16.6 Alarm Collection

It is possible to view the alarms of all ONS 15302 devices present in the network, for example currently reachable from the management system. The ONS 15302 device stores a list of all current alarms and a log of alarm events. The size of the log of alarm events is 1000 entries.

2.16.7 Alarm Classification

It is possible for the operator to change the assignment of alarm severity for each pair of Object Type Alarm ID.

The possible severity levels are:

- WARNING
- MINOR
- MAJOR
- CRITICAL

2.16.8 Alarm Indication

The Customer LED on indicates that one or more Tributary alarms are on.

The Operator LED on indicates any alarm on, other than AUX alarms and Tributary alarms.

It is possible to define an alarm severity threshold for each LED defining which alarm severity shall turn on the corresponding LED.

2.17 Configuration Management

The following subsections describes Cisco ONS 15302 configuration management.

Backup and Restoration of Configuration Data

It is possible to back up the configuration data of an ONS 15302 device. It is possible to reload the configuration from the back up. The back up media must be a central repository.

Note This feature is only possible from a GUI based Element Manager.

Software Download (Remote Access)

It is possible to download a new software version to the ONS 15302 device.

The download process does not influence traffic processing of TDM traffic (E1s) unless the update/upgrade includes FPGA changes. Ethernet traffic will always influence the Ethernet traffic running via LAN/WAN - ports and remote management connectivity will not be maintained during the reset period. The new software is used when booting after the next restart. The previous software version is saved in the device. If booting with the new software fails, the ONS 15302 reboots with the old software, and an alarm is raised.

The software can be downloaded locally via the management interface or remotely via the DCC channels.

Device Reset

It is possible to reset (reboot) the device with or without resetting the current configuration. Reboot have minimal impact on traffic processing. The following situations will affect Ethernet/IP traffic and require a Device reset to become operative:

- After configuration and changes of OSI(CLNP) related parameters (Ethernet/IP traffic affecting)
- When decreasing/increasing entries in tunable tables e.g. maxARP, maxIP-forwarding, maxVLAN's, maxDHCP, maxBridge, etc.
- Software upgrade without FPGA fix (Ethernet/IP traffic affecting)
- Software upgrade with FPGA fix (All traffic affected)

Device Replacement

It is possible to replace an ONS 15302 device with a new one with an identical physical configuration.

No manual configuration on the device is required. The ONS 15302 is assigned one IP address automatically from a BootP server. In addition, the BootP reply contains a reference to a configuration file, and the IP address of the FTP/TFTP server from where this file can be downloaded. Once the configuration has been received, the ONS 15302 must be rebooted.

Managed Object Attributes

All attributes defined in the chapter Chapter 9, "Managed Objects," are available for read or read/write access by the management applications specified in "Command Line Interface (ONSCLI)" section on page 25.

2.18 Performance Monitoring

The performance monitoring functions specified inTable 2-26 is available in ONSCLI.

2.18.1 Aggregate Port

Table 2-26 defines the mapping between the dialogue parameters and MIB variables for the Aggregate Port Statistics submenu.

Table 2-26 Aggregate Port Statistics Parameter Mappings

Parameter	MIB variable(s)	Comment
Aggregate Port		Choice between A or B
Path/Section		Choice between RS, MS, VC-4, or VC-12
VC-12 (KLM)	axx155TribPortMapPort ifStack LowerLayer (rfc1573) axx155SdhVc12MoTable axx155WanVc12Klm	Only valid if Path/Section choice is VC-12.ifIndex of tributary.ifIndex of VC-12 connected to tributary.K.L.M value of VC-12 connected to tributary.K.L.M value of VC-12s connected to WAN.
Date/Time	rndManagedTime rndManagedDate	
Current Interval Time Elapsed	sonetMediumTimeElapsed (rfc2558)	
Current ES	sonetSectionCurrentESs (rfc2558)sonetLineCurrentESs (rfc2558)sonetPathCurrentESs (rfc2558)sonetVTCurrentESs (rfc2558)	Regenerator Section.Multiplex Section. VC-4. VC-12.
Current Far End ES	sonetFarEndLineCurrentESs(rfc2558) sonetFarEndPathCurrentESs(rfc2558) sonetFarEndVTCurrentESs(rfc2558)	Multiplex Section. VC-4. VC-12.
Current SES	sonetSectionCurrentSESs (rfc2558)sonetLineCurrentSESs (rfc2558)sonetPathCurrentSESs (rfc2558)sonetVTCurrentSESs (rfc2558)	Regenerator Section. Multiplex Section. VC-4. VC-12.
Current Far End SES	sonetFarEndLineCurrentSESs(rfc2558) sonetFarEndPathCurrentSESs(rfc2558) sonetFarEndVTCurrentSESs(rfc2558)	Multiplex Section.VC-4.VC-12.
Current BBE	sonetSectionCurrentBBEs sonetLineCurrentBBEs sonetPathCurrentBBEs sonetVTCurrentBBEs	Regenerator Section. Multiplex Section. VC-4. VC-12.
Current Far End BBE	sonetFarEndLineCurrentBBEs sonetFarEndPathCurrentBBEs sonetFarEndVTCurrentBBEs	Multiplex Section. VC-4. VC-12.

Table 2-26 Aggregate Port Statistics Parameter Mappings (continued)

Parameter	MIB variable(s)	Comment
Current UAS	sonetSectionCurrentUASs sonetLineCurrentUASs (rfc2558)sonetPathCurrentUASs (rfc2558)sonetVTCurrentUASs (rfc2558)	Regenerator Section. Multiplex Section. VC-4. VC-12.
Current Far End UAS	sonetFarEndLineCurrentUASs(rfc2558)s onetFarEndPathCurrentUASs(rfc2558)so netFarEndVTCurrentUASs(rfc2558)	Multiplex Section. VC-4. VC-12.
Index	sonetLineIntervalNumber (rfc2558) sonetPathIntervalNumber (rfc2558) sonetVTIntervalNumber (rfc2558)	Multiplex Section. VC-4. VC-12.
Timestamp	rndManagedTime rndManagedDate sonetMediumTimeElapsed (rfc2558) sonetLIneIntervalNumber (rfc2558) sonetPathIntervalNumber ((rfc2558) sonetVTIntervalNumber ((rfc2558)	Timestamp must be calculated from these values and index. Multiplex Section. VC-4. VC-12.
ES	sonetSectionIntervalESs (rfc2558) sonetLineIntervalESs (rfc2558) sonetPathIntervalESs (rfc2558) sonetVTIntervalESs (rfc2558)	Regenerator Section. Multiplex Section. VC-4. VC-12.
Far End ES	sonetFarEndLineIntervalESs(rfc2558) sonetFarEndPathIntervalESs(rfc2558) sonetFarEndVTIntervalESs(rfc2558)	Multiplex Section. VC-4. VC-12.
SES	sonetSectionIntervalSESs (rfc2558) sonetLineIntervalSESs (rfc2558) sonetPathIntervalSESs (rfc2558) sonetVTIntervalSESs (rfc2558)	Regenerator Section. Multiplex Section. VC-4. VC-12.
Far End SES	sonetFarEndLineIntervalSESs(rfc2558) sonetFarEndPathIntervalSESs(rfc2558) sonetFarEndVTIntervalSESs(rfc2558)	Multiplex Section. VC-4. VC-12.
BBE	sonetSectionIntervalBBEssonetLineInterv alBBEs sonetPathIntervalBBEssonetVTIntervalB BEs	Regenerator Section. Multiplex Section. VC-4. VC-12.
Far End BBE	sonetFarEndLineIntervalBBEs sonetFarEndPathIntervalBBEs sonetFarEndVTIntervalBBEs	Multiplex Section. VC-4. VC-12.
UAS	sonetSectionIntervalUASssonetLineInterv alUASs (rfc2558) sonetPathIntervalUASs (rfc2558) sonetVTIntervalUASs (rfc2558)	Regenerator Section. Multiplex Section. VC-4. VC-12.
Far End UAS	sonetFarEndLineIntervalUASs(rfc2558) sonetFarEndPathIntervalUASs(rfc2558) sonetFarEndVTIntervalUASs(rfc2558)	Multiplex Section. VC-4. VC-12.

2.18.2 Bridge Port

Performance counters for the Bridge ports (including the WAN port) are available for the manager via the following variables in the RMON MIB:

- etherStatsDropEvents
- etherStatsOctets
- etherStatsPkts
- etherStatsBroadcastPkts
- etherStatsMulticastPkts
- etherStatsCRCAlignErrors
- etherStatsUndersizePkts
- etherStatsOversizePkts
- etherStatsFragments
- etherStatsJabbers
- etherStatsCollisions
- etherStatsPkts64Octets
- etherStatsPkts65to127Octets
- etherStatsPkts128to255Octets
- etherStatsPkts256to511Octets
- etherStatsPkts512to1023Octets
- etherStatsPkts1024to1518Octets

As opposed to the Aggregate port counters, the Bridge port counters must be started and stopped by the operator.

ONS 15302 keeps no history records for the Bridge port counters.

2.18.2.1 Ping

An IP ping service is available in the ONS 15302.

This service is available in all management solutions. In ONSCLI this option can be found under the Service menu options. With this service, ping series with different parameters to a number of different devices can be started. The result of each sequence is displayed in the Ping Table. The ping session supports different packet sizes as well as number of pings generated for reply.

2.19 Software Download (Local Access)

It is possible to load a new software version by means of a PC directly attached to the ONSCLI Port. This service requires local operator presence at the ONS 15302. Refer to Chapter 5, “Troubleshooting” for more information.

The file is loaded by means of the X modem protocol, and the transfer rate is 15.200 kbit/s.

Note Booting the system triggers local software download. Hence, the traffic is lost during the loading.

Table 2-27 S7oftware Download Parameters

Parameters	Description
File Name	Software File to be downloaded

2.20 Security

The management access to the ONS 15302 is controlled by parameters in a community table. This table can only be modified by users with Super access rights. The parameters in the community table are only visible for Super users.

For each defined user, the following parameters must be provided:

- IP address
- Community string
- Access Right (READ-ONLY, READ-WRITE, SUPER)
- Traps (Enable or Disable)

One management station (IP address) may have several users with different access rights. These users are identified by means of the community string.

The ONSCLI access is controlled by means of a password, one for the local access and one for the Telnet access. A management station Super user can modify the ONSCLI password.

The ONSCLI user has Super access rights.

2.21 Management Logs

This subsection summarizes the various logs used for alarms, errors and statistics as visualized in Figure 2-18 Management logs.

In addition to the logs described in Table 2-28, the system provides logs for troubleshooting, containing detailed debug information. These logs are not available for normal users, and they are not specified in this document.

Figure 2-18 Management Logs

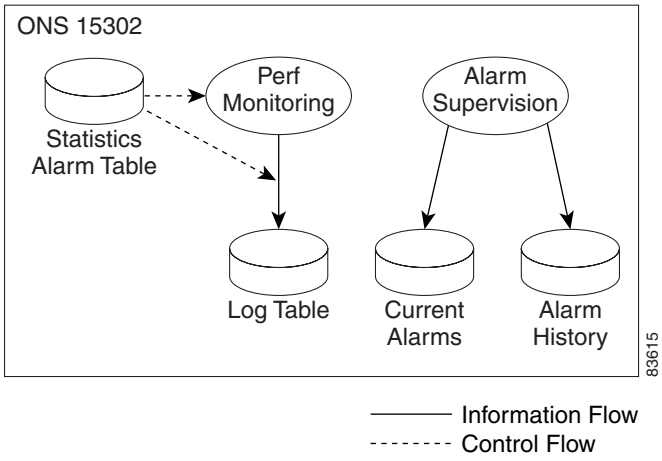


Table 2-28 Management Logs

Name	Location	Description
Statistics Alarm Table	ONS 15302	Controls the monitoring of Bridge and LAN port performance. It contains definition of threshold alarms and also decides if performance alarms shall be logged locally in Log Table, or sent as trap to the manager or both. This table corresponds to the RMON alarm table.
Log Table	ONS 15302	This table contains the logged performance alarms controlled by the Statistics Alarm Table. This table corresponds to the RMON log table.
Current Alarms	ONS 15302	This table contains all alarms currently on.
Alarm History	ONS 15302	This table contains a log of all events, including alarm events. The latest 1000 events are stored.

Pre-Installation Procedures

This chapter provides pre-installation procedures for the Cisco ONS 15302. Chapter topics include shipment verification, site preparation, and equipment unpacking.

3.1 Shipment Verification

When you receive ONS 15302 system equipment at the installation site, immediately verify that the shipment is correct.

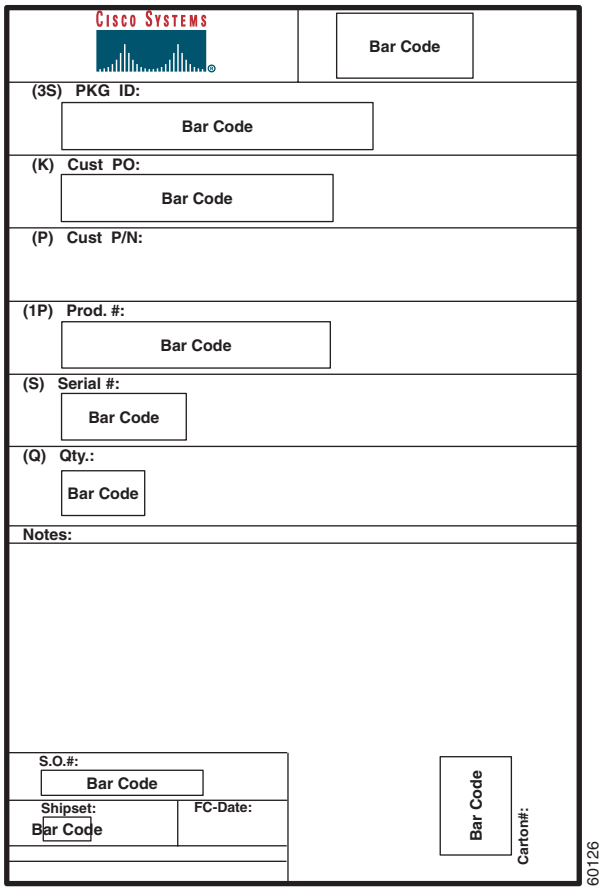
Note Cisco does not recommend shipping equipment that is mounted in racks. To ship equipment from one site to another, pack the equipment in the original box.

Note If you store the ONS 15302 before installing it, keep the ONS 15302 system equipment in the original shipping containers. The storage period should not exceed 12 months. Store the packed equipment indoors in a well-ventilated and static-safe environment.

3.1.1 ONS 15302 Shipping Container Label

The ONS 15302 shipping container label provides specific information about the shipped item. The label displays information in alphanumeric bar code format. Figure 3-1 shows a sample of a shipping container label.

Figure 3-1 Example of a Shipping Container Label



3.1.2 Preliminary Inventory Check

Compare the packing list information with the alphanumeric information provided on the shipping labels. The packing list and shipping labels should contain the same information. If there are any discrepancies between the shipping label information and the packing list information, call the Cisco Technical Assistance Center (TAC). The phone numbers from TAC are available in the www.cisco.com/warp/public/687/Directory/DirTAC.shtml please have a look into this side for your country contact.

3.1.3 Reporting Damage

To report damage to shipped articles, contact the Cisco Technical Assistance Center (TAC) (www.cisco.com/warp/public/687/Directory/DirTAC.shtml) to open a Return Material Authorization and Fault Symptom Report (RMA).

3.2 Site Preparation

Verify that the installation site meets the following criteria:

1. The site conforms to all environmental specifications in Chapter 2, "Product Overview".
2. The floor or mounting area where you will install the equipment can support the equipment.

Note The following tables are based on typical ONS 15302 system configurations. Floor loading, power consumption, heat dissipation, and clearances may vary in specific customer configurations.

3. The installation site meets the power supply requirements of the ONS 15302 equipment. Table 3-1 lists these requirements.

Table 3-1 Power Supply Requirements by ONS 15302 Equipment Type

Equipment Type	Power Supply Requirements
230 V 50Hz AC	230 V AC +/– 10%
–48 V DC	–36 to –72 V DC

4. The installation site meets the power consumption requirements of the ONS 15302 equipment. Table 3-2 lists these requirements.

Table 3-2 Power Consumption Requirements by ONS 15302 Equipment Type

Equipment Type	Power Consumption Requirements
ONS 15302	40 W

5. The installation site meets the circuit breakers requirements of the ONS 15302 equipment. Table 3-3 lists these requirements.

Table 3-3 Circuit Breakers Requirements by ONS 15302 Equipment Type

Equipment Type	Circuit Breakers Requirements
ONS 15302	1.5 A

6. Minimum recommended clearance is provided for accessing bays from the front and back, opening front covers, and clearing the top of the racks. Table 3-4 provides clearance requirements.

Table 3-4 Recommended Access Clearance

Item	Recommended Clearance
Bay access needed for maintenance	Front access only, 500 mm (19.7 in.)
Back clearance to bays (if necessary)	500 mm (19.7 in.)

3.3 Unpacking

Use the following considerations when unpacking and storing ONS 15302 equipment:

- Leave equipment packed until it is needed for immediate installation.
- Store packed equipment in the temperature and environmental conditions described in the Chapter 2, "Product Overview,".
- After unpacking the equipment, save and store the packaging material in case the equipment must be returned.
- If the packaging is damaged and possible equipment damage is present, preserve as much of the packaging as possible to allow Customer Service and the shipper to analyze the damage. To report damage to shipped articles, contact the Cisco Technical Assistance Center (TAC) to open an RMA, Chapter 3, "Reporting Damage".

The following procedures contain specific instructions for unpacking ONS 15302 system equipment.

Unpack the ONS 15302

Caution When opening the shipping container, use caution to avoid damaging the contents.

Caution Static electricity can damage electro-optical equipment. While unpacking and handling optical and electrical modules, wear a grounding wrist strap to discharge the static buildup. Before unpacking and installing modules or making system interconnections, connect the grounding wrist strap. The grounding wrist strap is designed to prevent equipment damage caused by static electricity.

Step 1 Open the top of the cardboard shipping container.

Step 2 Remove the ONS 15302 accessory kit and documentation CD out of the shipping container.

Step 3 Take the ONS 15302 out of the shipping container.

Step 4 Take the ONS 15302 out the plastic protective bag.

The ONS 15302 shipping container should contain the following items:

- One ONS 15302 configured as ordered
- One Accessory kit (15302-SHIPKIT=, Cisco Part number 74-3173-01), which includes brackets and screws for 19" and 23" rack, disposable ESD wrist straps, one –48 VDC power and ground connector, one 230 VAC power supply cable, one ONSCLI cable, one blade terminal with screw and blade jack, a registration and warranty card, and a documentation CD.

Installation

This chapter provides instructions for installing Cisco ONS 15302 system.

Note The instructions in this section primarily address the installation of the ONS 15302, and modules supplied by Cisco Systems. When installing racks, electrical wiring, raceways, and other equipment not covered in this manual, you should follow all local, state, federal, or international (if applicable) codes and regulations.

Caution Static electricity can damage electronic equipment. While unpacking and handling electronic modules, wear a grounding wrist strap to discharge the static buildup. Grounding wrist straps are designed to prevent equipment damage caused by static electricity. Before making the necessary interconnections, connect the grounding wrist strap.

4.1 Installation Overview

You should be thoroughly familiar with the instructions in this manual before starting any work. Use the following instructions when installing the ONS 15302.

Step 1 Read and observe all safety cautions and warnings in Chapter 1, "Safety Summary."

Step 2 Before inspecting the ONS 15302, first verify the ONS 15302 equipment according to the procedures in Chapter 3, "Pre-Installation Procedures." If there is a problem with the equipment, contact the Cisco TAC. The phone numbers from TAC are available in the www.cisco.com/warp/public/687/Directory/DirTAC.shtml. Please refer to this website for your country contact.

Step 3 If you do not install the equipment immediately, store as specified in Chapter 3, "Pre-Installation Procedures."

Step 4 Unpack equipment only after preparing the site as described in Chapter 3, "Pre-Installation Procedures."

Step 5 When installing equipment at a site, follow the procedures in this chapter in the order presented.

Step 6 Make connections using the information in Chapter 6, "Technical Specifications."

4.2 Installation Planning

Based on the configuration to be installed, determine the size, number, and location of racks, as well as the ONS 15302 installation requirements. The following are unit dimensions to take into consideration when installing the ONS 15302. The ONS 15302 can be installed in 485 mm (19-in.) equipment racks, and can be adapted for 600 mm ETSI (23.6-in.) racks. The racks must be accessible from the front and rear for equipment installation.

Note You need 500 mm (19.7-in.) space of rear access for installation of the equipment.

Use the following considerations when planning how to install in the rack a ONS 15302.

- Install the lowest unit in a rack first.
- Wire size and dimension requirements are based on cable length and local engineering standards and practices.
- Route the power cable from the power distribution panel (PDP) to the ONS 15302, along the edge of the equipment rack.
- Route the grounding cable from the station ground to the ONS 15302, proceeding down along the edge of the equipment rack.
- Route the electrical cables from the ONS 15302 along the edge of the rack to the overhead cable transport tray.
- Route the optical cables from the ONS 15302 along the edge of the rack to the overhead cable transport tray.

4.2.1 Required Items

In addition to a standard installers tool kit, the following items are also required:

- Phillips screwdriver (PH3) to attach the ONS 15302 to the rack, and Phillips screwdriver (PH1) to attach the brackets to the ONS 15302
- 2.5-mm Allen key (to attach the external grounding)
- 4 mounting screws, M6 (#12-24 x 3/4 pan head phillips) and nuts
- Power cable (from fuse to power connector), #18 AWG (0.75 mm²) up to #16 AWG (1.5 mm²) with four rigid wire
- Yellow green flexible ground cable, #16 AWG (1.25 mm²) up to #14 AWG (2.50 mm²) (for the external grounding)
- Cletop cleaning cassette (type A for SC connectors)
- Video fiber connector inspection instrument
- Caps for optical connectors
- Plugs for optical adapters
- Tie wraps

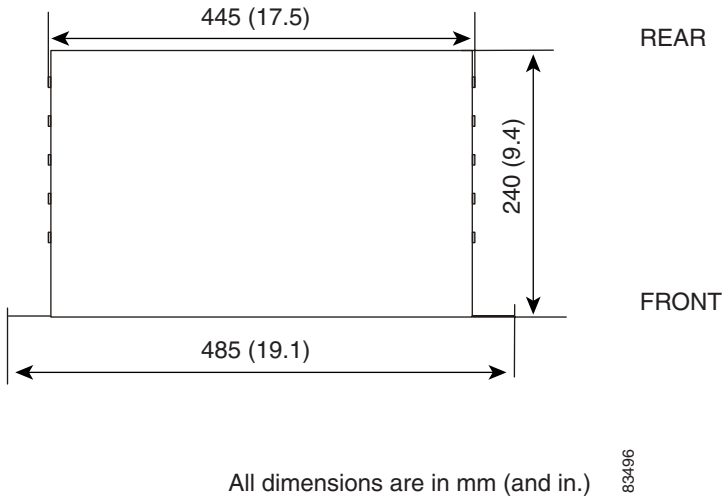
4.2.2 Installation Guidelines

When installing ONS 15302 equipment into a rack, follow these guidelines:

- Consider the effect of additional electronic equipment and its generated heat on the ONS 15302 system equipment.
- Make sure the equipment rack is properly bolted to the ground, and if required, to the ceiling. Ensure that the weight of the equipment does not make the rack unstable.
- When mounting the equipment between two posts or rails, ensure that the minimum clearance between the sides is 485 mm (19 in.).
- Maintain a minimum clearance of 500 mm (19.7 in.) in front of the equipment and 500 mm (19.7 in.) at the back of the equipment.

Figure 4-1 shows the outer dimensions of the ONS 15302 system equipment.

Figure 4-1 Outer Dimensions of the ONS 15302 System

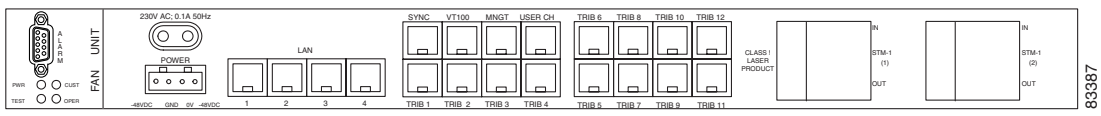


4.2.3 Install Ground to 48 V

It is vital that the ONS 15302 is properly grounded. The ONS 15302 is grounded via the 48V power connector to the rack ground, refer to "4.4.2 Install the ONS 15302 –48 VDC Power".

The location of the power connector on the ONS 15302 is shown in Figure 4-2.

Figure 4-2 ONS 15302 Faceplate (Connector Array)



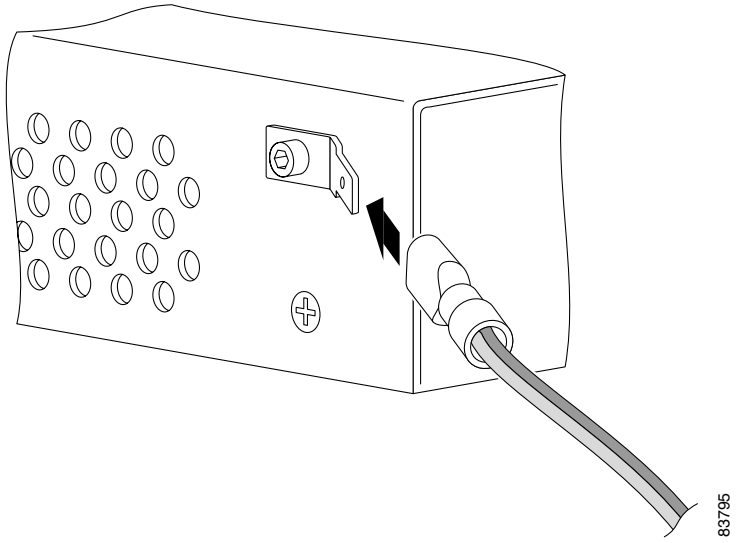
4.2.4 Install External Ground for 230 V Supply to the ONS 15302

Note This ground connection is only used when the system is powered with 230 VAC and the system is not installed in a rack.

The ONS 15302 should be grounded via the external ground connector to the rack ground.

The location of the ground connector on the ONS 15302 is shown in Figure 4-3.

Figure 4-3 Ground Connector Position on the ONS 15302



Install the Ground Connector

Step 1 Remove the phillips screw from the ONS 15302, Figure 4-3.

Step 2 Affix the flat connector with the washer and the socket screw on the ONS 15302, Figure 4-3.

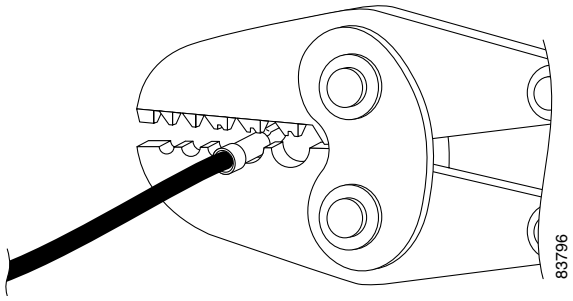
Step 3 Insert the grounding cable in the flat cable plug and crimp the plug with a crimping tool, Figure 4-4.

Step 4 Verify that the ground cable is affix in the flat cable plug.

Step 5 Connect the flat cable plug to the flat connector.

Step 6 Route the ground cable securely to the local ground connector and connect it according to local site practice.

Figure 4-4 Connection of the Ground Cable with a Crimp Tool



4.2.5 Power Considerations

The ONS 15302 can be powered using a regular telecommunication power supply of –48 VDC with a VDC return. The ONS 15302 supports redundant 48 VDC power supplies but if used the two supplies should be independently powered. The ONS 15302 can also be powered using 230 VAC regular power grid.

4.3 Fiber Cleaning

Cletop cleaning cassettes (type A for SC connectors) must be used to clean the fiber connectors and adapters before installing fiber. A video inspection instrument, with optical adapters for SC connectors is also required to inspect the fiber connectors and adapters before installing fiber.

Note Before powering the ONS 15302 clean and inspect the fiber, to prevent equipment damage. Dust particles and damaged fiber connectors will affect the optical transmission. Replace damaged fiber connectors immediately.

Warning **Invisible laser radiation may be emitted from the end of the unterminated fiber cable or connector. Do not view directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm may pose an eye hazard.**

Warning **Invisible laser radiation may be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments.**

Warning **Class 1 laser product.**

Clean Fiber Connectors

Step 1 Remove the dust cap from the fiber connector.

Step 2 Inspect connector for damage or dirt with a proper inspection tool.

Step 3 Insert the connector into the Cletop cleaning cassette slot, rotate one quarter turn, and gently swipe downwards. Repeat the inspection and cleaning from the connectors, until satisfactory results are achieved.

Step 4 Insert the fiber connector into the applicable adapter.

Step 5 Place dust caps on the fiber connectors when not in use.

Clean Fiber Adapters

Step 1 Remove the dust plug from the fiber adapter.

Step 2 Inspect the connector for damage or dirt with a proper inspection tool.

Step 3 Insert a cleaning stick into the adapter opening.

Step 4 Inspect results and continue Step 3 until satisfactory results are achieved.

Step 5 Place dust plugs on the fiber adapters when not in use.

4.4 ONS 15302 Installation

Use the following procedures to install the ONS 15302 in an equipment rack, but verify first that at least 3 RU of rack space is available.

When installing the ONS 15302, you can also use the extension brackets, included in the ONS 15302 accessory kit, to convert a 485-mm (19-inch) rack to a 600-mm (23.6-inch) rack.

Note 1 RU is 44.45 mm.

Caution Static electricity can damage electronic equipment. While unpacking and handling electronic modules, wear a grounding wrist strap to discharge the static buildup. Grounding wrist straps are designed to prevent equipment damage caused by static electricity. Before making the necessary interconnections, connect the grounding wrist strap.

Mount the ONS 15302 in an Equipment Rack

Step 1 Depending on access requirement, front or rear access, decide which side you want to use as the front side in the rack. Refer to Figure 4-5 and Figure 4-6.

Step 2 Remove the four phillips screws on the left and right side of the ONS 15302 and install the brackets with the longer phillips screws that are provided.

Step 3 Move the ONS 15302 to the desired rack position (Figure 4-5 and Figure 4-6).

Step 4 Affix the ONS 15302 to the rack with four M6 (#12-24 x3/4 pan head phillips) screws and nuts.

Figure 4-5 Install the ONS 15302 with the Connector Array in Front in a 19-in. Rack

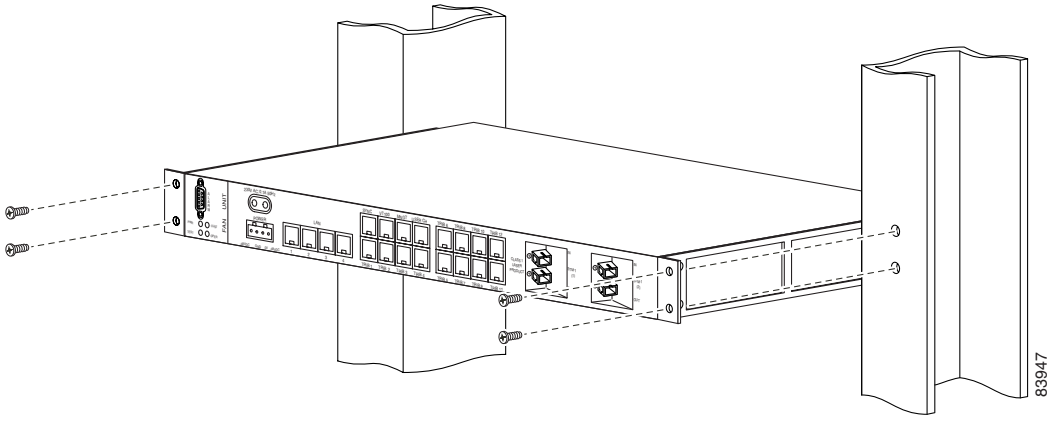
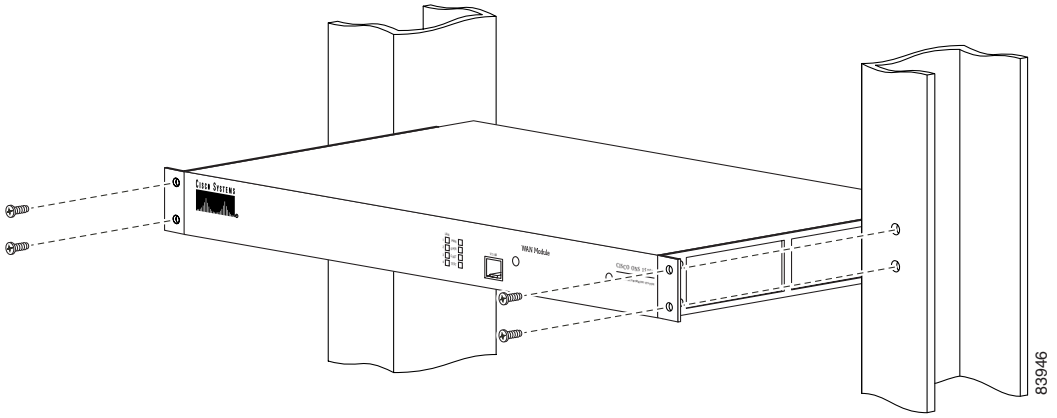


Figure 4-6 Install the ONS 15302 with the WAN Module in Front in a 19-in. Rack



Mount the ONS 15302 in an Equipment Rack Using Extension Brackets

The ONS 15302 can be installed in a 600-mm (23.6-in.) rack using the extension brackets. You need two 1 RU extension brackets for this procedure.

Step 1 Depending on access requirement, front or rear access, decide which side you want to use as the front side in the rack. Refer to See Figure 4-5 and Figure 4-6.

Step 2 Remove the four phillips screws on the left and right side of the ONS 15302 and install the brackets with the longer phillips screws that are provided.

Step 3 Move the ONS 15302 to the desired rack position.

Step 4 Affix the ONS 15302 to the equipment rack with four M6 (#12-24x3/4 pan head phillips) screws and nuts.

4.4.1 Installation in Restricted Access Locations

The ONS 15302 can be installed in a restricted access location (RAL) or outside of an RAL.

4.4.1.1 Definitions

This subsection describes definitions related to installation in restricted access location (RAL).

Restricted Access Location

A restricted access location is a site location for equipment where both of the following paragraphs apply:

- Access can only be gained by service persons or by users who have been trained on the restrictions and the precautions for this specific site.
- Access is by means of at least one of the following, special tool, lock and key, or other means of security.

SELV Circuits

Safety Extra-Low Voltage (SELV) circuits are ports that have maximum DC working voltage level less than 60 V (42.4 VAC). In addition, the ports must not be connected to telecommunication networks as defined in EN 60950 (see CEI/ IEC 60950-1 2001-10, standard clause 1.2.13.8).

In practice, the electrical cables shall not exit the building. In addition, the electrical cables shall connect to equipment that meets one of the following requirements:

- Installed in the RAL.
- Does not have electrical cables that exit the building unless those ports are TNV (Telecommunication Networks Voltage) circuits.
- Has a written consent (or in other evidence) that its connecting port towards the SELV circuit port is not a telecommunication network.

Telecommunication Network

A telecommunication network is a metallically terminated transmission medium intended for communication between equipment that might be located in separate buildings, excluding:

- Main system for supply, transmission and distribution of electrical power, if used as a telecommunication transmission medium
- Cable distribution system
- SELV circuits connecting units of information technology equipment

TNV Circuit

A TNV circuit in the equipment to which the accessible area of contact is limited. A TNV circuit is so designed and protected that, under normal operating conditions and single fault conditions (see CEI/IEC 60950-1 2001-10, standard clause 1.4.14), the voltages do not exceed specified limit values.

4.4.1.2 Installation in Restricted Access Location

After installation in a RAL, such as in a telecommunications center, the ONS 15302 must be properly installed in a rack with brackets or in other ways properly connected to a safety ground. The ONS 15302 48-VDC power must not be powered from a source external to the RAL. The E1 interface used should be limited to SELV.

4.4.1.3 Installation Outside of a Restricted Access Location

After installation in a non-RAL location, the ONS 15302 48-V power and all communication ports used must be connected to SELV circuits, for example, a port on a personal computer or 10/100-Mbit Ethernet hub/router or other information technology (IT) equipment. The 48-VDC power must not exceed 60 VDC, and must be powered from a certified external power supply unit (PSU) or a battery unit (with no connection to –48 V telecommunications voltage).

The optical ports and 230-VAC power plug have no limitations regarding safety recommendations.

4.4.2 Install the ONS 15302 –48 VDC Power

The following procedure explains how to install ONS 15302 power connections.

Connect the ONS 15302 A-side and B-side Power Connections to the PDP

Warning **Before performing any of the following procedures, ensure that power is removed from the DC circuit.**

Warning **The plug-socket combination must be accessible at all times, because it serves as the main disconnecting device.**

Caution Static electricity can damage electronic equipment. While unpacking and handling electronic modules, wear a grounding wrist strap to discharge the static buildup. Grounding wrist straps are designed to prevent equipment damage caused by static electricity. Before making the necessary interconnections, connect the grounding wrist strap.

Step 1 Remove the A- and B-side fuses from the power distribution panel (PDP).

Step 2 Make sure that –48 VDC (tolerance –36 to –72 VDC) power is present.

Step 3 Press a slot screwdriver in the rectangular opening on top of the connector to open the inside contact (Figure 4-7).

Step 4 Insert the wire in the contact and remove the screwdriver from the connector.

Step 5 To verify that the wire is properly fix in the unit, pull on the wire.

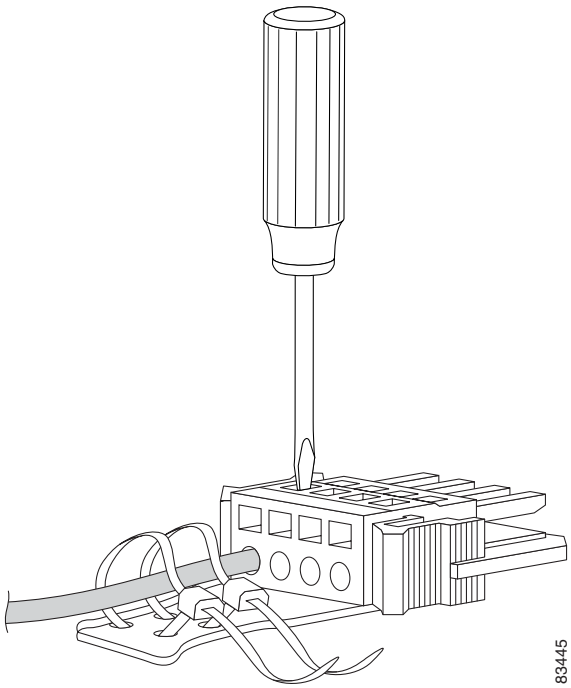
Step 6 Repeat Step 3 to Step 5 for the other three wires.

Step 7 Affix the four wires on the connector using the two tie wraps to ensure strain relief (Figure 4-7).

Note Be sure that the power cable is connected and verify the correct polarity. Check if is properly fused (1.5-A recommended).

Note Note that the ONS 15302 power cannot be switched off with a separate power switch.

Figure 4-7 Connect the Wire to the Connector



Step 8 Remove the A- and B-side fuses from the PDP.

Step 9 Connect the ONS 15302 power cable (with the ground) to the power connector of the connector array of the ONS 15302 as shown in Figure 4-2.

Step 10 Connect the first ONS 15302 –48 VDC power cable to the A-side of the PDP.

Step 11 Connect the first ONS 15302 0 VDC power cable to the A-side of the PDP

Step 12 Connect the second ONS 15302 –48 VDC power cable to the B-side of the PDP.

Step 13 Connect the second O NS 15302 0 VDC power cable to the B-side of the PDP

Note Be sure the poles are correct when you connect the power cable.

Step 14 Reinsert the A-side and B-side PDP fuses.

Step 15 Verify that the A- and B-side –48 VDC and –48 VDC return (0 VDC) of the ONS 15302 are connected to the proper poles at the power source. The –48 VDC return must be connected to ground the PDP on both the A and B sides.

Step 16 Verify that the incoming power is within the range of –36 VDC to –72 VDC before applying power.

Note The power supply has been connected correctly when the green LED is lit.

4.4.3 Install External Ground for 230 V Supply to the ONS 15302

The following procedure explains how to install ONS 15302 power connections.

Caution Static electricity can damage electronic equipment. While unpacking and handling electronic modules, wear a grounding wrist strap to discharge the static buildup. Grounding wrist straps are designed to prevent equipment damage caused by static electricity. Before making the necessary interconnections, connect the grounding wrist strap.

Connect the ONS 15302 to normal AC Outlet

Step 1 Remove the fuses from the normal AC outlet.

Step 2 Connect the ONS 15302 power cable to the 230 VAC power connector on the back of the ONS 15302 as shown in Figure 4-2.

Note Beware that ONS15302 power cannot be switched off with a separate power switch.

4.4.4 Install the ONS 15302 Fiber Cable

Caution Static electricity can damage electronic equipment. While unpacking and handling electronic modules, wear a grounding wrist strap to discharge the static buildup. Grounding wrist straps are designed to prevent equipment damage caused by static electricity. Before making the necessary interconnections, connect the grounding wrist strap.

To install fiber-optic cables in the ONS 15302, connect a fiber cable with SC connector type to the transmit and receive ports of the transmission system. On a the ONS 15302 module, the transmit and receive ports are located at the connector array of the unit. The receive port is named STM-1 IN and the transmit port is named STM-1 OUT.

Cisco recommends that you label the transmit and receive fiber (before installation) to and from the optical transmission system at each end of the fiber span to avoid confusion with cables that are similar in appearance.

Warning **Invisible laser radiation may be emitted from the end of the unterminated fiber cable or connector. Do not view directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm may pose an eye hazard.**

Warning **Invisible laser radiation may be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments.**

Warning **Class 1 laser product.**

Connect the Fiber Cable

Step 1 Remove the dust plugs from the SC (STM-1) connectors.

Step 2 Clean and inspect the SC jumper cable connectors.

Step 3 Connect the SC module input and output to the fiber termination rack.

Step 4 Repeat Step 1 to Step 3 for protection if applicable.

Step 5 Guide the fiber through the cable ties mounted on the sides of the rack. The cable ties affix the fiber to the side of the rack to reduce the risk of fiber pinching.

4.4.5 Install the ONS 15302 Electrical Cable

Caution Static electricity can damage electronic equipment. While unpacking and handling electronic modules, wear a grounding wrist strap to discharge the static buildup. Grounding wrist straps are designed to prevent equipment damage caused by static electricity. Before making the necessary interconnections, connect the grounding wrist strap.

To install electrical connection cables in the ONS 15302, connect the electrical cable with the corresponding ports of the transmission system. On the ONS 15302 module, the electrical ports are located at the connector array of the system only the VT100 (CLI Port) is located on both sides of the system. All electrical cables are equipped with RJ-45 connectors. The alarm cable is equipped with a DS-9 connector. Cisco recommends that you label the electrical cable at each end before installation to avoid confusion with cables that are similar in appearance.

Caution Follow all directions and warning labels when working with electrical cables.

Connect the Electrical Cables with RJ-45 Connector

Step 1 Carefully connect the electrical cables with RJ-45 connectors to the customer specified point.

Step 2 Repeat Step 1 to for all other electrical cables.

Step 3 Guide the cables through the cable ties mounted on the sides of the rack. The cable ties are used to hold the cables to the side of the rack to reduce the risk of fiber pinching.

Connect the Alarm Cable

Step 1 Carefully connect the alarm cable to the alarm port.

Step 2 Affix the connector with the retaining screw to the alarm port.

Step 3 Guide the cable through the cable ties mounted on the sides of the rack. The cable ties are used to hold the cables to the side of the rack to reduce the risk of fiber pinching.

4.5 Initial Configuration

By following the guides below you should be able to do the most important configurations of ONS 15302.

4.5.1 Factory Preconfiguration

Since the ONS 15302 is a flexible product with a lot of possible network applications, the factory preconfiguration is limited when delivered. Ethernet ports 1 to 5 are members of VLAN 1, the aggregate (STM-1) is enabled, and one VC-12 container is allocated to the Ethernet WAN (port number 5). In addition, an entry in the SNMP community table is preconfigured so that when an IP address is assigned, the ONS 15302 is able to take advantage of the GUI element manager. This configuration persists, regardless of whether the WAN module is inserted or not.

Example 4-1 Restore Factory Settings

The factory settings can also be restored by use of the ONSCLI command:

```
ONSCLI>Device\Factory-Reset
```

This command will only restore the factory settings properly if the configuration is cleared before the command is given. To make sure reset configuration is done, following line appears on the system terminal when Factory-Reset command is given:

```
Are device configuration) erased (y/n)?
```

4.5.2 Important Commands

Follow the steps in this section to perform initial configuration of the ONS 15302. The following tasks are the most important tasks involved in the configuration of an ONS 15302:

- System-Mode
- Assign IP address
- Define SNMPv1 community

– Erase a community string

4.5.3 Assign an IP Address to the ONS 15302

The ONS 15302 supports remote management solutions by the means of Telnet and SNMP.The possibilities as regards connectivity can be rather advanced for the ONS 15302 so the only explained solution in this document is when directly connected the management-port (MNGT). For more information please refer the *Cisco ONS 15302 Installation and Operations Guide* (Release 2.0).

To achieve one of the above mentioned management solutions it is necessary to assign an IP-address, subnet-mask and if required a default-gateway address must be defined.

4.5.3.1 System Mode

In ONS 15302 R2.0 an additional management mode, system mode is added.The System mode has two options, ip and ipunnumbered.

```
ONSCLI>...\Management-Configuration\sys?

Usage:
   System-Mode
[SYSTEM-MODE=<ip|ipunnumbered>]
```

Example 4-2 System Mode - IP

```
ONSCLI>...\Management-Configuration\sys sys=ip
Change management configuration, are you sure? (y/n)?
```

Example 4-3 Assign an IP-address:

If system mode is ip the command for IP configuration is:

```
ONSCLI>Device\Management-Configuration\Management-Port\IP-Configuration
IP-ADDRESS=193.69.136.104, SUBNET-MASK=255.255.255.0.
```

Example 4-4 System Mode - IP Unnumbered

```
ONSCLI>...\Management-Configuration\sys sys=ipunnum
Change management configuration, are you sure? (y/n)?
```

Example 4-5 Assign an IP-address:

If system mode is ipunnumbered the command for IP configuration is:

```
ONSCLI>Device\Management-Configuration\IP-Configuration IP-ADDRESS=193.69.136.104,
SUBNET-MASK=255.255.255.0.
```

4.5.3.2 Define SNMPv1 Community

Example 4-6 Factory pre-configured community:

```
Manager: 0.0.0.0
Community:public
Access:Super
Traps:Disabled
```

This is an insecure community, which enables all managers regardless of the IP-address for the SNMP manager to access the device with the community string "public".

Example 4-7 Add your own community string

To add your own community string please use the following command:

```
ONSCLI>Security\Community-Table\add manager=10.0.0.20 community=admin access=super
traps=enable
"Enter"
```

4.5.3.3 Erase a Community string

To remove a community string the following command can be used:

```
ONSCLI>Security\Community-Table\remove manager=0.0.0.0 community=public
"Enter"
```

Note Please see the Cisco EdgeCraft User Guide for further configuration and management of ONS 15302.

4.6 Software Download through Local VT100 Interface

The software is loaded using a PC connected directly to the ONS 15302 via the VT100 port. You must be on site with the ONS 15302 to install the software, you can not complete the installation remotely. The file is loaded using the Xmodem protocol. Booting the system triggers local software download. Ethernet traffic is lost during the software load process. Please secure the traffic on 2 MBit/s (Mbps) tributaries.

Please follow the steps below for a successful download operation.

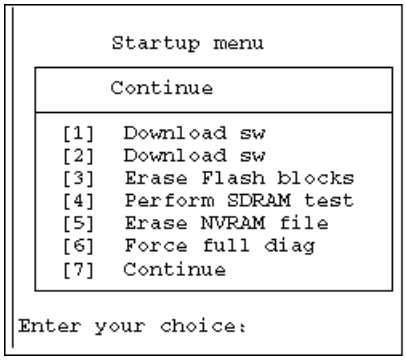
Step 1 Make sure that you are connected and the cursor ONSCLI>DEVICE\> is visible.

Step 2 Type *reset* and press **Enter**. Press **Y** to confirm command.

Step 3 You have now triggered a software restart, and the boot process will be started immediately.

Step 4 When you see the following window (Figure 4-8), press **1** immediately.

Figure 4-8 ONS 15302 Software Download Start Menu

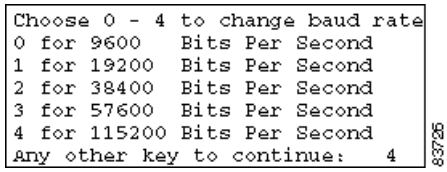


Note If you are too slow entering **1,** the device will continue the boot process and you will have to reboot again.

Step 5 If you successfully completed Step 4, you will immediately be prompted to choose a baud rate for the Xmodem. The recommended baud rate is 115 200 bit/s, Figure 4-9.

```
Choose the number for your selection
```

Figure 4-9 Select a Baud Rate



Step 6 After completing Step 5, you will be requested to set up your terminal according to chosen baud rate, Table 4-1.

Step 7 Disconnect and set terminal speed to 115 200 bit/s, connect and press **Enter** to continue.

Step 8 Set the parameters as shown in Table 4-1.

Table 4-1 EIA/TIA 232 Interface Parameter

Parameter	Settings
Bits per second	115200
Data bits	8
Parity	None
Stop bits	1
Flow control	Hardware

Step 9 When the setup is correct, the following message will appear in terminal window:

```
Please download program using XMODEM.
$$$$
```

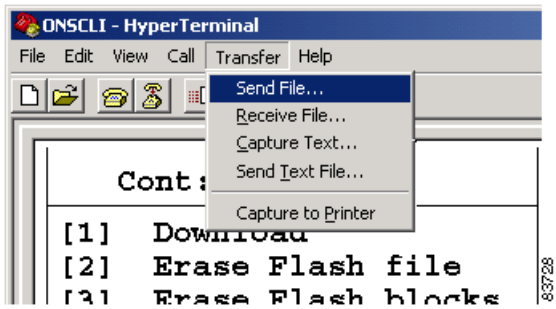
The device is now ready to receive the new software (firmware).

Step 10 If you perform this by using Hyper Terminal (Windows), please perform the steps shown in Figure 4-10.

a. Select **Transfer**.

b. Select **Send File**.

Figure 4-10 Hyper Terminal Window



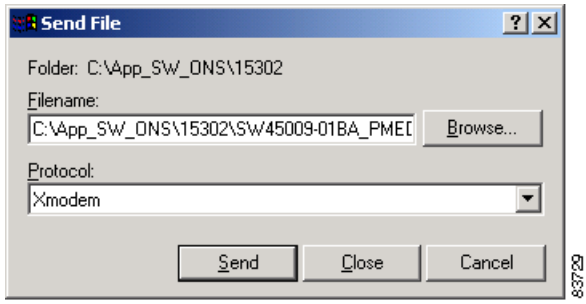
Step 11 Select the **Folder** containing the software, Figure 4-11.

The correct filename appears, otherwise press **Browse** and search for the right filename.

Choose **Protocol** Xmodem.

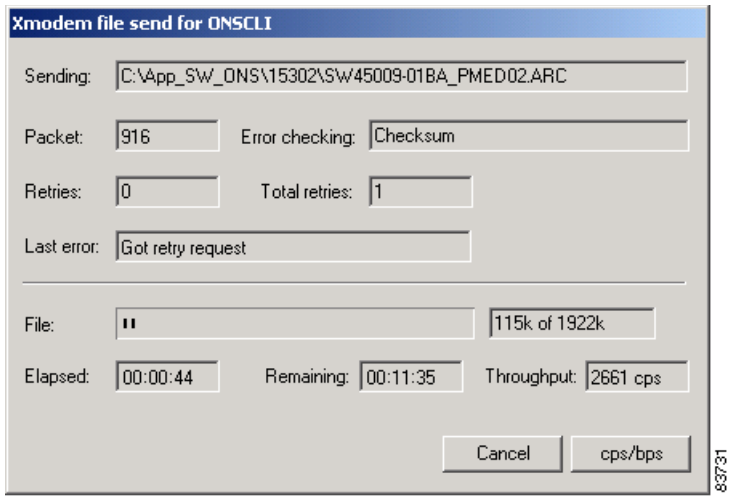
Press **Send.**

Figure 4-11 Send File Menu



The download is now started and you can monitor the download process in the **Remaining** field, Figure 4-12.

Figure 4-12 Download Response Menu



When the download has finished, the device will immediately start to write to flash and update its registry and automatically reboot. The total time for the download operation is approximately 10 minutes.

Step 12 At this time, the system instructs you to disconnect the connection and to change the baud rate to 9600. Then the system reboots.

Step 13 Check the inventory to make sure that the download operation was successful using the following string:

ONSCLI>**Device\Inventory**

Troubleshooting

This chapter allows you to solve problems with the ONS 15302.

5.1 Introduction

The ONS 15302 is tested extensively and verify before leaving the factory. However, if your system appears to have problems during start up, use the information to help isolate the cause.

When the initial system boot is complete, verify the following:

- Power is being supplied to the system.
- System software boots successfully.

If the start-up sequence fails before these conditions are met, use the procedures in this chapter to isolate and, if possible, resolve the problem.

If you are unable to easily solve the problem, contact TAC for assistance and further instructions. Have the following information ready to help TAC assist you as quickly as possible:

- Date you received the equipment
- Chassis serial number
- Type of software and release number
- Brief description of the problem you are having
- Brief explanation of the steps you have already taken to isolate and resolve the problem
- Maintenance agreement or warranty information

5.2 Problem Solving

The key to problem solving the system is to try to isolate the problem to a specific subsystem. The first step in solving start-up problems is to compare what the system is doing to what it should be doing. Since a start-up problem can usually be attributed to a single component, it is more efficient to first isolate the problem to a subsystem rather than troubleshoot each separate component in the system.

The ONS 15302 consists of the following subsystems.

- Main Card
- WAN-module
- Optical system (protected or unprotected)

5.3 Identify Start-up Problems

LEDs indicate all system states in the start-up sequence. By checking the state of the LEDs, you can determine when and where the system failed in the start-up sequence.

When you plug in the power supply to start the system, the following should occur:

- The Power LED turns green when you plug in the connector.
- The Operation, Customer and Test LEDs operate as follows during equipment start-up.

All LEDs are lit simultaneously for a few seconds with an interval of ~1 minute during start-up. The start-up procedure takes approximately 3 minutes.

The LED indicators used to visualize the ONS 15302 status are located on the WAN Module side, see Table 5-1/ Figure 6-3and on the connector array side, see Table 5-2/Figure 6-2.

Table 5-1 LED Functionality on the WAN Module Side

Identity	Color	State On	State Flashing	State Off
PWR (Power)	Green	Presence of power	NA	Power failure
OPER (Operation)	Red	Alarm detected on aggregate interface	NA	No alarm detected on aggregate interface
CUST (Customer)	Red	Alarm detected on tributary or LAN interface	NA	No alarm detected on tributary or LAN interface
TEST (Test)	Yellow		One or more test are activated	
LAN 1	Green	Link is present	Traffic is present	Link down
LAN 2	Green	Link is present	Traffic is present	Link down
LAN 3	Green	Link is present	Traffic is present	Link down
LAN 4	Green	Link is present	Traffic is present	Link down

Table 5-2 LED Functionality on the Connector Array Side

Identity	Position	Color	State On	State Flashing	State Off
PWR (Power)		Green	Presence of power	NA	Power failure
OPER (Operation)		Red	Alarm detected on aggregate interface	NA	No alarm detected on aggregate interface
CUST (Customer)		Red	Alarm detected on tributary or LAN interface	NA	No alarm detected on tributary or LAN interface
TEST (Test)		Yellow		One or more test are activated	

Table 5-2 LED Functionality on the Connector Array Side (continued)

Identity	Position	Color	State On	State Flashing	State Off
LANn (n-1,2,3,4)	Left	Green	100 MBits/s (Mbps)	NA	NA
LANn (n-1,2,3,4)	Left	Yellow	10 MBits/s (Mbps)	NA	NA
LANn (n-1,2,3,4)	Right	Green	Link OK	Ethernet traffic in operation	Link down

5.4 Restore Factory Pre-configuration

This section describes how to restore factory pre-configuration to the ONS 15302.

The simplest way to automatically configure an ONS 15302 is to take advantage of VT100 emulating software. From a VT100 terminal it is possible to send a text file (script) instead of manually writing paths and command(s) to change or add configuration on the device.

This procedure for restoring the factory pre-configuration assumes that the user has installed the HyperTerminal program on a common PC running Microsoft Windows 2000, but most of the content will work with any terminal emulation software. In addition it is necessary to use a console cable (CLI cable) according to the specification to connect a COM port on the PC with the VT100 interface on the ONS 15302.

5.4.1 Additional Terminal Settings

In addition to the standard parameters for communicating with the ONS 15302 (Table 5-3) it is also necessary to adjust the line delay (the time to wait between sending commands to the device), to allow for responses from the device. If the command issued results in the display of a long table, this will require more time than simple one-line responses The optimal time might vary between PC, so you might have to try a couple of different settings. A good start value is 500 ms. In some cases increasing character delay to a few milliseconds might help too. Exactly where to adjust this in HyperTerminal see Table 5-3.

Table 5-3 EIA/TIA 232 Interface

Parameter	Condition
Baud rate	19.2 kbaud
Data bits	8
Parity	None
Stop bits	1

Figure 5-1, Figure 5-2 and Figure 5-3 describes how to configure the Line delay.

Figure 5-1 Select Properties

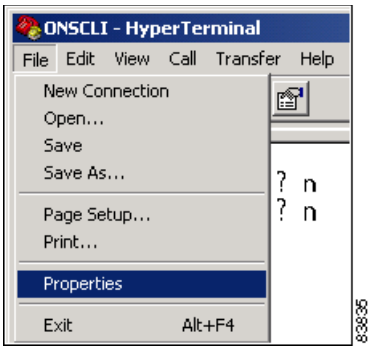


Figure 5-2 Select ASCII Setup

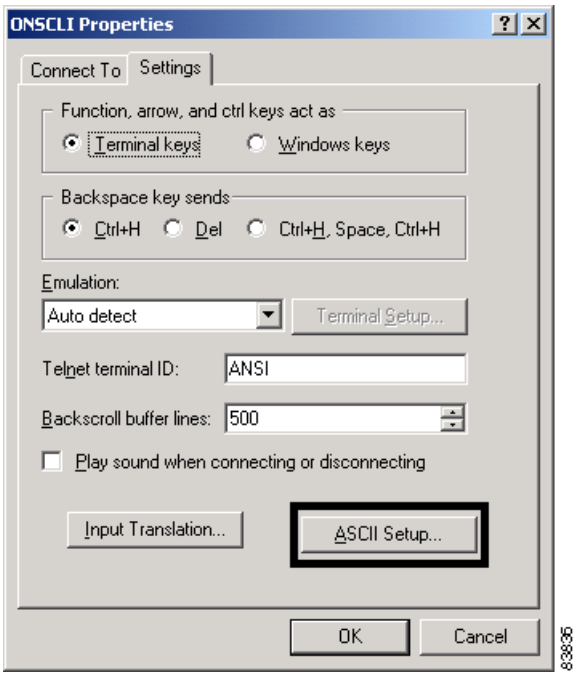
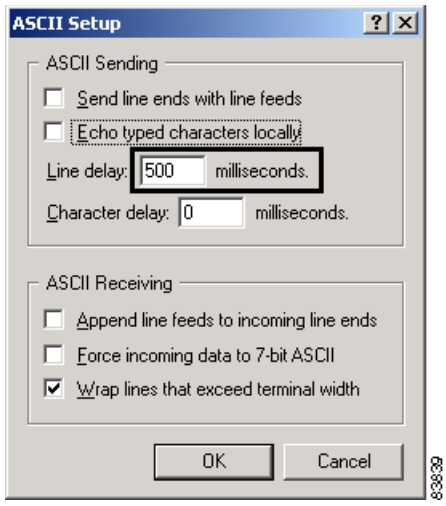


Figure 5-3 Configure Line Delay



5.4.2 Prepare the Script File

The script file can be prepared by using a text editor program, for example, Notepad for Windows computers. The content in a script file is only limited to valid commands and paths for ONSCLI. Examples below show the script files for the pre-configuration of the unprotected and protected versions that is to be used when installing a device from the factory.

Unprotected Version:

dev\vlan\vlan-t\add name=vlan1

dev\vlan\vlan-p\add if=100000 eth=1,2,3,4,5 tag=dis

port\agg\gen adm=en

port\eth\wan\add wan=5 nu=1

sec\commun\add man=0.0.0.0 comm=public acc=super tra=dis

Protected Version:

dev\vlan\vlan-t\add name=vlan1

dev\vlan\vlan-p\add if=100000 eth=1,2,3,4,5 tag=dis

port\agg\gen agg=1 adm=en

port\eth\wan\add wan=5 nu=1

sec\commun\add man=0.0.0.0 comm=public acc=super tra=dis

5.4.3 Erase a File (CDB file)

Since the purpose of this section is to restore factory pre-configurations the unit has most likely been configured with testing parameters. To make sure that CDB file is empty we recommend that it is erased before sending the text file down to the device. To perform this on the ONS 15302 follow the steps below.

Step 1 Login to command line interface by typing ONSCLI and ONSCLI again when prompted for password

Step 2 Select the following command:

```
>ONSCLI\Device\erase
```

Typing **yes** when prompted!

Step 3 To complete the CDB erase you will have to reboot the system. Write the following command:

```
>ONSCLI\Device\reset
```

Typing **yes** when prompted!

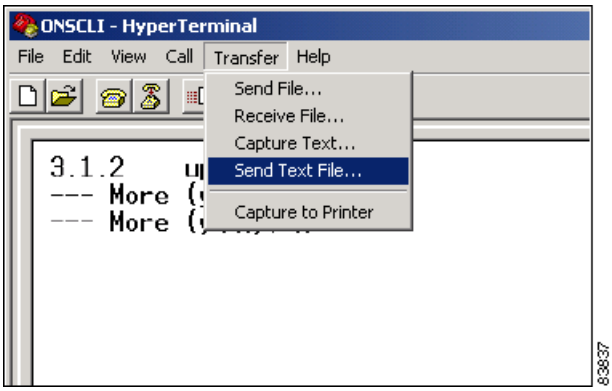
When the ONS 15302 has restarted you are ready to perform the procedure in 5.4.4 Send Scripts Procedure.

5.4.4 Send Scripts Procedure

The procedure for sending scripts to the device is rather simple if the above preparations are completed. Please login to the ONSCLI, and follow these steps to accomplish the restoration of factory pre-configuration.

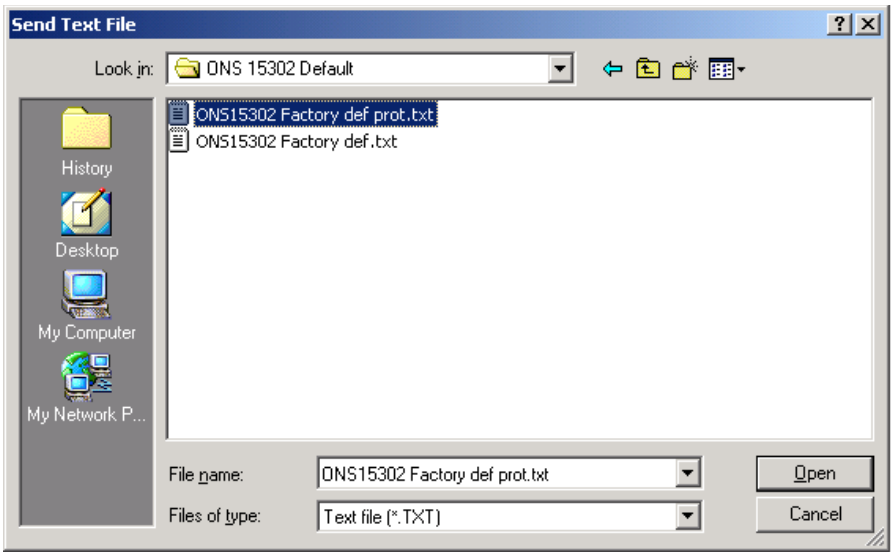
Step 1 Select in the pull down menu transfer and the command send text file, Figure 5-4.

Figure 5-4 Select Send Text File



Step 2 Select in the send text file window the file that you want to download, Figure 5-5.

Figure 5-5 Select the File



If all necessary preparations are performed as described in this section the ONS 15302 should now be successfully configured according to factory pre-configuration.

Technical Specifications

This chapter provides Technical Specifications of the Cisco ONS 15302.

6.1 Mechanical Overview

The equipment is provided as a subrack suitable for mounting within a 485mm (19-in.) and 600mm (23.6-in) equipment cabinet.

Figure 6-1 shows the outer dimensions of the ONS 15302 system equipment.

Figure 6-1 Outer Dimensions of the ONS 15302 System

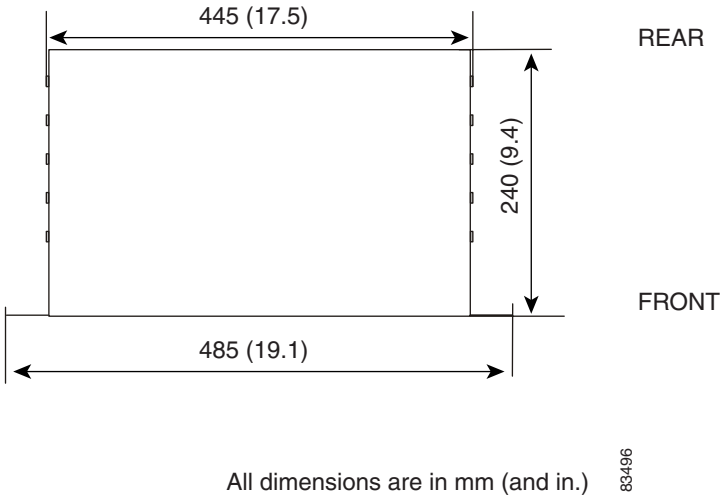


Figure 6-2 and Figure 6-3 display the two different views of the ONS 15302 with the different LEDs and connectors.

Figure 6-2 View of the ONS 15302 with the Connector Array in Front

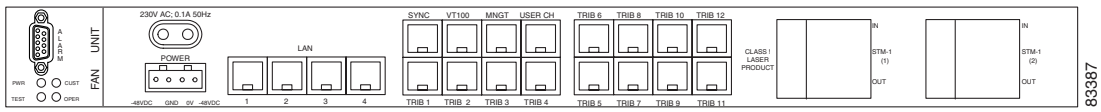


Figure 6-3 View of the ONS 15302 with the WAN Module in Front

6.2 Interfaces

Table 6-1 show the relationship between the type of interface and the logical names use in this document.

Table 6-1 ONS 15302 Interfaces

Interface	No. of interfaces	Logical name
Optical/Electrical	2	Aggregate Port
Tributary	12	Tributary Port
Ethernet	5	LAN Ports and Management Port
(Ethernet)	4	WAN ports
Alarm	6	4 alarm input and 2 alarm out
Synchronization	1	Sync Port
EIA/TIA 232	1	ONSCLI Port
Power supply	2	-48V DC and 230V AC
User Channel	1	User Channel Port
Indicators	8	4 Traffic Indicators, Power Indicator, Operator Indicator, Customer Indicator, Test Indicator

6.3 Light Emitting Diodes (LEDs)

The LED indicators are used to visualize the ONS 15302 status.

Table 6-2 LED Functionality on the WAN Module Side

Identity	Color	State On	State Flashing	State Off
PWR (Power)	Green	Presence of power	NA	Power failure
OPER (Operation)	Red	Alarm detected on aggregate interface	NA	No alarm detected on aggregate interface
CUST (Customer)	Red	Alarm detected on tributary or LAN interface	NA	No alarm detected on tributary or LAN interface
TEST (Test)	Yellow		One or more test are activated	

Table 6-2 LED Functionality on the WAN Module Side (continued)

Identity	Color	State On	State Flashing	State Off
LAN 1	Green	Link is present	Traffic is present	Link down
LAN 2	Green	Link is present	Traffic is present	Link down
LAN 3	Green	Link is present	Traffic is present	Link down
LAN 4	Green	Link is present	Traffic is present	Link down

Table 6-3 LED Functionality on the Connector Array Side

Identity	Position	Color	State On	State Flashing	State Off
PWR (Power)		Green	Presence of power	NA	Power failure
OPER (Operation)		Red	Alarm detected on aggregate interface	NA	No alarm detected on aggregate interface
CUST (Customer)		Red	Alarm detected on tributary or LAN interface	NA	No alarm detected on tributary or LAN interface
TEST (Test)		Yellow		One or more test are activated	
LANn (n-1,2,3,4)	Left	Green	100 MBits/s (Mbps)	NA	NA
LANn (n-1,2,3,4)	Left	Yellow	10 MBits/s (Mbps)	NA	NA
LANn (n-1,2,3,4)	Right	Green	Link OK	Ethernet traffic in operation	Link down

6.4 Optical Aggregate Line Interface

The ONS 15302 aggregate line interface is bidirectional with a transmit (Tx) and a receive (Rx) direction. The two fibre variant is a short haul (SH), ITU-T Rec. G.957 S-1.1 compliant variant. The transmission cable can be either Single Mode (SM) or Multi Mode fibre (MM) type.

ONS 15302 is also available in protected variants with duplicated optical interfaces and protection switching logic to maintain traffic in case of fibre faults.

The optical interfaces are located at connector array side and equipped with SC connectors.

Parameters

The ONS 15302 aggregate line interface optical power budget is shown in Table 6-4.
See Table 6-5 - Table 6-7 for details relevant when cable planning for ONS 15302.

Note The definitions of optical parameters and reference points S and R refer to ITU-T G.957. Reference point S means transmit direction while R is the receive direction of the fibre.

Table 6-4 Optical Power Budget ONS 15302

Parameter	Short Haul (S-1.1)	Unit
Type of fibre: ITU-T Rec. G.652	10/125	micrometer
Type of fibre: ITU-T Rec. G.651	50/125	micrometer
IEC 739-2	62.5/125	micrometer
Modulation rate on optical line	155 520	kbit/s
Wavelength range	1270 to 1335	nm
Transmitter at reference point S		
Source type	MLM	
Spectral characteristics (max. RMS width)	3	nm
Mean launched power (max.)	–8	dBm
Mean launched power (min.)	–12	dBm
Min. extinction ratio	8.2	dB
Optical path between S and R		
Attenuation range	0 to 17	dB
Max. tolerable dispersion	280	ps/nm
Min. optical return loss	NA	
Max. discrete reflectance between S and R	NA	
Receiver at reference point R		
Min. sensitivity (BER < 1 in 1010)	–30	dBm
Min. overload	0	dBm
Max. optical path penalty	1	dB
Max. reflectance at R	NA	

Factory testing to Power Budget: Mean Launched Power adjusted to –10 dBm. Receiver sensitivity test: Max. signal level –32 dBm at R point at BER < 1 in 10 exp –10. Initial equipment margin: >3 dB.

Table 6-5 Example of Cable Planning for ONS 15302 (Cable Loss)

Cable Loss, according to ITU-T Rec. G.957	Single Mode fibre Acc. to ITU-T G.652	Multi Mode fibre Acc. to ITU-T G.651
Fibre Cable Attenuation	0.5 dB/km	1.0 dB/km
Cable Margin (Mc)	Incl. in	3 dB
Loss in Optical Distribution Frame	Incl. in	1 dB

Table 6-6 Example of Cable Planning for ONS 15302 (Cable Dispersion)

Cable Dispersion:		
Maximum Chromatic Dispersion Coefficient	3.5 ps/nm km	6 ps/nm km
Modal bandwidth	—	800 MHz km
Overall bandwidth (Requirement >80 MHz)	—	84 MHz (9km)

Table 6-7 Typical Link Spans for ONS 15302

ONS 15302 type of fibre	Mode	Loss Limited Span	Dispersion Limited Span	Overall Link Span
Short-Haul	SM	34 km	80 km	34 km
Short-Haul	MM	13 km	9 km	9 km

Jitter on the Tx optical output signal is lower than the values specified in ITU-T Rec. G.813, (Table 6-8).

Table 6-8 Optical Output Jitter Requirements as given in ITU-T Rec. G.813.

Filter bandwidth	Jitter limit
500 Hz to 1.3 MHz	0.50 Uipp
65 kHz to 1.3 MHz	0.10 Uipp

The input aggregate port tolerates the input jitter and wander specified in ITU-T Rec. G.825, (Table 6-9). This applies in the whole operating optical range of the receiver.

Table 6-9 Maximum Tolerable Input Jitter on the Optical Rx Interface.

Frequency range	Jitter limit
500 Hz to 6.5 kHz	1.5 Uipp
6.5 kHz to 65 kHz	Decaying, slope equal to 20 dB/decade
65 kHz to 1.3 MHz	0.15 Uipp

6.5 Tributary Ports

This section describes technical specifications for the ONS 15302 tributary ports.

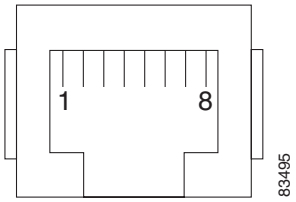
Connectors

The connectors are RJ-45 connectors, with pinout as shown in Table 6-10.

Table 6-10 Pinout Tributary Interface

Pin	Signal
1	RxD+
2	RxD–
3	GND
4	TxD+
5	TxD–
6	Screen, (the outer screen is always connected to ground)
7	NC
8	NC

Figure 6-4 Tributary 120 Ohm Interface Connector



Parameters

The next tables displays the parameters of the tributary port

Table 6-11 Tributary input jitter parameters is compliant to the ITU-T G.823 02/00 table 16 requirements.

Table 6-11 Tributary Input Jitter Parameters

Frequency range	Jitter limit
20 Hz to 2.4 kHz	1.5 Uipp
2.4 kHz to 18 kHz	Decaying, slope equal to 20 dB/decade
18 kHz to 100 kHz	0.2 Uipp

Table 6-12 Tributary input reflection loss is complaint to ITU-T G.703

Table 6-12 Tributary Input Reflection Loss

Frequency range	Reflection loss
51 kHz to 102 kHz	12 dB
102 kHz to 2048 kHz	18 dB
2048 kHz to 3072 kHz	14 dB

The requirements for output jitter in the absence of input jitter and pointer movements are shown in Table 6-13. The output jitter is complaint to requirements ITU-T G.783.

Table 6-13 Tributary Output Jitter without Pointer Movements

Filter Bandwidth	Jitter output (p-p)
20 Hz to 100 kHz	< 0.25 UI
700 Hz to 100 kHz	< 0.075 UI

The requirements for output jitter in the absence of input jitter but with pointer movements are shown in Table 6-14. The output jitter is complaint to requirements ITU-T G.783

Table 6-14 Tributary Output Jitter with Pointer Movements

Filter Bandwidth	Jitter output (p-p)
20 Hz to 100 kHz	< 0.4 UI
700 Hz to 100 kHz	< 0.075 UI

6.6 LAN Ports and Management Port

This section describes technical specifications for the ONS 15302 LAN and management ports.

Connectors

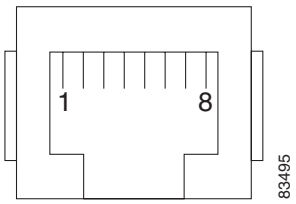
The connectors are RJ-45 connectors see Figure 6-5, with pinout as described in Table 6-15.

Table 6-15 Pinout Ethernet Ports

Pin	Signal
1	TxD+
2	TxD–
3	RxD+
4	NC
5	NC
6	RxD–
7	NC
8	NC

Note The Management Port is configured with a fixed setup - 10Mb / half-duplex.

Figure 6-5 LAN Ports and Management Connector



Note In order to conform to the requirements of EN50081-1 Class B it is recommended to use a STP cable for connection to the Management port. If a UTP cable is used the unit conform to EN50081-1 Class A.

6.7 Alarm Interface

This section describes technical specifications for the ONS 15302 alarm interface.

Connectors

The alarm interface connector is a DS-9 connector, with pinout as described in Table 6-16

:

Table 6-16 Pinout Alarm Interface

Pin	Signal
1	Gnd
2	Alarm input 1 (aux 1)
3	Alarm input 2 (aux 2)
4	Alarm input 3 (aux 3)
5	Alarm input 4 (aux 4)
6	Alarm input return
7	Alarm output 1
8	Alarm output return
9	Alarm output 2

Parameters

The electrical specification for the alarm input is described in Table 6-17. The electrical specification for the alarm output is described in Table 6-18.

Table 6-17 Electrical Specification at Alarm Input

Parameter	Value
Nominal open contact voltage	3.3 V
Nominal closed contact current	1 mA

Table 6-17 Electrical Specification at Alarm Input (continued)

Parameter	Value
Maximum closed contact resistance	0.8 kohm
Minimum open contact resistance	10 kohm

Table 6-18 Electrical Specification at Alarm Output

Parameter	Value
Maximum load bias referred to common return	+/– 75 V
Maximum load current	50 mA
Common return to earth	+/– 250 V
Maximum contact resistance	50 ohm

6.8 Synchronization Port

ONS 15302 has one 2048 kHz synchronization output port and input port.

Connectors

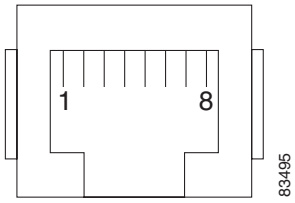
Both input and output is provided on 8 pin RJ-45 connector (Figure 6-6), with the pinout given in Table 6-19.

:

Table 6-19 Pinout Synchronization Port

Pin	Signal
1	Sync input +
2	Sync input –
3	GND
4	Sync output +
5	Sync output –
6	Screen (the outer screen is always connected to ground)
7	NC
8	NC

Figure 6-6 Synchronization Connector



Parameters

Table 6-20 Synchronization Input Jitter Parameters

Frequency range	Jitter limit
20 Hz to 2.4 kHz	1.5 Uipp
2.4 kHz to 18 kHz	Decaying, slope equal to 20 dB/decade
18 kHz to 100 kHz	0.2 Uipp

Table 6-21 Synchronization Input Reflection Loss Parameters

Frequency	Reflection loss
2048 kHz	15 dB

Table 6-22 Synchronization Output Jitter Parameters

Filter bandwidth	Jitter output (p-p)
20 Hz to 100 kHz	< 0.05UI

6.9 ONSCLI Port

The ONSCLI Port is accessible from both side of the unit by means of two parallel connectors.

Connectors

The EIA/TIA 232 interface for ONS 15302 is provided using a RJ-45 connector, with the following pinout Table 6-13.

Table 6-23 Pinout CLI Connector

Pin	Signal
1	GND
2	TxD
3	RxD
4	DB_TxD (are only used for debug purposes)
5	NC
6	RTS
7	DB_RxD (are only used for debug purposes)
8	NC

Figure 6-7 ONSCLI Port Connector

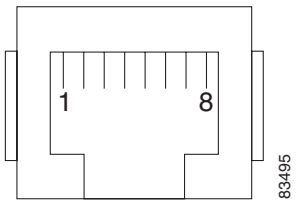


Table 6-24 CLI Connector Pinout (RJ-45 to DS-9)

RJ-45 Connector		DS-9 Connector	
Pin 1	GND	Pin 5	NC
Pin 2	Tx	Pin 2	Rx
Pin 3	Rx	Pin 3	Tx
Pin 4	NC		
Pin 5	NC		
Pin 6	CTS	Pin 8	CTS
Pin 7	NC		
Pin 8	RTS	Pin7	RTS

Pin 4 and 7 are only used for debug purposes.

Parameters

The interface is running at a data rate of 19.200 baud.

6.10 Power Supply

ONS 15302 supports two different power supplies:

- Single phase 230 V 50 Hz AC mains supply
- –48 V DC supply

Connectors

The –48V DC supply input on the ONS 15302 is provided via a 4 pin power connector, with the following pinout Table 6-25.

Table 6-25 Pinout Power Supply Connector

Pin	Signal
1	–48V (supply 1)
2	GND

Table 6-25 Pinout Power Supply Connector (continued)

Pin	Signal
3	0V (–48V return)
4	–48V (Supply 2)

The 230V mains supply input on the ONS 15302 is provided via a standard connector according to EN60320.

Parameters

The –48V DC input and the 230V mains input are according to the specifications given in the table below

Table 6-26 Power Supply Parameters

Parameter	Limit
Power dissipation	Less than 40W
Fuse	1.5A
Battery voltage range	–36 to –72 V DC
Mains voltage	230V AC +/– 10%

6.11 User Channel

A user channel is provided for transportation of general data. The port is balanced V.11 and support synchronous 64 kBit/s or asynchronous 19.2 kBit/s by configuration.

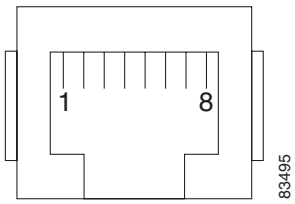
Connectors

The user channel interface for ONS 15302 is provided using a RJ-45 connector, with the following pinout Table 6-27

Table 6-27 Pinout User Channel Connector

Pin	Signal
1	TxD+
2	TxD–
3	RxD+
4	TxCLK–
5	TxCLK+
6	RxD–
7	RxCLK+
8	RxCLK–

Figure 6-8 User Channel Port Connector



6.12 Fan Unit

The main feature of the fan unit is to ventilate the 19"/ 1U cabinet used for ONS 15302. The fan unit is a plug in device consisting of a circuit board with two fans. The air is sucked in via two circular openings in the left sidewall, and emerges via holes in the right side cabinet wall. Two fans are used to improve reliability and give a lifetime of 10 years for this module.

Note Make sure that there is minimum 10 cm free space around the air intake (placed in the left sidewall)

Parameters

Fan operation is shown in the table below. Threshold temperatures are approximate and depend on ventilation conditions.

Note The ventilation holes must not be blocked.

Table 6-28 Fan Operation and Alarm

Conditions	Behavior	Alarms
Ambient temperature below 50 to 60 degrees C	Normal operation	No Alarm
Failure of a fan, no fan tray present or fans stopped by obstruction	Trying to start the other fan or no fan is running	FAN alarm
Ambient temperature above 50 to 60 degrees C	Fan running on full speed	TEMP alarm
Every ~24-hours	Working fan is interleaved with the other fan	

Note The TEMP alarm will always be cleared if ambient temperature fall below 45 degrees C

6.13 Reliability

The overall error ratio of a tributary channel is better than 10 exp –10.

According to MIL-HDBK-217F with a correction factor adjustment related to the following conditions:

- Ground benign
- +35 degrees C ambient temperature
- Stress value 0.5

Table 6-29 Reliability

Equipment	MTBF [Years]
ONS 15302 non-redundant optics	40
ONS 15302 redundant optics	47

ONSCLI Command Line Interface

ONSCLI is a line oriented ASCII based management interface to the ONS 15302, by means of which simple commands (possibly with parameters) may be issued to access or modify the ONS 15302 configuration.

7.1 User Interface

The ONSCLI uses a UNIX style, character based user interface that allows you to communicate directly and provides commands that allows users to add, delete, and configure objects, alarms, and parameters.

7.1.1 Document Conventions

Many commands available in the ONSCLI have parameters that allow you to configure specific aspects of a given command. Command parameter syntax follows rules that help the user identify which parameters are optional, which are required, which need to be repeated, and so on. These rules follow in the next tables:

Table 7-1 Documents Conventions

Convention	Description
string	A string is a non-quoted set of characters shown in italics. For example, when setting an SNMP community string to public, do not use quotation marks around the string or the string will include the quotation marks.

Table 7-2 Syntax Conventions

Convention	Description
boldface	Command or keyword that you must enter.
<*italic*>	Parameter or argument for which you supply a value.
[x]	Optional keyword or argument that you may enter.
|	Choice within an optional or required set of keywords or arguments.
[x | z]	Keywords or arguments separated by a vertical line indicate an optional choice.

7.1.2 User Privileges

The user privileges are split up into three categories.

The read only user is allowed to see and read the commands. This user has no write-privileges.

The read and write users is allowed to read and right commands this means he is allowed to execute the commands.

The super user has privileges to manage the system and to change IP address and subnet mask.

7.1.3 Login

ONSCLI is accessed via the VT100-port or via an IP connection (Telnet). The serial connection communications parameters are fixed (Table 7-3). VT100 terminal codes are used. The system prompted for a user name and a password before access is granted.

Table 7-3 EIA/TIA 232 Parameters

Parameter	Value
Speed	19200 bps
Data bits	8
Parity	None
Stop bits	1
Flow control	None

The VT100-port (Console port) for the ONS 15302 is provided using a RJ-45 connector.

Invoke an ONSCLI Session

An ONSCLI session is invoked by typing ONSCLI at the CLI terminal.

User authentication (a password containing between 8 and 12 ASCII characters, with no case sensitivity) is required, as the following session start-up sequence shows:

```
>
>ONSCLI

--------------------------------------------------
          ONS 15302 Command Line Interface
--------------------------------------------------

Enter ONSCLI password: ******

ONSCLI>
```

Note The default password for the ONS 15302 is ONSCLI.

Incorrect Password

Each password characters is echoed as *. An incorrect password is rejected with the message:

```
invalid password
```

After the password is rejected, the password prompt is re-issued.

Note The number of attempts is 3.

An authorized ONSCLI user has full access rights to the available management information.

Exit

The **Exit** command is used to terminate an ONSCLI session. The ONSCLI session is automatically terminated after a period of 30 minutes of inactivity. ONSCLI does not accept simultaneous sessions.

Syntax Rules

An ONSCLI command line begins with a prompt (issued by ONSCLI), which serves to indicate the current position in the command hierarchy.

An ONSCLI command is issued by typing the command followed by **Enter**. Optionally, and only at the lowest level in the command hierarchy, one or more parameters can also be supplied. These are identified by keywords. The command name, parameter keywords, and parameter values are delimited by one or more spaces. Command line editing features are listed in Table 7-4.

Note It is only necessary to type sufficient leading characters of the command name to avoid ambiguity—the same applies to keywords.

Backspace or Delete may be used to edit the command line. Commands and keywords are Not case sensitive, although for clarity they are written in this document using both upper and lowercase letters. A list of valid commands that have been issued in the current session is maintained in a command history.

Table 7-4 Command Line Editing Features

Key	Result
Delete or Backspace	Erases the character in the command line.
Arrow left	Moves the cursor to the left side.
Arrow right	Moves the cursor to the right side.
Arrow Up	Recalls the previous command in command history.
Arrow Up	Recalls the previous command in command history.
Return or Enter	At the command line, processes a command.
..	Returns to the previous command level.
\	Goes to the top command level.
?	Issues a list of commands valid at the current level, or shows the command usage.

ONSCLI Commands are listed in Table 7-5

Table 7-5 ONSCLI Commands

Command	Result
Free	Shows VC-12 containers that are not yet utilized.
Used	Lists the VC-12 container(s) in use.
Status	Presents current device and port status.
Exit	Exits ONSCLI.

Some commands (in particular the **show** command) can potentially produce many lines of output. After a predetermined number of lines of output in response to a single command, the user is prompted to enter **y(es)** or **n(o)** to continue the output. The default line number limit is 23 and maximum is 998.

7.2 Basic Command Syntax

A basic command has the following syntax:

```
<basic command>      ::= [<path>]<command> [<parameter>]… <CR>
<path>               ::= [\]<command\>[<command>\]…
<command>            ::= <command name> | ..
<parameter>          ::= <spaces> <keyword>=<value> | ?
<value>              ::= <integer> |
                         <choice> |
                         <IP address> |
                         <string> |
                         <MAC address> |
                         <NSAP address> |
                         <time> |
                         <date> |
                         <KLM> |
                         <portList> |
                         <port>

<NSAP address>     ::= <area address>:<system id>:<selector>
<portList>         ::= <port>[,<port>]..
<areaAddressList>  ::= <area address>[,<area address>]...

where:

<spaces>       is a string of one or more ASCII spaces;

<integer>      is a decimal integer in the range [m:n], where the values m and n are
               context-dependent;

<choice>       is a literal string, whose permissible values and their significance are
               context-dependent and may be obtained by using the help ("?") parameter;

<IP address>   is an IP address of the form ddd.ddd.ddd.ddd,  where d is a decimal digit.
               Leading zeroes in each ddd may be omitted;

<string>       is a string of graphical ASCII characters, excluding quotation marks (").
               If the string contains one or more spaces, then it MUST be enclosed in
               quotation marks. The maximum length of the string is context-dependent;

<MAC address>  is exactly 12 hexadecimal digits;

<time>         is a time-of-day of the form hh:mm:ss, where h, m and s are decimal digits;
```

```
<date>         is a date of the form dd/mm/yy, where d, m and y are decimal digits;
<KLM>          is a string of the form k.l.m, where k is a decimal digit in the range
               [1:3], l is a decimal digit in the range [1:7], and m is a decimal digit
               in the range [1:3].
<port>         is a decimal integer;
<area address> is a hexadecimal string;
<system id>    is a hexadecimal string;
<selector>     is a hexadecimal string;
```

The Help Command

The help command **?** will display all available commands at the current level, each with a short description. E.g. typing **?** at the root level will list the commands which are available at this level:

```
ONSCLI>?

*** current menu path:
<root>

*** valid commands:
Device:     Device configuration
Ports:      Port properties
Bridge:     Bridge/Spanning Tree Protocol settings
Router:     Router configuration
Security:   Security settings
Statistics: Performance monitoring and statistics
Services:   Utility functions
Alarms:     Current alarms and alarm history
Do's:        Quality of service
Running:    Show Running Config
Exit:       Exit from ONSCLICommand Hierarchy
```

In the command hierarchy, the lowest level is represented by a basic command with one or more parameters.

The ONS 15302 supports remote management solutions by the means of Telnet and SNMP .The possibilities as regards connectivity can be rather advanced for the ONS 15302 so the only explained solution in this document is when directly connected the management-port (MNGT). For more information please refer the *Cisco ONS 15302 Installation and Operations Guide* (Release 2.0).

To achieve one of the above mentioned management solutions it is necessary to assign an IP-address, subnet-mask and if required a default-gateway address must be defined.

System Mode

In ONS 15302 R2.0 an additional management mode, system mode is added.The System mode has two options, ip and ipunnumbered.

```
ONSCLI>...\Management-Configuration\sys ?

Usage:
   System-Mode
[SYSTEM-MODE=<ip|ipunnumbered>]
```

System Mode - IP

```
ONSCLI>...\Management-Configuration\sys sys=ip
Change management configuration, are you sure? (y/n)?
```

Example 1 Assign an IP-address:

If system mode is ip the command for IP configuration is:

```
ONSCLI>Device\Management-Configuration\Management-Port\IP-Configuration
IP-ADDRESS=193.69.136.104, SUBNET-MASK=255.255.255.0.
```

System Mode - IP Unnumbered

```
ONSCLI>...\Management-Configuration\sys sys=ipunnum
Change management configuration, are you sure? (y/n)?
```

Example 2 Assign an IP-address:

If system mode is ipunnumbered the command for IP configuration is:

```
ONSCLI>Device\Management-Configuration\IP-Configuration IP-ADDRESS=193.69.136.104,
SUBNET-MASK=255.255.255.0.
```

Example 7-3 Displays the IP Configuration

ONSCLI\Device\Management-Configuration\IP-Management-Port\IP-Configuration

Example 7-3 displays the current management interface information in the following manner:

```
IP-ADDRESS:193.69.136.104
SUBNET-MASK: 255.255.255.0
DEFAULT-GATEWAY: 193.69.136.54
```

If the help parameter (**?**) is supplied, then all other parameters are ignored and the basic command usage is displayed.

Table entries are accessed by introducing an additional command level giving access to the entire table. At this lowest level, the **Add** command (with the index and required table entries as parameters) can be used to add an element to the table and the **Edit** command can be used to replace an existing element in the table (if these operations are permitted on the table).

Similarly the **Remove** command (with the entry index as a parameter) can be used to remove an existing element from the table if this is permitted.

The **Show** command (with an entry index value as a parameter) displays the specified table entry. If no parameter is supplied with the **Show** command, the current contents of the entire table is displayed.

ONSCLI Error Messages

This section describes ONSCLI error messages.

SNMP Errors

The general ONSCLI output string for SNMP errors is **MIB access error**. Additional SNMP error information might be printed depending on the return code (Table 7-6).

Table 7-6 Additional ONSCLI SNMP Error Messages

Error Message (Output String)	Description
No Such Object	Scalar or table entry not found
End Of MIB View	End of table reached
No Creation	Creation of new entry failed
Not Writable	Accessed instance write protected
Wrong Length	Wrong specified field length
Wrong Value	Wrong value used for specified field
Inconsistent Value	Wrong value used for specified field
Resource Unavailable	Instance status not free for update
General Error	No additional error info
No Write To CDB	Write to Flash failed
Instance Exists	Table entry already exists

Input Errors

Error messages due to mistyping or incorrect ONSCLI input format are shown in Table 7-7.

Table 7-7 ONSCLI Input Error Messages

Error Message (Output String)	Description
Unknown parameter specification	Input parameter incorrectly specified
Ambiguous parameter specification	Parameter value out of range
Multiple parameter specification	Input parameter specified twice
Missing parameter specification	Mandatory parameter missing
Incompatible parameter specification	Wrong combination of parameters
Missing value	Wrong formatted or empty input value
Invalid integer value	Wrong input integer value
Invalid choice value	Input value (set element name) not found
Invalid length of string value of	Input string too long
Badly-formed string value of	Input string incorrectly formatted
Invalid IP address	IP address incorrectly formatted
Invalid length of hex string	Length of hex string not according to input requirement
Invalid character in hex string	Hex value used to define a digit is out of range.
Invalid escape sequence in string	'\0' value detected inside the string
Bad value	Incorrectly formatted input value
Integer out of range	Input integer value is not within limits.
List too long	List of integers longer than 10
Badly-formed list	Incorrect integer value found in integer list
Table empty	No entries found in SNMP table

Table 7-7 ONSCLI Input Error Messages (continued)

Error Message (Output String)	Description
Element not in table	Specified entry not found in SNMP table
This command is not available in this release	Command not supported
No modification parameters found	Modification command with no modification values received

ONSCLI Menu Structure

The complete ONSCLI command hierarchy for ONS 15302 is describes in Chapter 8, "ONSCLI Command Hiearchy.".

ONSCLI Command Hierarchy

The complete ONSCLI command Hierarchy for ONS 15302 shown in this chapter.

Tip Each basic command is shaded, and is marked by a number that refers to the appropriate line in the parameter description table, Table 8-1.

Note Blank columns in the parameter description table are reserved for future commands with their parameters.

The complete names of both commands and parameter keywords are shown in Table 8-1. Optional parameters are enclosed in square brackets. For clarity, parameter command keywords are written in capital letters, and lengthy commands are shown on several lines.

The order of parameters (keyword and value pairs) is not significant. The help command **?** will display all available commands at the current level, each with a short description.

8.1 Menu Tree

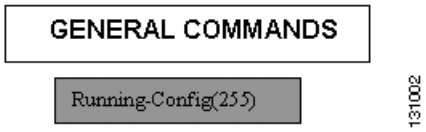
This section displays all available commands of the ONS 15302 in a graphical version and it also describes the following main commands and sub commands:

- General Commands
- Device
- Ports
- Bridge
- Security
- Statistics
- Services
- Alarms

8.1.1 General Commands

General commands are shown in Figure 8-1.

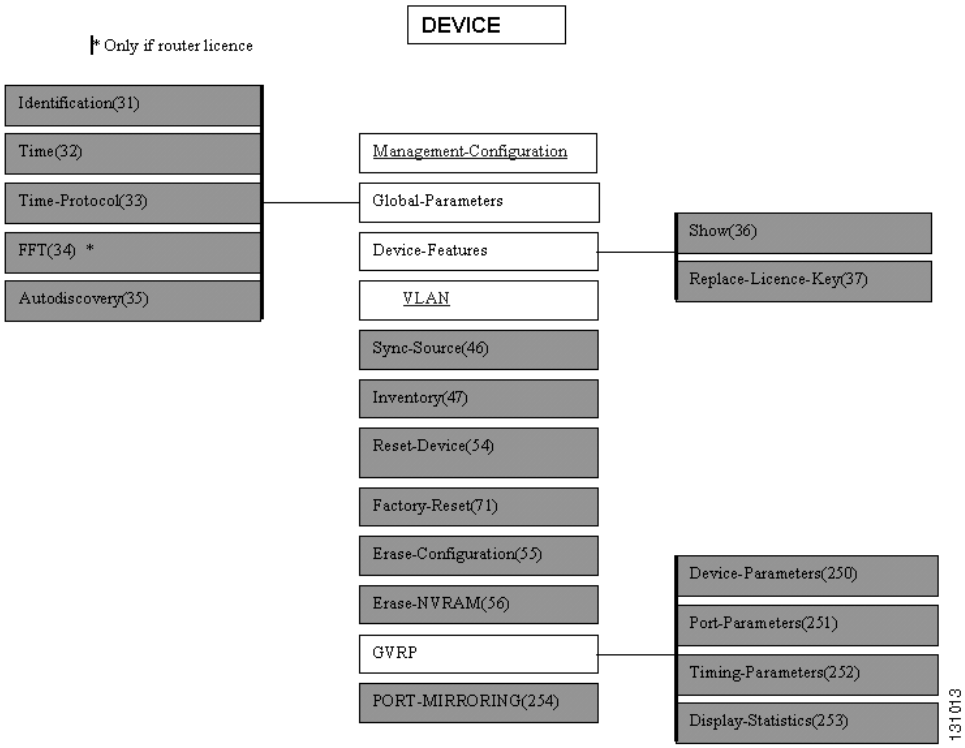
Figure 8-1 General Commands - ONSCLI



8.1.2 Device Commands

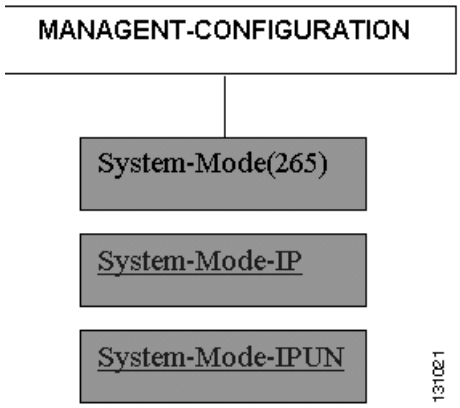
Device commands are shown in Figure 8-2.

Figure 8-2 Device commands - ONSCLI



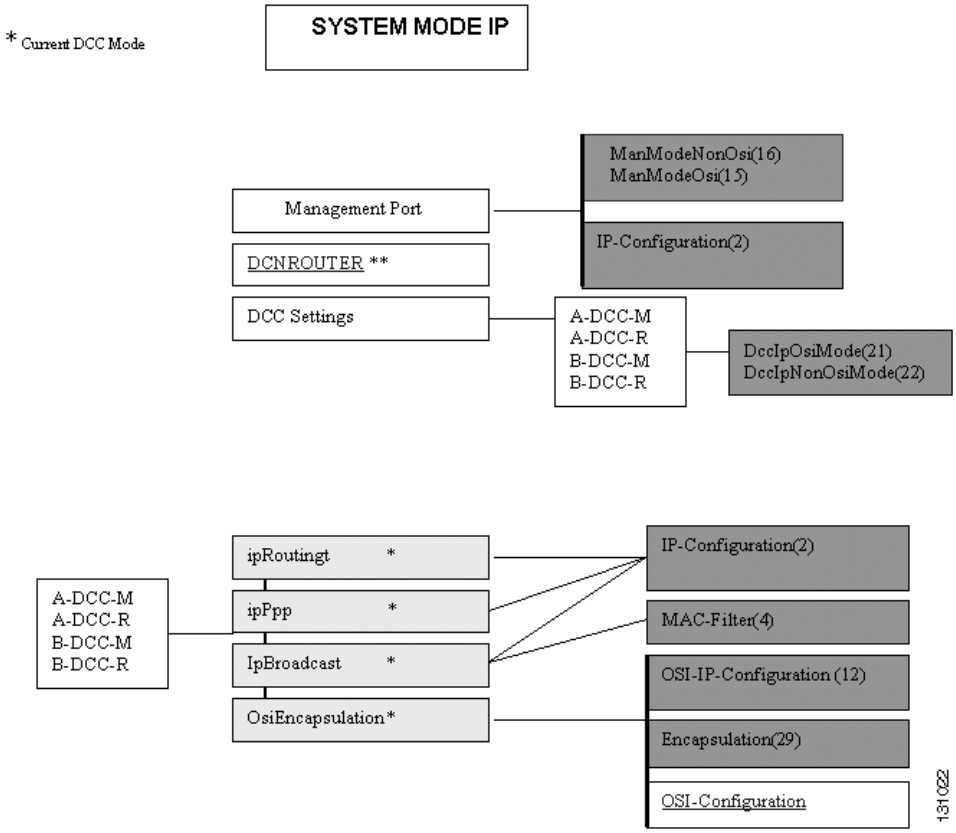
Management Configuration commands are shown in Figure 8-3.

Figure 8-3 Management Configuration commands - ONSCLI



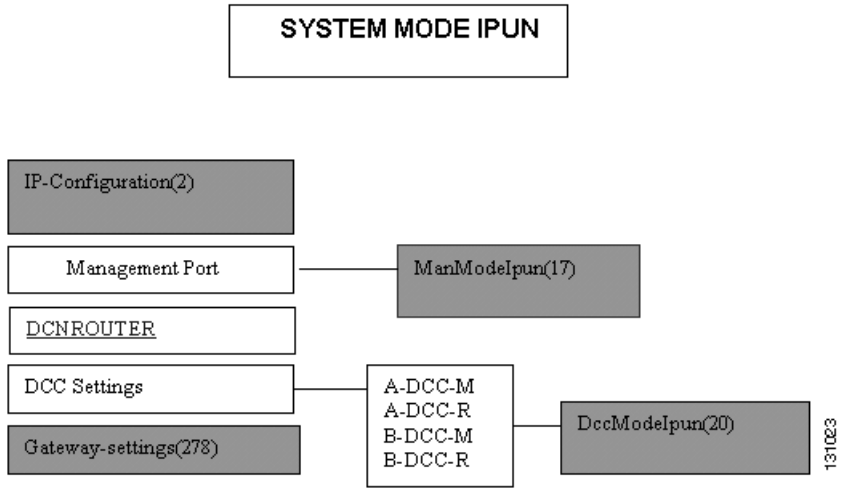
System Mode IP commands are shown in Figure 8-4.

Figure 8-4 System Mode IP - ONSCLI



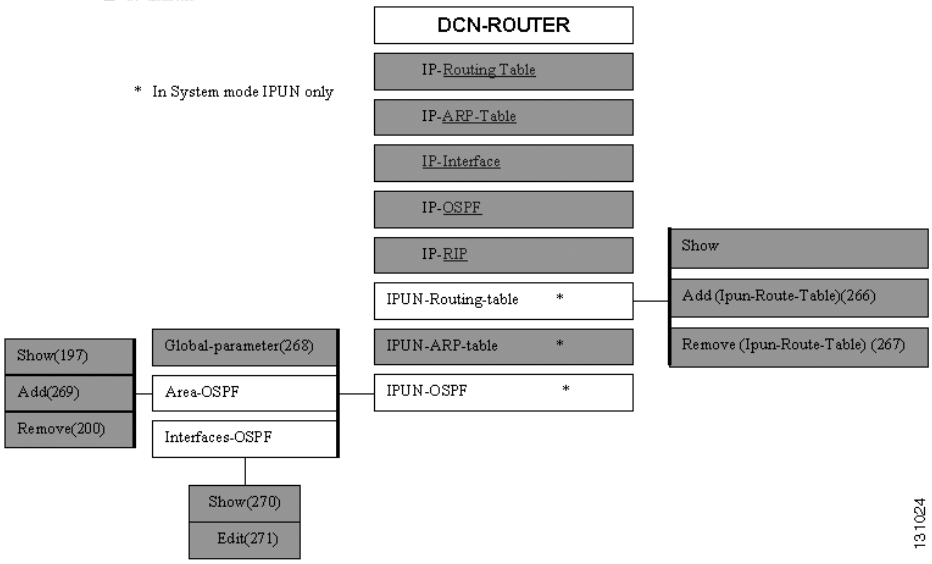
System Mode IP Unnumbered are shown in Figure 8-5.

Figure 8-5 System Mode IP Unnumbered commands - ONSCLI



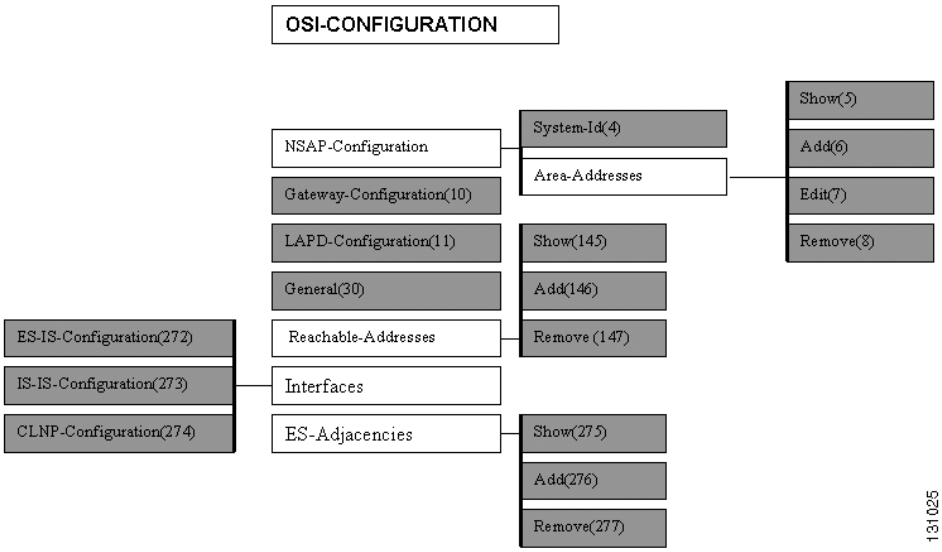
DCN Router commands are shown in Figure 8-6.

Figure 8-6 DCN Router commands - ONSCLI



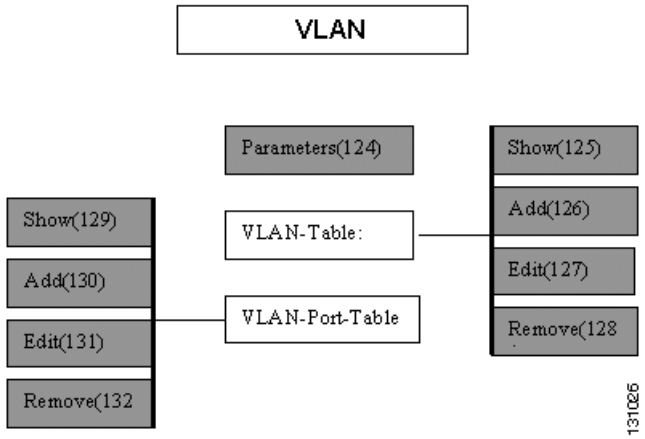
OSI Configuration commands are shown in Figure 8-7.

Figure 8-7 OSI Configuration commands - ONSCLI



VLAN commands are shown in Figure 8-8.

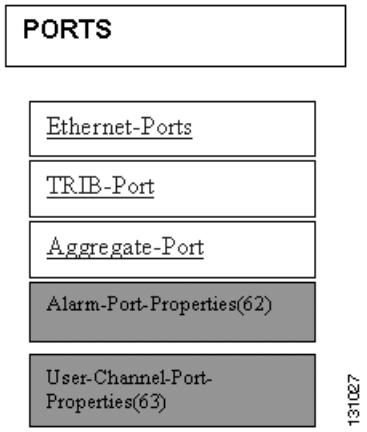
Figure 8-8 VLAN commands - ONSCLI



8.1.3 Ports Commands

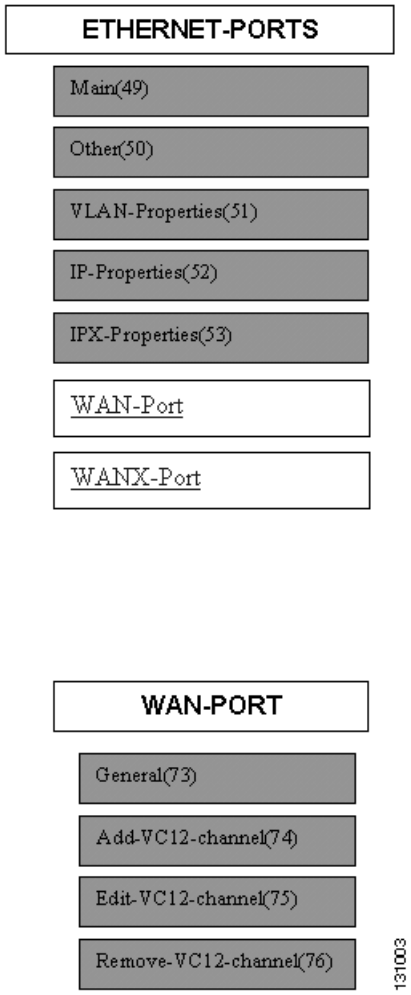
Ports commands are shown in Figure 8-9.

Figure 8-9 Ports commands - ONSCLI



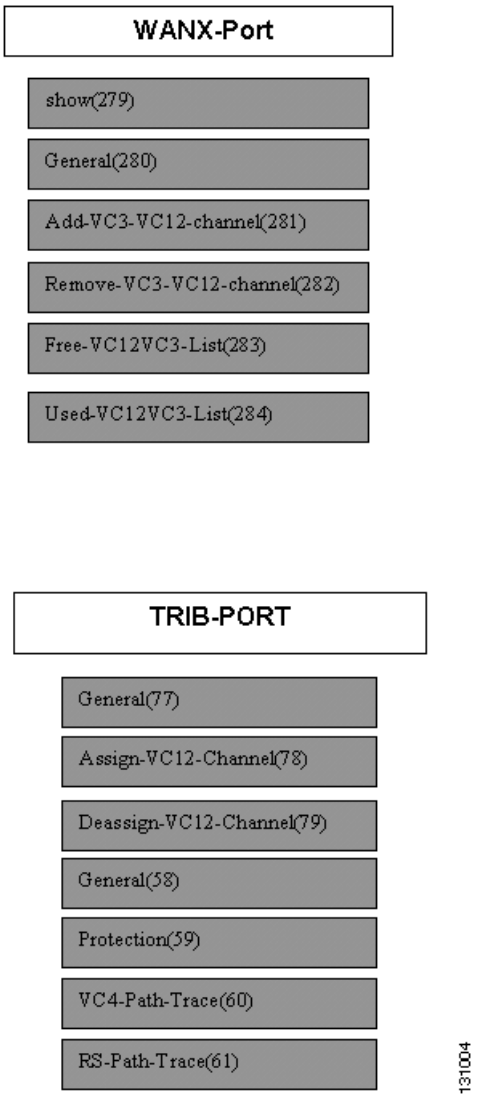
Ethernet- and WAN ports commands are shown in Figure 8-10.

Figure 8-10 Ethernet- and WAN ports commands - ONSCLI



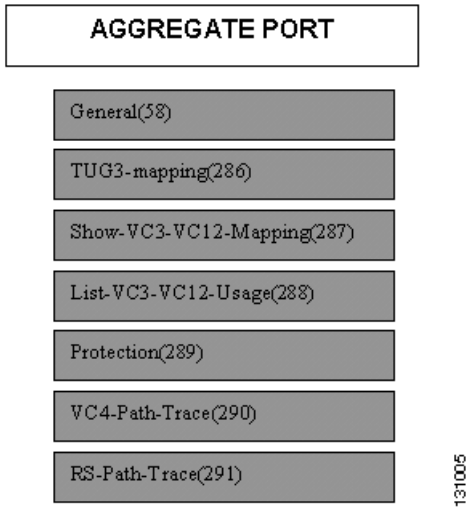
WANX and Tributary port commands are shown in Figure 8-11.

Figure 8-11 WANX and Trib port commands - ONSCLI



Aggregate ports commands are shown in Figure 8-12.

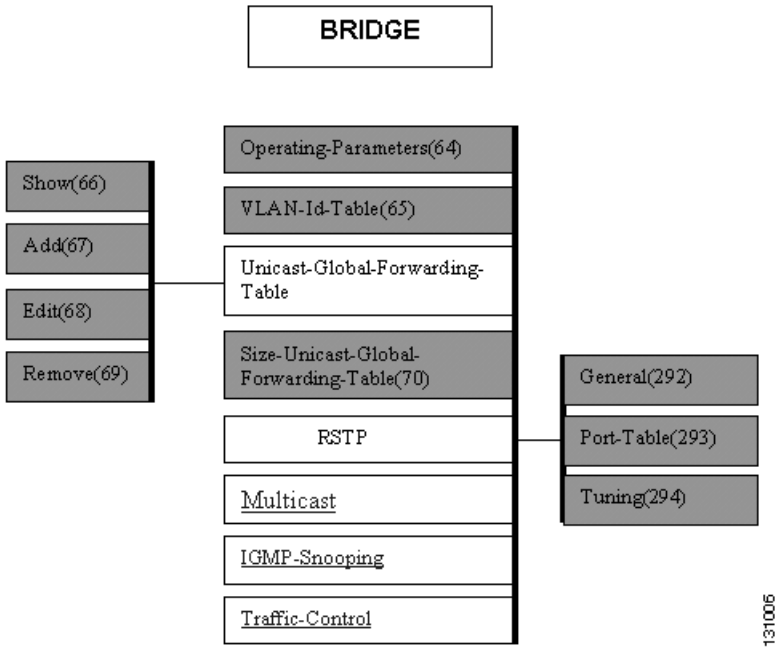
Figure 8-12 Aggregate ports commands - ONSCLI



8.1.4 Bridge Commands

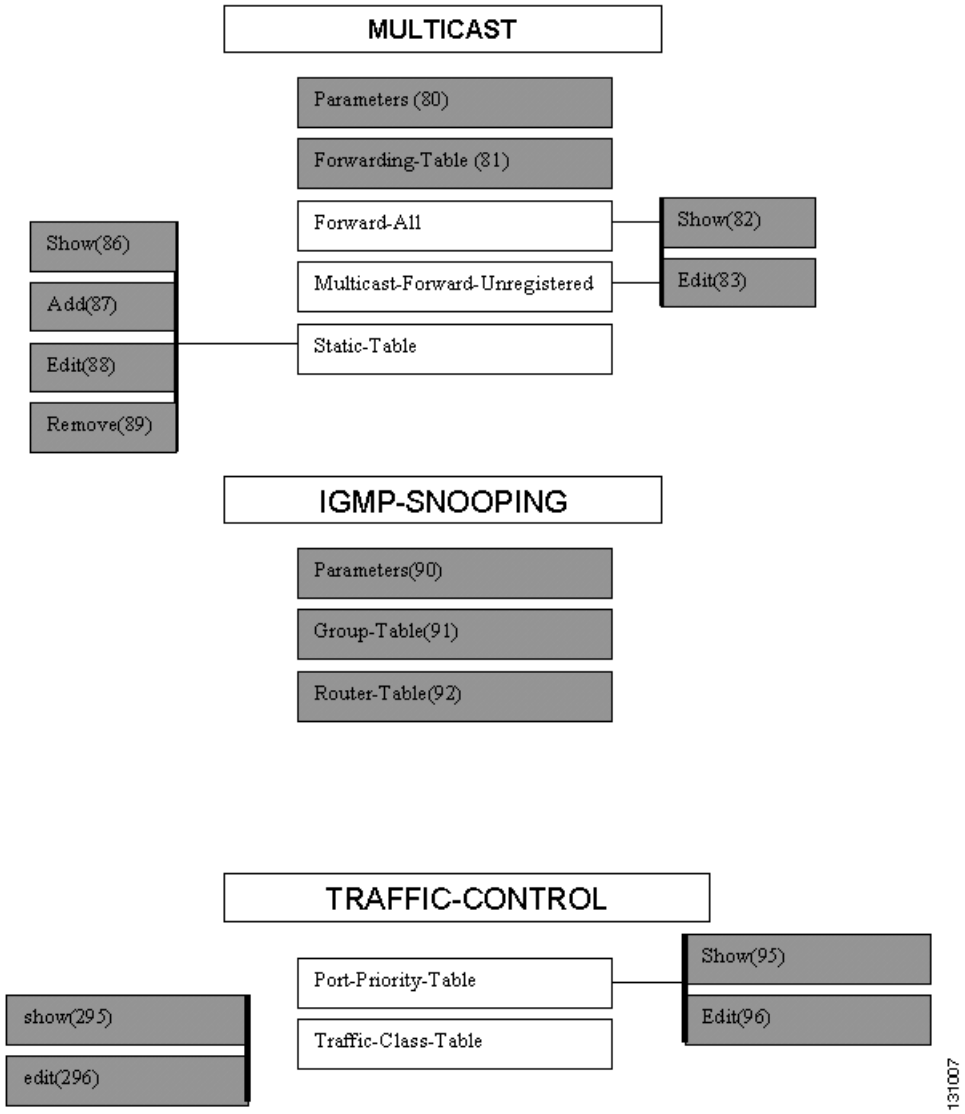
Bridge commands are shown in Figure 8-13.

Figure 8-13 Bridge commands - ONSCLI



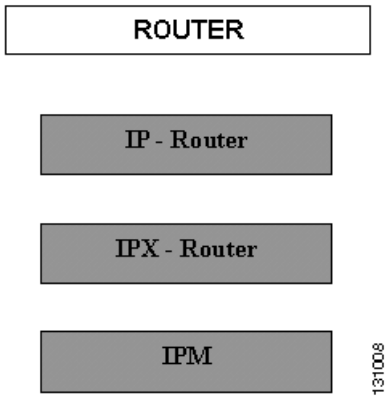
Multicast, IGMP Snooping and Traffic Control commands are shown in Figure 8-14.

Figure 8-14 Multicast, IGMP Snooping and Traffic Control commands - ONSCLI



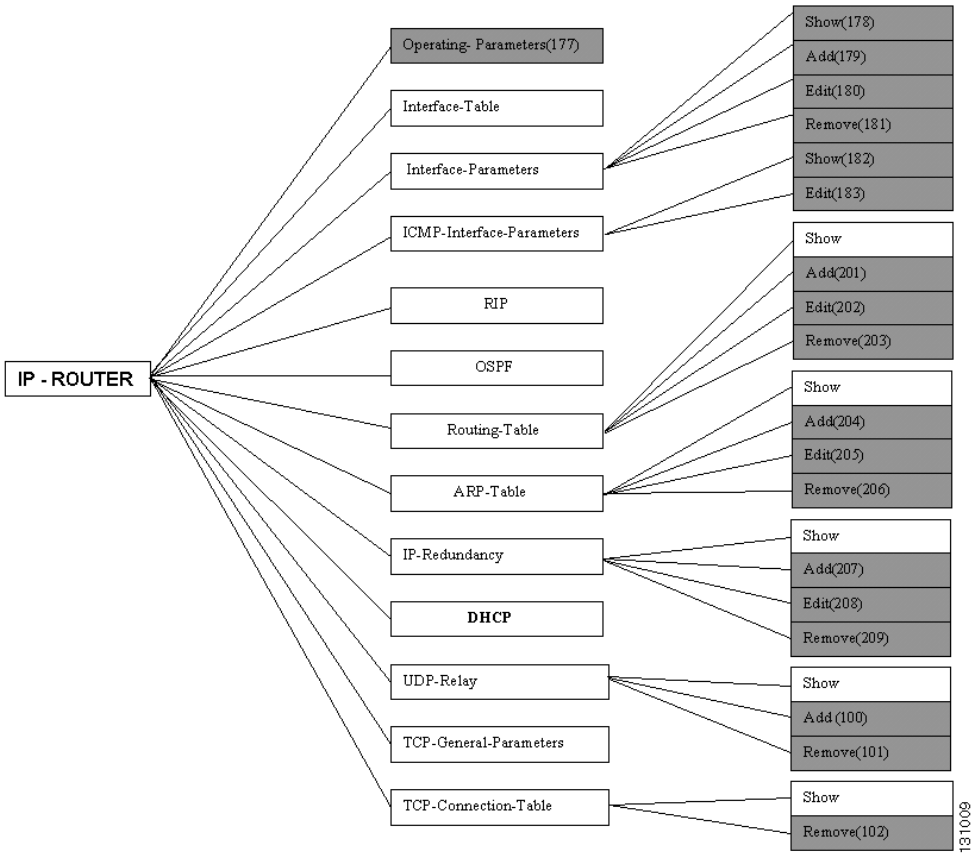
Router commands are shown in Figure 8-15.

Figure 8-15 Router commands - ONSCLI



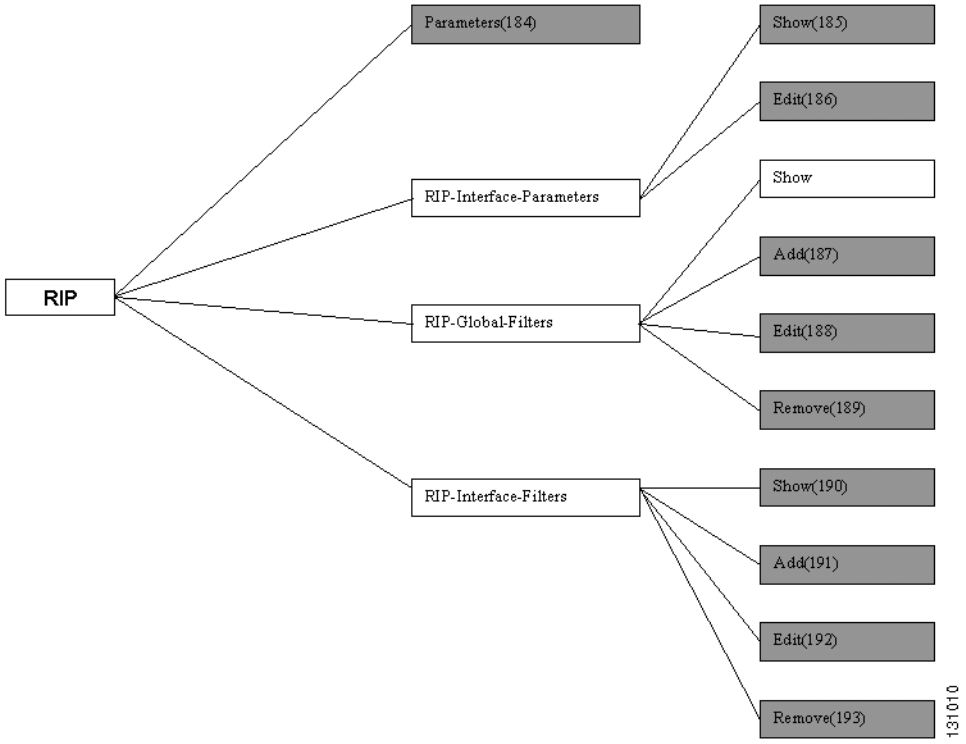
IP Router command are shown in Figure 8-16.

Figure 8-16 IP Router commands - ONSCLI



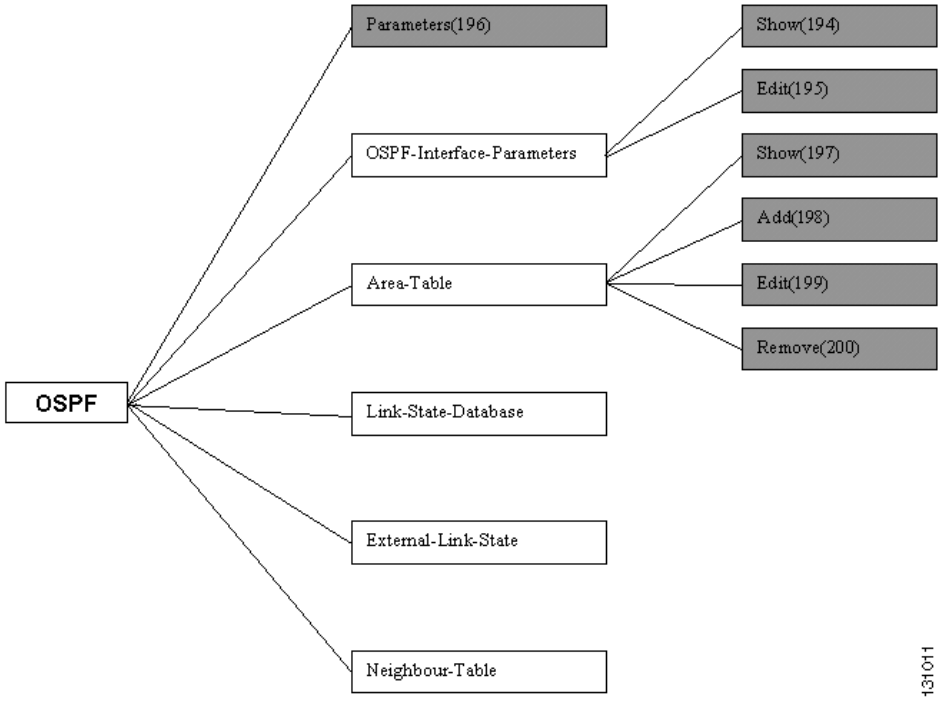
RIP commands are shown in Figure 8-17.

Figure 8-17 RIP commands - ONSCLI



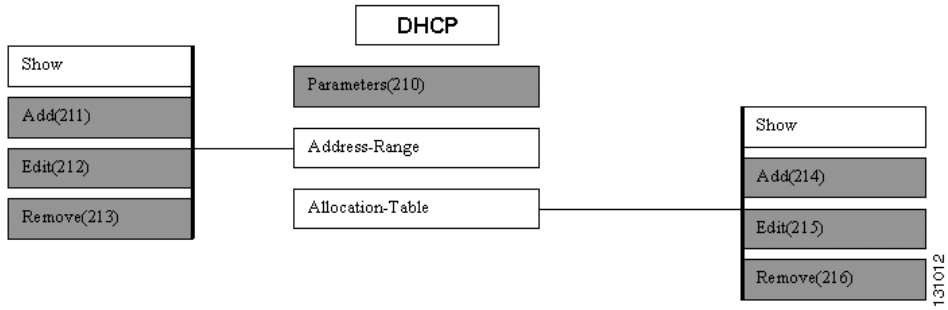
OSPF commands are shown in Figure 8-18.

Figure 8-18 OSPF commands - ONSCLI



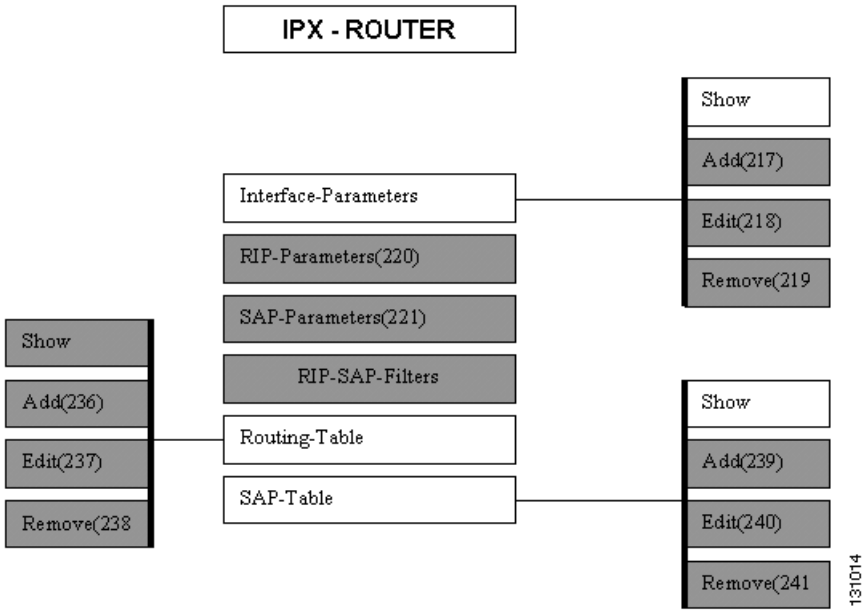
DHCP commands are shown in Figure 8-19.

Figure 8-19 DHCP commands - ONSCLI



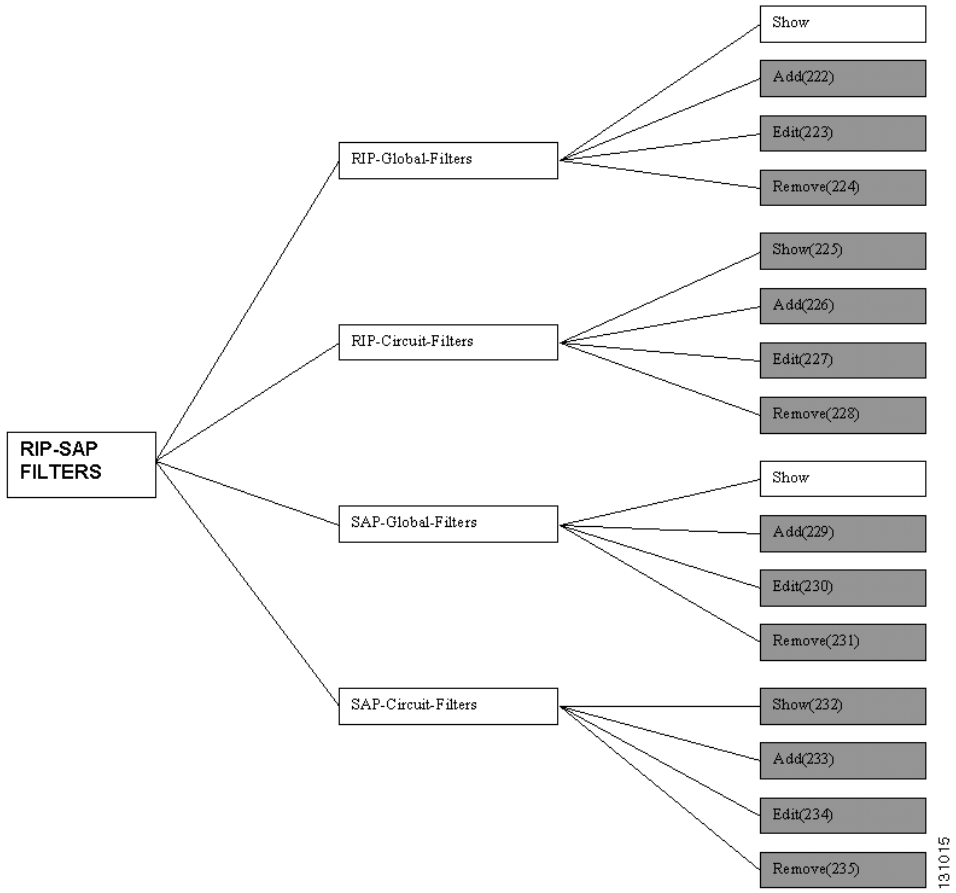
IPX commands are shown in Figure 8-20.

Figure 8-20 IPX commands - ONSCLI



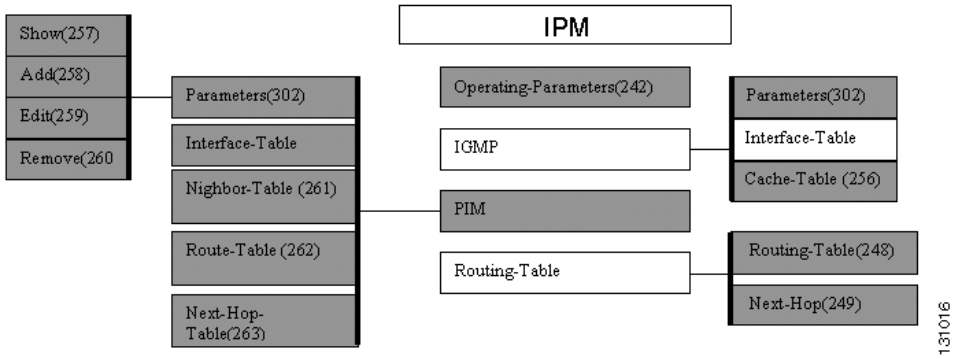
RIP-SAP Filters commands are shown in Figure 8-21.

Figure 8-21 RIP-SAP Filters commands - ONSCLI



IPM commands are shown in Figure 8-22.

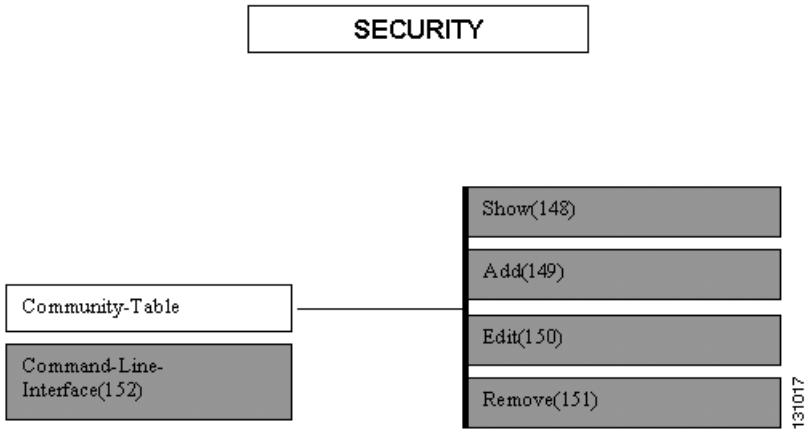
Figure 8-22 IPM commands - ONSCLI



8.1.5 Security Commands

Security commands are shown in Figure 8-23.

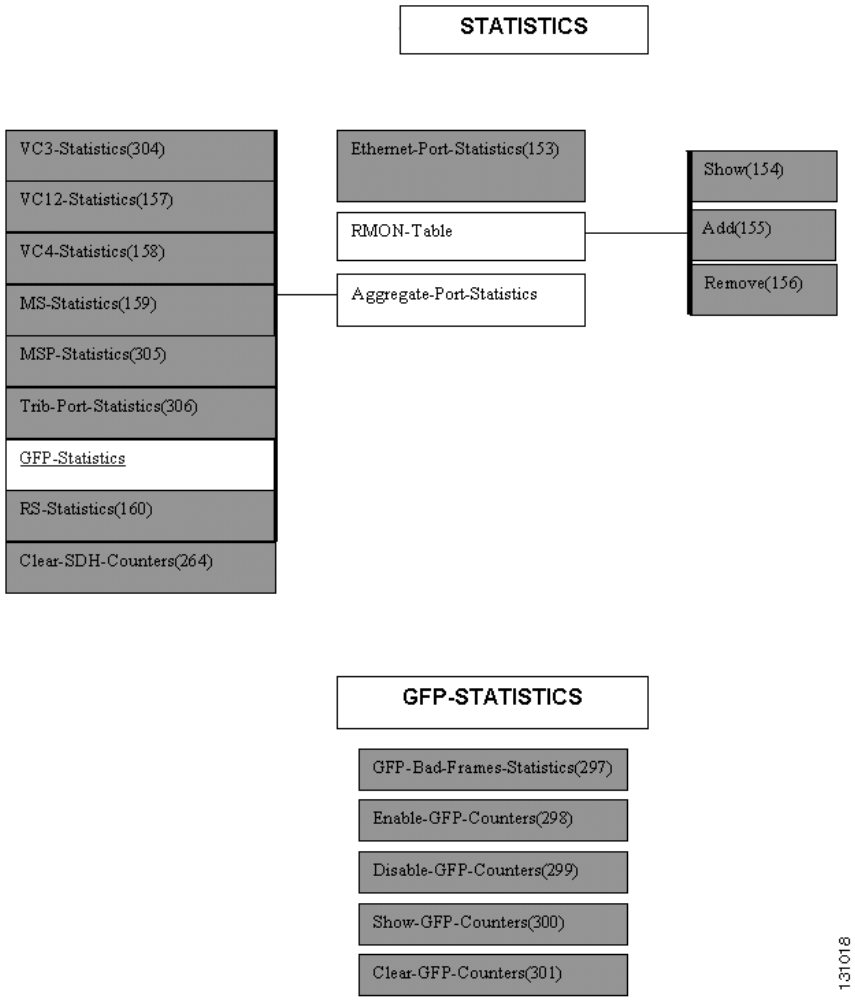
Figure 8-23 Security commands - ONSCLI



8.1.6 Statistics Commands

Statistics commands are shown in Figure 8-24.

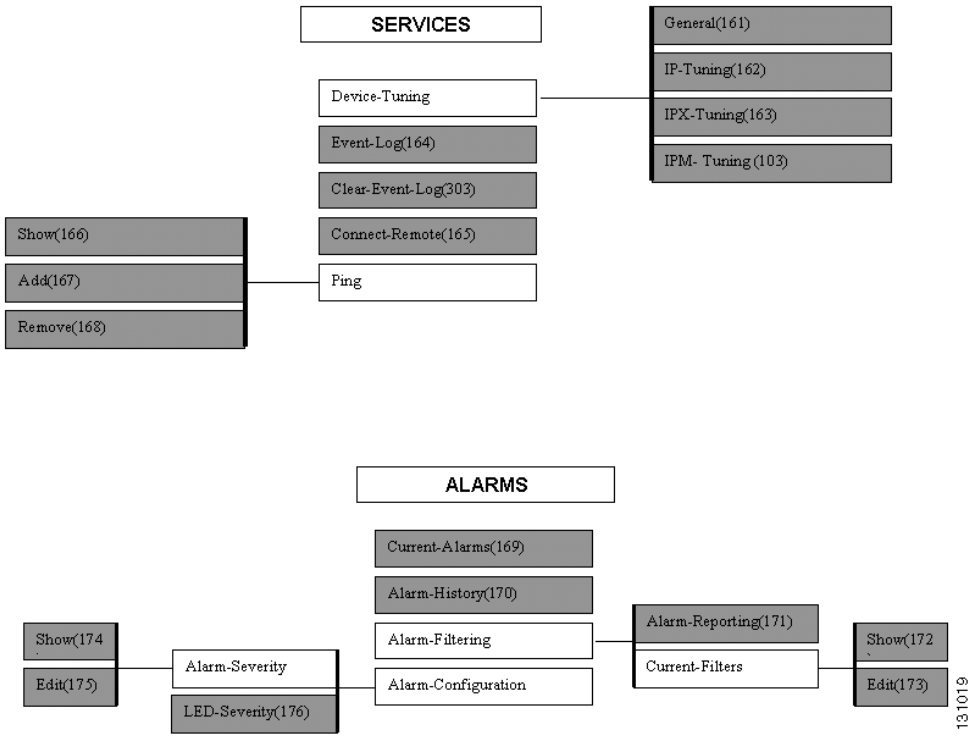
Figure 8-24 Statistics commands - ONSCLI



8.1.7 Services and Alarms Commands

Service and Alarms commands are shown in Figure 8-25.

Figure 8-25 Service and Alarms commands - ONSCLI



QoS commands are shown in Figure 8-26.

Figure 8-26 QoS commands - ONSCLI

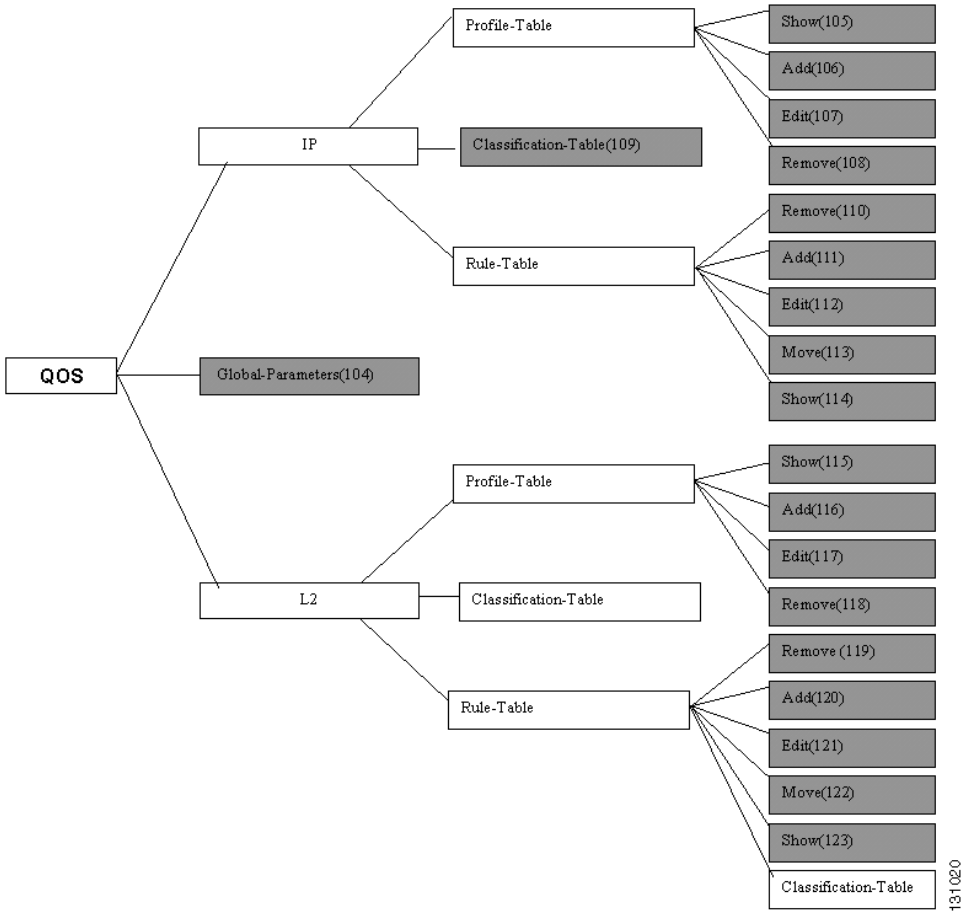


Table 8-1 ONS 15302 - ONSCLI Command and Parameters

Command		Parameters
1.	IP-ConfigurationRouter	[IP-ADDRESS=<IP address>] [SUBNET-MASK=<IP address>]
2.	IP-Configuration	[IP-ADDRESS=<IP address>] [SUBNET-MASK=<IP address>] [DEFAULT-GATEWAY=<IP address>]
3.	MAC-Filter	[MAC-FILTER-SWITCH=<enabled | disabled>]
4.	System-Id	[SYSTEM-ID=<NSAP system ID - hexString[2:16]>] [NSEL=<NSAP selector - hexString[2:2]>]
5.	Show	<none>
6.	Add	AREA-ADDRESS=<NSAP area address - hexString[4:36]>
7.	Edit	INDEX=<integer value 1:3> AREA-ADDRESS=<NSAP area address - hexString[4:36]>
8.	Remove	INDEX=<integer value 1:3>
9.	ModeOsi	MODE=<notUsed|ip|clnp|ipAndClnp>>

Table 8-1 ONS 15302 - ONSCLI Command and Parameters (continued)

Command		Parameters
10.	Gateway-Configuration	[NSAP-ADDRESS=<NSAP address - hexString[6:40]>] [STATUS=<enabled|disabled>]
11.	LAPD-Configuration	[LAPD-ROLE=<network|user>][TOGGLE-CR=<enabled|disabled>][N201=<integer value 0:65535>]
12.	OSI-IP-ConfigurationRouter	[OSI-IP-ADDRESS=<IP address>] [OSI-SUBNET-MASK=<IP address>]
13.	DccIpNonOsiMode	[MODE=<notUsed|ipBroadcast|ipRouting|ipPppCrc16|ipPppCrc32>]
14.	IP-Configuration	[IP-ADDRESS=<IP address>] [SUBNET-MASK=<IP address>]
15.	ManModeOsi	[[MODE=<notUsed|ip|clnp|ipAndClnp>]
16.	ManModeNonOsi	[[MODE=<notUsed|ip|>]
17.	ManModeIpun	[MODE=<notUsed|ip>]
18.	OSI-IP-ConfigurationBridge	[OSI-IP-ADDRESS=<IP address>] [OSI-SUBNET-MASK=<IP address>] [OSI-DEFAULT-GATEWAY=<IP address>]
19.	OsiMode	[MODE=<notUsed|ip|clnp|ipAndClnp>]
20.	DccModeIpun	[[MODE=<notUsed|ipPppCrc16|ipPppCrc32>]
21.	DccIpOsiMode	[MODE=<notUsed|ipBroadcas|ipRouting|osiEncapsulation|ipPppCrc16|ipPppCrc32>]
22.	DccIpNonOsiMode	[MODE=<notUsed|ipBroadcast|ipRouting|ipPppCrc16|ipPppCrc32>]
23.	Add	IP-ADDRESS=<IP address> IF-NUM=<integer value> SUBNET-MASK=<IP address> [DEFAULT-GATEWAY=<IP address>]
24.	Edit	IP-ADDRESS=<IP address> [IF-INDEX=<integer value>] [SUBNET-MASK=<IP address>] [DEFAULT-GATEWAY=<IP address>]
25.	Remove	IP-ADDRESS=<IP address>
26.	Show	IP-ADDRESS=<IP address>
27.	PPP-IP-Routing	[IP-ADDRESS=<IP address>][SUBNET-MASK=<IP address>]
28.	PPP-IP-Routing	[IP-ADDRESS=<IP address>] [SUBNET-MASK=<IP address>] [DEFAULT-GATEWAY=<IP address>]
29.	Encapsulation	[HELLO-INTERVAL=<integer value 0:65535>]
30.	General	[L1-LSP=<integer value 0:1492>][L2-LSP=<integer value 0:1492>][IS-MODE=<disabled|is|l1Is|l2Is>]
31.	Identification	[NAME=<string[0:160]>] [LOCATION=<string[0:160]>] [CONTACT=<string[0:160]>]
32.	Time	[TIME=<hh:mm:ss>] [DATE=<yyyy-mm-dd>]

Table 8-1 ONS 15302 - ONSCLI Command and Parameters (continued)

Command		Parameters
33.	Time-Protocol	[SERVER-IP-ADDRESS=<IP address>] [SYNC-INTERVAL=<integer value 0:2147483647>] [UTC-DELTA=<integer value -720:720>]
34.	FFT	[IP-FASTFORWARDING=<enable|disable>] [IPX-FASTFORWARDING=<enable|disable>]
35.	Autodiscovery	[STATUS=<enabled|disabled>] [TRAP-FREQUENCY=<integer value 0:2147483647>]
36.	Show	<none>
37.	Replace-Licence-Key	LICENCE-KEY=<string[1:50]>
38.	Show	[VLAN-NUMBER=<integer>]
39.	Add	NAME=<string> [ADDRESS-TYPE=<default|reserve>] [TAG=<integer>]
40.	Edit	VLAN-NUMBER=<integer> [NAME=<string>] [ADDRESS-TYPE=<default|reserve>] [TAG=<integer>]
41.	Remove	VLAN-NUMBER=<integer>
42.	Show	[VLAN-NUMBER=<integer>]
43.	Add	VLAN-NUMBER=<integer> ETHERNET-PORTS=<portList> [TAGGING=<enable|disable>]
44.	Edit	VLAN-NUMBER=<integer> ETHERNET-PORTS =<portList> TAGGING=<enable|disable>
45.	Remove	VLAN-NUMBER=<integer> ETHERNET-PORTS =<portList>
46.	Sync-Source	[ADMIN-SOURCE=<Trib1|Trib2|Trib3|Trib4|Trib5|Trib6|Trib7|Trib8|Trib9|Trib10| Trib11|Trib12|Aggr1|Aggr2|Active|Local|External>]
47.	Inventory	<none>
48.	Remote-Device-Identification	[REMOTE-DEVICE=<IP address>]
49.	Main	[ETHERNET-PORT=<integer value 1:8>] [SPEED-ADMIN-MODE=<10M|100M>] [ADMINISTRATIVE-STATUS=<on|off>] [DESCRIPTION=<string[0:64]>] [DUPLEX-ADMIN-MODE=<none|half|full>] [PHYSICAL-ADDRESS-ASSIGNMENT=<default|reserve>][AUTONEGOTIATION-MODE=<enabled|disabled>]
50.	Other	[ETHERNET-PORT=<integer value 1:8>] [BACK-PRESSURE-MODE=<enable|disable>][FLOW-CONTROL-MODE=<on|off|autoNegotiation>]
51.	VLAN-Properties	[ETHERNET-PORT=<integer value 1:8>]
52.	IP-Properties	[ETHERNET-PORT=<integer value 1:8>]
53.	IPX-Properties	[ETHERNET-PORT=<integer value 1:8>]

Table 8-1 ONS 15302 - ONSCLI Command and Parameters (continued)

Command		Parameters
54.	Reset-Device	<none>
55.	Erase-Configuration	<none>
56.	Erase-NVRAM	<none>
57.	Tributary-Port-Properties	[TRIBUTARY-PORT=<port>] [DESCRIPTION=<string>] [ADMINISTRATIVE-STATUS=<enable|disable>] [MODE=<TRA|PRA>] [LOOP-MODE=<NONE|LL2|LL3>] [PATH-TRACE=<enabled|disabled>] [EXPECTED-TI=<string>] [TRANSMIT-TI=<string>] [MONITORING-STATUS=<ENABLED|DISABLED>]
58.	General	AGGREGATE-PORT=<integer value 1:2> [ADMINISTRATIVE-STATUS=<enable|disable>] [DESCRIPTION=<string[0:64]>] [CONNECTED-TO=<string[0:160]>]
59.	Protection	[MSP-STATUS=<enabled|disabled>] [PROTECTION-TYPE=<unidirectional|bidirectional>] [REVERTING-STATUS=<enabled|disabled>] [WAIT-TO-RESTORE-TIME=<integer>][SWITCHING-COMMAND=<clear|exercise|manualSwitchToProtecting|manualSwitchToWorking| forcedSwitchToProtecting|forcedSwitchToWorking|lockoutProtection>]
60.	VC4-Path-Trace	[PATH-TRACE=<enabled|disabled>] [EXPECTED-TI=<string[1:15]>] [HEX-EXPECTED-TI=<string[2:44]>][TRANSMIT-TI=<string[1:15]>] [HEX-TRANSMIT-TI=<string[2:44]>]
61.	RS-Path-Trace	AGGREGATE-PORT=<integer value 1:2> [PATH-TRACE=<enabled|disabled>] [EXPECTED-TI=<string[1:15]>][HEX-EXPECTED-TI=<string[2:44]>] [TRANSMIT-TI=<string[1:15]>] [HEX-TRANSMIT-TI=<string[2:44]>]
62.	Alarm-Port-Properties	[ALARM-PORT=<integer value 1:4>] [MODE=<enabled|disabled>] [DESCRIPTION=<string[0:64]>] [TRIGGERED-WHEN=<opens|closes>]
63.	User-Channel-Port-Properties	[ADMINISTRATIVE-STATUS=<enabled|disabled>] [DESCRIPTION=<string[0:64]>] [AGGREGATE-PORT=<SDH-A|SDH-B|ACTIVE>] [DATA-RATE=<sync64000|async19200>]
64.	Operating-Parameters	[FORWARDING-TABLE-AGING-TIME=<integer value 10:1000000>][BRIDGE-MODE=<normal|provider>]
65.	VLAN-Id-Table	ETHERNET-PORT=<integer value 1:8>
66.	Show	<none>

Table 8-1 ONS 15302 - ONSCLI Command and Parameters (continued)

Command		Parameters
67.	Add	VLAN-TAG-ID=<integer value 1:4000>MAC-ADDRESS=<MAC address - hexString[12:12]>ETHERNET-PORT=<integer value 1:8>[STATUS=<permanent|deleteOnReset>]
68.	Edit	VLAN-TAG-ID=<integer value 1:4000>MAC-ADDRESS=<MAC address - hexString[12:12]>ETHERNET-PORT=<integer value 1:8>[STATUS=<permanent|deleteOnReset>]
69.	Remove	VLAN-TAG-ID=<integer value 1:4000>MAC-ADDRESS=<MAC address - hexString[12:12]>ETHERNET-PORT=<integer value 1:8>
70.	Size-Unicast-Global-Forwarding-Table	<none>
71.	Factory-Reset	<none>
72.	Show	[IP-ADDRESS=<IP address>]
73.	General	[WAN-PORT=<integer value 5:8>] [PATH-TRACE=<enabled|disabled>][EXPECTED-TI=<string [1:15]>][HEX-EXPECTED-TI=<string[2:44]>][TRANSMIT-TI=<string[1:15]>][HEX-TRANSMIT-TI=<string[2:44]>][CHANNEL-TI=<integer value 0:50>]
74.	Add-VC12-channel	WAN-PORT=<integer value 5:8> [KLM=<K.L.M - integer value 1:3.integer value 1:7.integer value 1:3>][ADMIN-STATUS=<enabled|disabled>] [NUMBER-TO-ADD=<integer value 1:50>] [SORT-MODE=<LEX|G707>]
75.	Edit-VC12-channel	[WAN-PORT=<integer value 5:8>] [WAN-CHANNEL=<integer value 1:50>] [ADMIN-STATUS=<enabled|disabled>]
76.	Remove-VC12-channel	WAN-PORT=<integer value 5:8> [NUMBER-TO-REMOVE=<integer value 1:50>]
77.	General	[[TRIB-PORT=<integer value 1:12>] [DESCRIPTION=<string[0:64]>] [ADMINISTRATIVE-STATUS=<enable|disable>][MODE=<TRA|PRA>] [LOOP-MODE=<NONE|LL2|LL3>][PATH-TRACE=<enabled|disabled>] [EXPECTED-TI=<string[1:15]>] [HEX-EXPECTED-TI=<string[2:44]>][TRANSMIT-TI=<string[1:15]>] [HEX-TRANSMIT-TI=<string[2:44]>]
78.	Assign-VC12-Channel	TRIB-PORT=<integer value 1:12> [KLM=<K.L.M - integer value 1:3.integer value 1:7.integer value 1:3>][NUMBER-TO-ADD=<integer value 1:12>] [SORT-MODE=<LEX|G707>]
79.	Deassign-VC12-Channel	TRIB-PORT=<integer value 1:12> [NUMBER-TO-REMOVE=<integer value 1:12>]
80.	Parameters	[MULTICASTING-ENABLE=<true|false>]

Table 8-1 ONS 15302 - ONSCLI Command and Parameters (continued)

Command		Parameters
81.	Forwarding-Table	[[VLAN-TAG-ID=<integer value 1:4000>] [MULTICAST-ADDRESS=<MAC address - hexString[12:12]>]
82.	Show	[[VLAN-TAG-ID=<integer value 0:8>]
83.	Edit	[VLAN-TAG-ID=<integer value 1:4000> [STATIC-PORTS=<integer value 0:8,...>] [FORBIDDEN-PORTS=<integer value 0:8,...>]
84.	Show	[[VLAN-TAG-ID=<integer value 1:4000>]
85.	Edit	[VLAN-TAG-ID=<integer value 1:4000> [STATIC-PORTS=<integer value 0:8,...>] [FORBIDDEN-PORTS=<integer value 0:8,...>]
86.	Show	[[VLAN-TAG-ID=<integer value 1:4000>] [MULTICAST-ADDRESS=<MAC address - hexString[12:12]>]
87.	Add	[VLAN-TAG-ID=<integer value 1:4000> MULTICAST-ADDRESS=<MAC address - hexString[12:12]> [EGRESS-PORTS=<integer value 0:8,...>] [FORBIDDEN-PORTS=<integer value 0:8,...>][STATUS=<other|invalid|permanent|deleteOnReset|deleteOnTimeout>]
88.	Edit	[VLAN-TAG-ID=<integer value 1:4000> MULTICAST-ADDRESS=<MAC address - hexString[12:12]>[EGRESS-PORTS=<integer value 0:8,...>] [FORBIDDEN-PORTS=<integer value 0:8,...>][STATUS=<other|invalid|permanent|deleteOnReset|deleteOnTimeout>]
89.	Remove	[VLAN-TAG-ID=<integer value 1:4000> MULTICAST-ADDRESS=<MAC address - hexString[12:12]>
90.	Parameters	[IGMP-ENABLE=<true|false>] [HOST-AGING-TIME-IGMP=<integer value>] [ROUTER-AGING-TIME-IGMP=<integer value>]
91.	Group-Table	[VLAN-TAG-ID =<integer value 1:4000>] [PORT=<integer value 1:8>] [MULTICAST-ADDRESS=<MAC address - hexString[12:12]>]
92.	Router-Table	[VLAN-TAG-ID =<integer value 1:4000>] [PORT=<integer value 1:8>]
93.	Show	[PORT=<integer value 1:8>] [TYPE-OF-PROTOCOL=<notUsed|preDefined|ethUserDefined|llcUserDefined>][PROTOCOL=<NotUsed|Other|IP|RESERVED|IPX_RAW|IPX_Ethernet|IPX_LLC|IPX_SNAP|DECNET|DECLAT|NETBIOS|APPLETALK|XNS|SNA>]

Table 8-1 ONS 15302 - ONSCLI Command and Parameters (continued)

Command		Parameters
94.	Edit	PORT=<integer value 1:8> TYPE-OF-PROTOCOL=<notUsed|preDefined|ethUserDefined|llcUserDefined>PROTOCOL=<NotUsed|Other|IP|RESERVED|IPX_RAW|IPX_Ethernet|IPX_LLC|IPX_SNAP|DECNET|DECLAT|NETBIOS|APPLETALK|XNS|SNA>[DEFAULT-PRIOR=<integer value 0:7>] [TRAFFIC-CLASSES=<integer value 1:8>]
95.	Show	[PORT=<integer value 1:8>]
96.	Edit	PORT=<integer value 1:8>[DEFAULT-PRIOR=<integer value 0:7>]
97.	Priority-Group-Table	[PORT=<integer value 1:8>]
98.	Port-Table	[VLAN-TAG=<integer value 1:4000>] [ETHERNET-PORT=<integer value 1:8>] [STATUS=<true|false>]
99.	Forced-SW-Version-Table	[VLAN-TAG=<integer value 1:4000>] [STATE=<STPCompatibility|NormalRSTP>]
100.	Add	UDP-DEST-PORT=<integer value> SOURCE-IP-ADDRESS=<IP address> DEST-IP-ADDRESS=<IP address>
101.	Remove	UDP-DEST-PORT=<integer value> SOURCE-IP-ADDRESS=<IP address> DEST-IP-ADDRESS=<IP address>
102.	Remove	LOCAL-IP-ADDR=<IP address> LOCAL-PORT=<integer value 0:65535> REMOTE-IP-ADDR=<IP address>REMOTE-PORT=<integer value 0:65535>
103.	IPM- Tuning	[FFT-ENTRIES-AFTER-RESET=<integer value>] [NEIGBOUR-ENTRIES-AFTER-RESET=<integer value>][ROUTE-ENTRIES-AFTER-RESET=<integer value>] [INTERFACE-ENTRIES-AFTER-RESET=<integer value>][IGMP-ENTRIES-AFTER-RESET=<integer value>]
104.	Global-Parameters	[POLICY-ENABLE=<true|false>]
105.	Show	[INDEX=<integer value 1:256>] [DETAILED=<False|True>]
106.	Add	[DESCRIPTION=<string[0:40]>] PROFILE-TYPE=<minBandwidth|bandwidthGuarantee|minDelay|minDelayPerSession>RATE(Kbps)=<integer value> [MAX-SESSION=<integer value>] [NEW-TOS-OR-DSCP=<integer value 0:255>][CHANGE-TOS-OR-DSCP=<true|false>] [BURST-SIZE=<integer value>] [NEW-VPT=<integer value 0:7>]

Table 8-1 ONS 15302 - ONSCLI Command and Parameters (continued)

Command		Parameters
107.	Edit	INDEX=<integer value 1:256> [DESCRIPTION=<string[0:40]>][PROFILE-TYPE=<minBandwidth|bandwidthGuarantee|minDelay|minDelayPerSession>] [RATE(Kbps)=<integer value>] [MAX-SESSION=<integer value>] [NEW-TOS-OR-DSCP=<integer value 0:255>][CHANGE-TOS-OR-DSCP=<true|false>] [BURST-SIZE=<integer value>] [NEW-VPT=<integer value 0:7>]
108.	Remove	INDEX=<integer value 1:256>
109.	Classification-Table	[TOS=<true|false>] [PROTOCOL=<true|false>] [SRC-IP-BIT-MASK=<integer value 0:32>] [DST-IP-BIT-MASK=<integer value 0:32>] [SOURCE-PORT-PROTOCOL=<true|false>] [DESTINATION-PORT-PROTOCOL=<true|false>] [INPUT-PORTS=<true|false>]
110.	Remove	INDEX=<integer value>
111.	Add	INDEX=<integer value> [DESCRIPTION=<string[0:40]>] [TOS=<integer value 0:255>] [PROTOCOL=<NotDefined|TCP|UDP>] [SRC-IP=<IP address>] [SRC-MASK=<integer value 0:32>] [DST-IP=<IP address>] [DST-MASK=<integer value 0:32>] [SRC-PORT=<integer value 0:65535>] [DST-PORT=<integer value 0:65535>] [CONDITION=<equal|notEqual|bigger|smaller>] [IN-PORT=<integer value 0:8,...>] [ACTION=<block|blockAndTrap|permit>] [PROFILE-POINTER=<integer value 1:256>] [OUT-PORT=<integer value 0:8,...>] [STATUS=<Active|NotActive>]
112.	Edit	INDEX=<integer value> [DESCRIPTION=<string[0:40]>] [TOS=<integer value 0:255>] [PROTOCOL=<NotDefined|TCP|UDP>] [SRC-IP=<IP address>] [SRC-MASK=<integer value 0:32>] [DST-IP=<IP address>] [DST-MASK=<integer value 0:32>] [SRC-PORT=<integer value 0:65535>] [DST-PORT=<integer value 0:65535>] [CONDITION=<equal|notEqual|bigger|smaller>] [IN-PORT=<integer value 0:8,...>] [ACTION=<block|blockAndTrap|permit>] [PROFILE-INDEX=<integer value 1:256>] [OUT-PORT=<integer value 0:8,...>] [STATUS=<Active|NotActive>]
113.	Move	INDEX=<integer value> NEW-INDEX=<integer value>
114.	Show	[INDEX=<integer value>] [DETAILED=<False|True>]
115.	Show	[INDEX=<integer value 1:256>] [DETAILED=<False|True>]

Table 8-1 ONS 15302 - ONSCLI Command and Parameters (continued)

Command		Parameters
116.	Add	[DESCRIPTION=<string[0:40]>] PROFILE-TYPE=<minBandwidth|bandwidthGuarantee> RATE(Kbps)=<integer value> [BURST-SIZE=<integer value>] [NEW-VPT=<integer value 0:7>]
117.	Edit	INDEX=<integer value 1:256> [DESCRIPTION=<string[0:40]>] [PROFILE-TYPE=<minBandwidth|bandwidthGuarantee>] [RATE(Kbps)=<integer value>][BURST-SIZE=<integer value>] [NEW-VPT=<integer value 0:7>]
118.	Remove	INDEX=<integer value 1:256>
119.	Remove	INDEX=<integer value>
120.	Add	INDEX=<integer value> IN-PORT=<integer value 0:8,...> OUT-PORT=<integer value 0:8,...> [DESCRIPTION=<string[0:40]>] [ACTION=<block|blockAndTrap|permit>] [PROFILE-INDEX=<integer value 1:256>][STATUS=<Active|NotActive>]
121.	Edit	INDEX=<integer value> [DESCRIPTION=<string[0:40]>] [IN-PORT=<integer value 0:8,...>] [ACTION=<block|blockAndTrap|permit>] [PROFILE-INDEX=<integer value 1:256>] [OUT-PORT=<integer value 0:8,...>] [STATUS=<Active|NotActive>]
122.	Move	INDEX=<integer value> NEW-INDEX=<integer value>
123.	Show	[INDEX=<integer value>] [DETAILED=<False|True>]
124.	Parameters	[VLAN-SUPPORTED-TYPE-AFTER-RESET=<perPort|perProtAndPort>]
125.	Show	[IF-INDEX.=<integer value>]
126.	Add	NAME=<string[0:20]>[ADDRESS-TYPE=<default|reserve>] [TAG=<integer value 1:4000>]
127.	Edit	IF-INDEX=<integer value> [NAME=<string[0:20]>] [ADDRESS-TYPE=<default|reserve>]
128.	Remove	IF-INDEX=<integer value>
129.	Show	[IF-INDEX=<integer value>]
130.	Add	IF-INDEX=<integer value> ETHERNET-PORTS=<integer value 1:8,...> [TAGGING=<enable|disable>][EGRESS-FORBIDDEN=<true|false>]
131.	Edit	IF-INDEX=<integer value> ETHERNET-PORTS=<integer value 1:8,...> [TAGGING=<enable|disable>][EGRESS-FORBIDDEN=<true|false>]

Table 8-1 ONS 15302 - ONSCLI Command and Parameters (continued)

Command		Parameters
132.	Remove	IF-INDEX=<integer value> ETHERNET-PORTS=<integer value 1:8,...>
133.	Show	[INDEX=<integer value>]
134.	Add	PROTOCOL-NAME=<string[0:20]> PROTOCOL-NUM=<string[4:4]> [PROTOCOL-MASK=<string[4:4]>]
135.	Edit	INDEX=<integer value> [PROTOCOL-NAME=<string[0:20]>] [PROTOCOL-NUM=<string[4:4]>] [PROTOCOL-MASK=<string[4:4]>]
136.	Remove	INDEX=<integer value>
137.	Show	[VLAN-IF-INDEX.=<integer value>]
138.	Add	TYPE-OF-PROTOCOL=<preDefined_protocols|ethUserDefined_protocols> NAME=<string[0:20]>[PROTOCOL=<|Other|IP|IPX_RAW|IPX_Ethernet|IPX_LLC|IPX_SNAP|DECNET|NETBIOS|SNA>][ADDRESS-TYPE=<default|reserve>] [TAG=<integer value 1:4000>]If TYPE-OF-PROTOCOL = ethUserDefined_protocols, PROTOCOL input not needed(taken from vlanEthUserDefProtEntry)
139.	Edit	VLAN-IF-INDEX.=<integer value> [NAME=<string[0:20]>] [ADDRESS-TYPE=<default|reserve>]
140.	Remove	VLAN-NUMBER=<integer value>
141.	Show	[VLAN-NUMBER=<integer value>]
142.	Add	VLAN-NUMBER=<integer value> ETHERNET-PORTS=<integer value 1:8,...> [TAGGING=<enable|disable>][EGRESS-FORBIDDEN=<true|false>]
143.	Edit	VLAN-NUMBER=<integer value> ETHERNET-PORTS=<integer value 1:8,...> [TAGGING=<enable|disable>][EGRESS-FORBIDDEN=<true|false>]
144.	Remove	VLAN-NUMBER=<integer value> ETHERNET-PORTS=<integer value 1:8,...>
145.	Show	<none>
146.	Add	PREFIX=<NSAP area address - hexString[4:36]>
147.	Remove	PREFIX=<NSAP area address - hexString[4:36]>
148.	Show	[MANAGER=<IP address>]
149.	Add	MANAGER=<IP address> COMMUNITY=<string[1:20]> ACCESS=<readOnly|readWrite|super>TRAPS=<enable|disable>
150.	Edit	MANAGER=<IP address> COMMUNITY=<string[1:20]> [ACCESS=<readOnly|readWrite|super>][TRAPS=<enable|disable>]

Table 8-1 ONS 15302 - ONSCLI Command and Parameters (continued)

Command		Parameters
151.	Remove	MANAGER=<IP address> COMMUNITY=<string[1:20]>
152.	Command-Line-Interface	[XXXCLI-PASSWORD=<string[6:12]>] [TELNET-PASSWORD=<string[6:12]>] [DISPLAY-LINES=<integer value 0:999>] [ALLOW-MESSAGES=<YES|NO>]
153.	Ethernet-Port-Statistics	ETHERNET-PORT=<integer value 1:8>
154.	Show	<none>
155.	Add	ETHERNET-PORT=<integer value 1:8>
156.	Remove	ETHERNET-PORT=<integer value 1:8>
157.	VC12-Statistics	KLM=<K.L.M - integer value 1:3.integer value 1:7.integer value 1:3>
158.	VC4-Statistics	<none>
159.	MS-Statistics	AGGREGATE-PORT=<integer value 1:2>
160.	RS-Statistics	AGGREGATE-PORT=<integer value 1:2>
161.	General	[BRIDGE-FORWARDNG-TABLE-AFTER-RESET=<integer value>] [RMON-LOG-TABLE-AFTER-RESET=<integer value>] [GVRP-VLAN-ENTRIES-AFTER-RESET=<integer value>][RULES-POLICY-MIB-AFTER-RESET=<integer value>] [PROFILES-POLICY-MIB-AFTER-RESET=<integer value>] [VLAN-ENTRIES-AFTER-RESET=<integer value>][ERROR-REPORT-LEVEL=<integer value>]
162.	IP-Tuning	[IP-RIP-MAX-ENTRIES-AFTER-RESET=<integer value>] [ARP-FORWARDING-MAX-ENTRIES-AFTER-RESET=<integer value>] [IP-FFT-MAX-ENTRIES-AFTER-RESET=<integer value>] [DHCP-MAX-CONNECTION-AFTER-RESET=<integer value>] [IP-FFT-UPPER-LIMIT=<integer value 0:100>][IP-FFT-LOWER-LIMIT=<integer value 0:100>]
163.	IPX-Tuning	[IPX-RIP-MAX-ENTRIES-AFTER-RESET=<integer value>] [IPX-SAP-MAX-ENTRIES-AFTER-RESET=<integer value>] [IPX-FFT-MAX-ENTRIES-AFTER-RESET=<integer value>][IPX-FFT-UPPER-LIMIT=<integer value 1:100>][IPX-FFT-LOWER-LIMIT=<integer value 0:100>]
164.	Event-Log	<none>
165.	Connect-Remote	<none>
166.	Show	[IP-ADDRESS=<IP address>]
167.	Add	IP-ADDRESS=<IP address> [COUNT=<integer value 1:2147483647>] [SIZE=<integer value>] [TIMEOUT=<integer value 0:3600000>] [DELAY=<integer value 0:3600000>]
168.	Remove	IP-ADDRESS=<IP address>
169.	Current-Alarms	<none>

Table 8-1 ONS 15302 - ONSCLI Command and Parameters (continued)

Command		Parameters
170.	Alarm-History	<none>
171.	Alarm-Reporting	[ALARM-REPORTING=<enabled|disabled>]
172.	Show	[OBJECT-TYPE=<DEVICE|GFP|VCATLC|ALARM|TRIB|SPI|RST|MST|MSP|VC-4|AU-4|TU-12|VC-12|TU-3|VC-3>]
173.	Edit	OBJECT-TYPE=<DEVICE|GFP|VCATLC|ALARM|TRIB|SPI|RST|MST|MSP|VC-4|AU-4|TU-12|VC-12|TU-3|VC-3>[ALARM-REPORTING=<enabled|disabled>][PORT=<integer value 1:12>][PERSISTENCY-ON=<integer value 0:255>][PERSISTENCY-OFF=<integer value 0:255>][SD-THRESHOLD=<integer value 6:9>][AIS=<enabled|disabled>][RDI=<enabled|disabled>]

Table 8-1 ONS 15302 - ONSCLI Command and Parameters (continued)

Command		Parameters
174.	Show	[ALARM-ID=<unknownAlarmId|hwFail|losSy|aux|losTx|aisRx|lfaRx|lfaTx|los|lof| td|tf|exc|deg|csf|tim|ais|rdi|msp|lom|lop|uneq|plm|fan|temp|unass| wanDelay|syncHoldOver|seqFail|plc|tlc|degFcs|degtHec|upm|clos|lfd| exm|pfm|sqnc|sqm|loa|loaNoTraf|acMstTimeout|rsAckTimeout| eosMultiple|eosMissing|sqNonCont|sqMultiple|sqOor|gidErr|ctrlOor| lcasCrc|nonLcas|mnd|fopr|plcr|tlcr|plct|tlct|info|lanOn|lanOff| rxOverflowHWFault|txOverflowHWFault|routeTableOverflow| resetRequired|endTftp|abortTftp|startTftp|faultBackUp|mainLinkUp| ipxRipTblOverflow|ipxSapTblOverflow|facsAccessVoilation| autoConfigurationCompleted|forwardingTabOverflow| framRelaySwitchConnectionUp|framRelaySwitchConnectionDown| errorsDuringInit|vlanDynPortAdded|vlanDynPortRemoved| rsSDclientsTableOverflow|rsSDinactiveServer| rsIpZhrConnectionsTableOverflow|rsIpZhrReqStaticConnNotAccepted| rsIpZhrVirtualIpAsSource|rsIpZhrNotAllocVirtualIp| rsSnmpSetRequestInSpecialCfgState|rsPingCompletion| pppSecurityViolation|frDLCIStatudChange|papFailedCommunication| chapFailedCommunication|rsWSDRedundancySwitch| rsDhcpAllocationFailure|rlIgmpTableOverflow|rlPimTableOverflow| rlIpFftStnOverflow|rlIpFftSubOverflow|rlIpxFftStnOverflow| rlIpxFftSubOverflow|rlIpmFftOverflow|rlPhysicalDescriptionChanged| rldot1dStpPortStateForwarding|rldot1dStpPortStateNotForwarding| rlPolicyDropPacketTrap|rlPolicyForwardPacketTrap>]

Table 8-1 ONS 15302 - ONSCLI Command and Parameters (continued)

Command		Parameters
175.	Edit	ALARM-ID=<unknownAlarmId|hwFail|losSy|aux|losTx|aisRx|lfaRx|lfaTx|los|lof|td tf|exc|deg|csf|tim|ais|rdi|msp|lom|lop|uneq|plm|fan|temp|unass| wanDelay|syncHoldOver|seqFail|plc|tlc|degFcs|degtHec|upm|clos|lfd| exm|pfm|sqnc|sqm|loa|loaNoTraf|acMstTimeout|rsAckTimeout| eosMultiple|eosMissing|sqNonCont|sqMultiple|sqOor|gidErr|ctrlOor| lcasCrc|nonLcas|mnd|fopr|plcr|tlcr|plct|tlct|info|lanOn|lanOff| rxOverflowHWFault|txOverflowHWFault|routeTableOverflow| resetRequired|endTftp|abortTftp|startTftp|faultBackUp|mainLinkUp| ipxRipTblOverflow|ipxSapTblOverflow|facsAccessVoilation| autoConfigurationCompleted|forwardingTabOverflow| framRelaySwitchConnectionUp|framRelaySwitchConnectionDown| errorsDuringInit|vlanDynPortAdded|vlanDynPortRemoved| rsSDclientsTableOverflow|rsSDinactiveServer| rsIpZhrConnectionsTableOverflow|rsIpZhrReqStaticConnNotAccepted| rsIpZhrVirtualIpAsSource|rsIpZhrNotAllocVirtualIp| rsSnmpSetRequestInSpecialCfgState|rsPingCompletion| pppSecurityViolation|frDLCIStatudChange|papFailedCommunication| chapFailedCommunication|rsWSDRedundancySwitch| rsDhcpAllocationFailure|rlIgmpTableOverflow|rlPimTableOverflow| rlIpFftStnOverflow|rlIpFftSubOverflow|rlIpxFftStnOverflow| rlIpxFftSubOverflow|rlIpmFftOverflow|rlPhysicalDescriptionChanged| rldot1dStpPortStateForwarding|rldot1dStpPortStateNotForwarding| rlPolicyDropPacketTrap|rlPolicyForwardPacketTrap>ALARM-POINT=<unknownAlarmPoint|device|sdhPhysical|rst|mst| msp|au4|vc4|tu12| vc12|trib|aux|ethernet|wan|tu3|vc3|wanx|gfp|lcas|vcat>[SEVERITY=<critical|major|minor|warning>][DESCRIPTION=<string[0:160]>]
176.	LED-Severity	[CUSTOMER-LED-MIN-SEVERITY=<critical|major|minor|warning>][OPERATOR-LED-MIN-SEVERITY=<critical|major|minor|warning>]
177.	Operating- Parameters	[IP-REDUNDANCY-ADMIN-STATUS=<enable|disable>] [ARP-INACTIVE-TIMEOUT=<integer value>][ARP-PROXY=<enable|disable>] [ICMP-ERROR-MSG=<enable|disable>]
178.	Show	[IP-ADDRESS=<IP address>]

Table 8-1 ONS 15302 - ONSCLI Command and Parameters (continued)

Command		Parameters
179.	Add	IP-ADDRESS=<IP address> SUBNET-MASK=<IP address> IF-NUMBER=<integer value> [FWD-BROADCAST=<enable|disable>] [BROADCAST-TYPE=<ZERO-FILL|ONE-FILL>] [ARP-SERVER=<enable|disable>]
180.	Edit	IP-ADDRESS=<IP address> [SUBNET-MASK=<IP address>] [IF-NUMBER=<integer value>][FWD-BROADCAST=<enable|disable>] [BROADCAST-TYPE=<ZERO-FILL|ONE-FILL>][ARP-SERVER=<enable|disable>]
181.	Remove	IP-ADDRESS=<IP address>
182.	Show	[IP-ADDRESS=<IP address>]
183.	Edit	IP-ADDRESS=<IP address> [DESTINATION=<ALL-SYSTEMS-MULTICAST|LIMITED-BROADCAST>][MAX-INTERVAL=<integer value 4:1800>] [MIN-INTERVAL=<integer value 3:1800>] [LIFETIME=<integer value 4:9000>] [ADVERTISE=<enable|disable>] [PREFERENCE-LEVEL=<integer value>][DEFAULT-VALUES=<TRUE|FALSE>]
184.	Parameters	[ADMINISTRATIVE-STATUS=<enable|disable>] [LEAK-OSPF=<enable|disable>] [LEAK-STATIC=<enable|disable>]
185.	Show	[IP-ADDRESS=<IP address>]
186.	Edit	IP-ADDRESS=<IP address>[OUTGOING-RIP=<doNotSend|ripVersion1|rip1Compatible|ripVersion2|ripV1Demripv2Demand>][INCOMING-RIP=<rip1|rip2|rip1OrRip2|doNotRecieve>] [DEFAULT-METRIC=<integer value 0:15>][AUTO-SEND=<enable|disable>] [VIRTUAL-DISTANCE=<integer value>] [STATUS=<valid|invalid>]
187.	Add	TYPE=<input|output> NETWORK-ADDRESS=<IP address> NUM-MATCH-BITS=<integer value 1:32>ACTION=<deny|permit>
188.	Edit	TYPE=<input|output> NUMBER=<integer value> [NETWORK-ADDRESS=<IP address>] [NUM-MATCH-BITS=<integer value 1:32>] [ACTION=<deny|permit>]
189.	Remove	TYPE=<input|output> NUMBER=<integer value>
190.	Show	[IP-ADDRESS=<IP address>]
191.	Add	IP-ADDRESS=<IP address> TYPE=<input|output> NETWORK-ADDRESS=<IP address> NUM-MATCH-BITS=<integer value 1:32> ACTION=<deny|permit>

Table 8-1 ONS 15302 - ONSCLI Command and Parameters (continued)

Command		Parameters
192.	Edit	IP-ADDRESS=<IP address> TYPE=<input|output> NUMBER=<integer value> [NETWORK-ADDRESS=<IP address>] [NUM-MATCH-BITS=<integer value 1:32>] [ACTION=<deny|permit>]
193.	Remove	IP-ADDRESS=<IP address> TYPE=<input|output> NUMBER=<integer value>
194.	Show	[IP-ADDRESS=<IP address>]
195.	Edit	IP-ADDRESS=<IP address> [AREA-ID=<IP address>] [IF-TYPE=<broadcast|nbma|pointToPoint|pointToMultipoint>][ADMINISTRATIVE-STATUS=<enabled|disabled>] [PRIORITY=<integer value 0:255>] [HELLO-INTERVAL=<integer value 1:65535>] [ROUTER-DEAD-INTERVAL=<integer value 0:2147483647>][IF-AUTHENTICATION-KEY=<string[0:8] >] [AUTHENTICATION-TYPE=<none|password>][METRIC-VALUE=<integer value 0:65535>]
196.	Parameters	[ADMINISTRATIVE-STATUS=<enabled|disabled>] [ROUTER-ID=<IP address>] [LEAK-RIP=<enable|disable>][LEAK-STATIC=<enable|disable>] [LEAK-EXTERNAL=<enable|disable>]
197.	Show	[AREA-ID=<IP address>]
198.	Add	AREA-ID=<IP address> IMPORT-AS-EXTERN=<importExternal|importNoExternal|importNssa> [METRIC=<integer value 0:16777215>]
199.	Edit	AREA-ID=<IP address> [IMPORT-AS-EXTERN=<importExternal|importNoExternal|importNssa>][METRIC=<integer value 0:16777215>]
200.	Remove	AREA-ID=<IP address>
201.	Add	DEST-IP-ADDRESS=<IP address> DEST-SUBNET-MASK=<IP address> NEXT-HOP=<IP address>IF-NUMBER=<integer value> ROUTE-TYPE=<remote|reject> METRIC=<integer value>
202.	Edit	DEST-IP-ADDRESS=<IP address> DEST-SUBNET-MASK=<IP address> NEXT-HOP=<IP address>METRIC=<integer value>
203.	Remove	DEST-IP-ADDRESS=<IP address> DEST-SUBNET-MASK=<IP address> NEXT-HOP=<IP address>
204.	Add	IF-NUMBER=<integer value> IP-ADDRESS=<IP address> MAC-ADDRESS=<MAC address - hexString[0:320]>
205.	Edit	IF-NUMBER=<integer value> IP-ADDRESS=<IP address> MAC-ADDRESS=<MAC address - hexString[0:320]>
206.	Remove	IF-NUMBER=<integer value> IP-ADDRESS=<IP address>

Table 8-1 ONS 15302 - ONSCLI Command and Parameters (continued)

Command		Parameters
207.	Add	IF-IP-ADDRESS=<IP address> MAIN-ROUTER-IP-ADDRESS=<IP address> [POLL-INTERVAL=<integer value>][TIMEOUT=<integer value>]
208.	Edit	IF-IP-ADDRESS=<IP address> MAIN-ROUTER-IP-ADDRESS=<IP address> [OPERATIONAL-STATUS=<activelinactive>] [POLL-INTERVAL=<integer value>] [TIMEOUT=<integer value>]
209.	Remove	IF-IP-ADDRESS=<IP address> MAIN-ROUTER-IP-ADDRESS=<IP address>
210.	Parameters	[SERVER-ENABLE=<enable|disable>] [NEXT-SERVER-ADDRESS=<IP address>] [SECURITY-THRESHOLD=<integer value>] [DNS-IP-ADDRESS=<IP address>] [PROBE-ENABLE=<enable|disable>] [PROBE-RETRIES=<integer value>] [PROBE-TIMEOUT=<integer value>][PRIMARY-WINS-SERVER=<IP address>] [SECONDARY-WINS-SERVER=<IP address>] [NODE-TYPE=<BROADCAST|POINT-TO-POINT|HYBRID|MIXED>]
211.	Add	IF-IP-ADDRESS=<IP address> IP-ADDRESS-FROM=<IP address> IP-ADDRESS-TO=<IP address>DEFAULT-ROUTER=<IP address> LEASE-TIME=<integer value> PROBE-ENABLE=<enable|disable>
212.	Edit	IF-IP-ADDRESS=<IP address> IP-ADDRESS-FROM=<IP address> IP-ADDRESS-TO=<IP address>[DEFAULT-ROUTER=<IP address>] [LEASE-TIME=<integer value>] [PROBE-ENABLE=<enable|disable>]
213.	Remove	IF-IP-ADDRESS=<IP address> IP-ADDRESS-FROM=<IP address> IP-ADDRESS-TO=<IP address>
214.	Add	IP-ADDRESS=<IP address> MAC-ADDRESS=<MAC address - hexString[0:320]> HOST-NAME=<string[0:20]>DEFAULT-ROUTER=<IP address> CONFIG-SERVER-IP=<IP address> CONFIG-FILE-NAME=<string[0:128]>
215.	Edit	IP-ADDRESS=<IP address> [MAC-ADDRESS=<MAC address - hexString[0:320]>] [HOST-NAME=<string[0:20]>][DEFAULT-ROUTER=<IP address>] [CONFIG-SERVER-IP=<IP address>] [CONFIG-FILE-NAME=<string[0:128]>]
216.	Remove	IP-ADDRESS=<IP address>

Table 8-1 ONS 15302 - ONSCLI Command and Parameters (continued)

Command		Parameters
217.	Add	IF-NUMBER=<integer value> NETWORK-ADDRESS=<IPX network number - hexString[8:8]> TIME-TO-NETWORK=<integer value 1:65535> LAYER2-ENCAP=<novell|ethernet|llc|snap|none> NETBIOS=<enabled|disabled> ADMINISTRATIVE-STATUS=<off|on|sleeping>
218.	Edit	CIRCUIT-NUMBER=<integer value> [TIME-TO-NETWORK=<integer value 1:65535>][LAYER2-ENCAP=<novell|ethernet|llc|snap|none>] [NETBIOS=<enabled|disabled>] [ADMINISTRATIVE-STATUS=<off|on|sleeping>]
219.	Remove	CIRCUIT-NUMBER=<integer value>
220.	RIP-Parameters	CIRCUIT-NUMBER=<integer value> [UPDATE-INTERVAL=<integer value>] [AGE-MULTIPLIER=<integer value>][STATUS=<off|on>]
221.	SAP-Parameters	CIRCUIT-NUMBER=<integer value> [UPDATE-INTERVAL=<integer value>] [AGE-MULTIPLIER=<integer value>][RESPOND-TO-GET-SERVER=<no|yes>] [STATUS=<off|on>]
222.	Add	TYPE=<input|output> NETWORK-ADDRESS=<IPX network number - hexString[8:8]>NETWORK-MASK=<IPX network number - hexString[8:8]> ACTION=<deny|permit>
223.	Edit	TYPE=<input|output> NUMBER=<integer value> [NETWORK-ADDRESS=<IPX network number - hexString[8:8]>][NETWORK-MASK=<IPX network number - hexString[8:8]>] [ACTION=<deny|permit>]
224.	Remove	TYPE=<input|output> NUMBER=<integer value>
225.	Show	[CIRCUIT-NUMBER=<integer value>]
226.	Add	CIRCUIT-NUMBER=<integer value> TYPE=<input|output> NETWORK-ADDRESS=<IPX network number - hexString[8:8]> NETWORK-MASK=<IPX network number - hexString[8:8]> ACTION=<deny|permit>
227.	Edit	CIRCUIT-NUMBER=<integer value> TYPE=<input|output> NUMBER=<integer value>[NETWORK-ADDRESS=<IPX network number - hexString[8:8]>] [NETWORK-MASK=<IPX network number - hexString[8:8]>] [ACTION=<deny|permit>]
228.	Remove	CIRCUIT-NUMBER=<integer value> TYPE=<input|output> NUMBER=<integer value>

Table 8-1 ONS 15302 - ONSCLI Command and Parameters (continued)

Command		Parameters
229.	Add	TYPE=<input|output> NETWORK-ADDRESS=<IPX network number - hexString[8:8]> NETWORK-MASK=<IPX network number - hexString[8:8]> SERVICE-TYPE=<IPX server type - hexString[4:4]>SERVICE-NAME=<string[1:48]> ACTION=<deny|permit>
230.	Edit	TYPE=<input|output> NUMBER=<integer value> [NETWORK-ADDRESS=<IPX network number - hexString[8:8]>][NETWORK-MASK=<IPX network number - hexString[8:8]>] [SERVICE-TYPE=<IPX server type - hexString[4:4]>][SERVICE-NAME=<string[1:48]>] [ACTION=<deny|permit>]
231.	Remove	TYPE=<input|output> NUMBER=<integer value>
232.	Show	[CIRCUIT-NUMBER=<integer value>]
233.	Add	CIRCUIT-NUMBER=<integer value> TYPE=<input|output> NETWORK-ADDRESS=<IPX network number - hexString[8:8]> NETWORK-MASK=<IPX network number - hexString[8:8]> SERVICE-TYPE=<IPX server type - hexString[4:4]>SERVICE-NAME=<string[1:48]> ACTION=<deny|permit>
234.	Edit	CIRCUIT-NUMBER=<integer value> TYPE=<input|output> NUMBER=<integer value> [NETWORK-ADDRESS=<IPX network number - hexString[8:8]>] [NETWORK-MASK=<IPX network number - hexString[8:8]>] [SERVICE-TYPE=<IPX server type - hexString[4:4]>][SERVICE-NAME=<string[1:48]>] [ACTION=<deny|permit>]
235.	Remove	CIRCUIT-NUMBER=<integer value> TYPE=<input|output> NUMBER=<integer value>
236.	Add	DEST-NETWORK=<IPX network number - hexString[8:8]> CIRCUIT-NUMBER=<integer value> NEXT-HOP=<IPX network number - hexString[8:8]> [TICKS-TO-NET=<integer value>] [HOPS-TO-NET=<integer value>] [FORWARDING-ROUTER=<MAC address - hexString[12:12]>]
237.	Edit	DEST-NETWORK=<IPX network number - hexString[8:8]> CIRCUIT-NUMBER=<integer value>[TICKS-TO-NET=<integer value>] [HOPS-TO-NET=<integer value>][FORWARDING-ROUTER=<IPX node address - hexString[12:12]>] [NEXT-HOP=<IPX network number - hexString[8:8]>]
238.	Remove	DEST-NETWORK=<IPX network number - hexString[8:8]>CIRCUIT-NUMBER=<integer value>

Table 8-1 ONS 15302 - ONSCLI Command and Parameters (continued)

Command		Parameters
239.	Add	SERVER-NAME=<string[1:48]> SERVER-TYPE=<IPX server type - hexString[4:4]> NETWORK=<IPX network number - hexString[8:8]> SERVER-ADDRESS=<IPX node address - hexString[12:12]>SOCKET=<IPX socket type - hexString[4:4]> HOPS-TO-SERVER=<integer value>
240.	Edit	SERVER-NAME=<string[1:48]> SERVER-TYPE=<IPX server type - hexString[4:4]> [NETWORK=<IPX network number - hexString[8:8]>] [SERVER-ADDRESS=<IPX node address - hexString[12:12]>][SOCKET=<IPX socket type - hexString[4:4]>] [HOPS-TO-SERVER=<integer value>]
241.	Remove	SERVER-NAME=<string[1:48]> SERVER-TYPE=<IPX server type - hexString[4:4]>
242.	Operating-Parameters	[IPM-ENABLE=<enabled|disabled>]
243.	Show	[IF-INDEX=<integer value>]
244.	Add	IF-INDEX=<integer value> [QUERY-INTERVAL=<integer value>] [VERSION=<integer value>] [MAX-RESPONSE-TIME=<integer value 0:255>] [ROBUSTNESS=<integer value 1:255>] [LAST-MEMBER-QUERY-INTVL=<integer value 0:255>]
245.	Edit	IF-INDEX=<integer value> [QUERY-INTERVAL=<integer value>] [VERSION=<integer value>] [MAX-RESPONSE-TIME=<integer value 0:255>] [ROBUSTNESS=<integer value 1:255>][LAST-MEMBER-QUERY-INTVL=<integer value 0:255>
246.	Remove	[IF-INDEX=<integer value>]
247.	Cache-Table	[CACHE-ADDRESS=<IP address>] [IF-INDEX=<integer value>]
248.	Routing-Table	[GROUP=<IP address>] [SOURCE=<IP address>] [MASK=<IP address>]
249.	Next-Hop	[GROUP=<IP address>] [SOURCE=<IP address>] [MASK=<IP address>] [IF-INDEX=<integer value>] [ADDRESS=<IP address>]
250.	Device-Parameters	[GVRP-STATUS=<enabled|disabled>]
251.	Port-Parameters	[PORT-NUMBER=<integer value 1:8>] [GVRP-STATUS=<enabled|disabled>]
252.	Timing-Parameters	[PORT-NUMBER=<integer value 1:8>] [JOIN-TIME=<integer value>] [LEAVE-TIME=<integer value>] [ALL-LEAVE-TIME=<integer value>]
253.	Display-Statistics	[PORT-NUMBER=<integer value 1:8>]
254.	PORT-MIRRORING	[MIRRORED-PORT=<disabled|1|2|3|4|5|6|7|8>] [COPY-PORT=<disabled|1|2|3|4|5|6|7|8>]

Table 8-1 ONS 15302 - ONSCLI Command and Parameters (continued)

Command		Parameters
255.	Running-Config	[SECTION-LIST=<integer value 1:9,...>] No input parameter starts all sections. 1 - Section 1 General information. 2 - Section 2 Alarms. 3 - Section 3 Routing(IP) information. 4 - Section 4 Management configuration. 5 - Section 5 Bridge configuration. 6 - Section 6 Ports configuration. 7 - Section 7 VLAN configuration. 8 - Section 8 Statistics. 9 - Section 9 Compressed status report.
256.	Used	[SORT-MODE=<LEX|G707>]
257.	Show	[IF-INDEX=<integer value>]
258.	Add	IF-INDEX=<integer value> [JOIN-PRUNE-INTV=<integer value>] [MODE=<dense|sparse|sparseDense>] [HELLO-INTV=<integer value>]
259.	Edit	IF-INDEX=<integer value> [JOIN-PRUNE-INTV=<integer value>] [MODE=<dense|sparse|sparseDense>][HELLO-INTV=<integer value>]
260.	Remove	[IF-INDEX=<integer value>]
261.	Nighbor-Table	[ADDRESS=<IP address>]
262.	Route-Table	[GROUP=<IP address>] [SOURCE=<IP address>] [MASK=<IP address>]
263.	Next-Hop-Table	[GROUP=<IP address>] [SOURCE=<IP address>] [MASK=<IP address>] [IF-INDEX=<integer value>] [ADDRESS=<IP address>]
264.	Clear-SDH-Counters	<none>
265.	System-Mode	[SYSTEM-MODE=<ip|ip-unnumbered>]
266.	Add (Ipun-Route-Table)	DEST-IP-ADDR=<IP address>SUBNET-MASK=<IP address>NEXT-HOP=<IP address>[METRIC=<integer value>]
267.	Remove (Ipun-Route-Table)	DEST-IP-ADDR=<IP address>SUBNET-MASK=<IP address>NEXT-HOP=<IP address>
268.	Global-parameter	[OSPF-IPUN-ADMINISTRATIVE-STATUS=<enabled|disabled>][LEAK-STATIC-ROUTES-TO-OSPF=<enable|disable>][LEAK-EXTERNAL-ROUTES-TO-OSPF=<enable|disable>]
269.	Add	AREA-ID=<IP address>
270.	Show	[IP-ADDRESS=<IP address>][IF-INDEX=<integer value>]

Table 8-1 ONS 15302 - ONSCLI Command and Parameters (continued)

Command		Parameters
271.	Edit	IP-ADDRESS=<IP address>IF-INDEX=<integer value>[AREA-ID=<IP address>][ADMIN-STATUS=<enabled|disabled>][ROUTER-PRIORITY=<integer value 0:255>][RETRANSMISSION-INTERVAL=<integer value 0:3600>][HELLO-INTERVAL=<integer value 1:65535>][TRANSMISSION-DELAY=<integer value 0:3600>][ROUTER-DEAD-INTERVAL=<integer value 0:2147483647>]
272.	ES-IS-Configuration	[STATUS=<enabled|disabled>][ES-HOLD-TIMER=<integer value 0:65535>][ES-REPORT-TIMER=<integer value 0:65535>][IS-HOLD-TIMER=<integer value 0:65535>][IS-REPORT-TIMER=<integer value 0:65535>][SUGGESTED-TIMER=<integer value 0:65535>]
273.	IS-IS-Configuration	[STATUS=<enabled|disabled>][L1-METRIC=<integer value 1:63>][L2-METRIC=<integer value 1:63>][CIRCUIT-OUTSIDE-DOMAIN=<enabled|disabled>][IS-IS-HELLO-TIMER=<integer value 0:65535>][L1-DIS-PRIORITY=<integer value 1:127>][L2-DIS-PRIORITY=<integer value 1:127>][DIS-IIH-TIMER=<integer value 0:65535>]
274.	CLNP-Configuration	[MAXIMUM-CLNP-PDU-LIFETIME=<integer value 0:65535>][MAXIMUM-CLNP-REASSEMBLY-TIME=<integer value 0:65535>]
275.	Show	<none>
276.	Add	NSAP=<NSAP address - hexString[6:40]>
277.	Remove	NSAP=<NSAP address - hexString[6:40]>
278.	Gateway-settings	[GATEWAY-ENABLED=<true|false>]
279.	show	WANX-PORT=<integer value 6:8>
280.	General	WANX-PORT=<integer value 6:8>[CONCATENATION=<vcatvc12|vcatvc3|axxessit>][CHANNEL-TI/SIGNAL-LABEL=<integer value 0:50>][PATH-TRACE=<enabled|disabled>][EXPECTED-TI=<string[1:15]>][HEX-EXPECTED-TI=<string[2:44]>][TRANSMIT-TI=<string[1:15]>][HEX-TRANSMIT-TI=<string[2:44]>][LCAS-OPERATIONAL-MODE=<lcas|nolcas|nolcasbidirectional>][ADMIN-UPSTREAM-CAPASITY=<integer value>][ADMIN-DOWNSTREAM-CAPASITY=<integer value>][PAYLOAD-FCS-INDICATOR=<FCS-ENABLED|FCS-DISABLED>][QTAG-STATUS=<transparentPriority|extractPriority|disabled>][FLOW-CONTROL=<enabled|disabled>][PROTOCOL-TUNNELING=<enabled|disabled>][STP-TUNNELING=<enabled|disabled>][VTP-TUNNELING=<enabled|disabled>][CDP-TUNNELING=<enabled|disabled>]

Table 8-1 ONS 15302 - ONSCLI Command and Parameters (continued)

Command		Parameters
281.	Add-VC3-VC12-channel	WAN-PORT=<integer value 6:8>[KLM=<K.L.M - integer value 1:3.integer value 1:7.integer value 1:3>][ADMIN-STATUS=<enabled|disabled>][NUMBER-TO-ADD=<integer value 1:50>][SORT-MODE=<LEX|G707>]
282.	Remove-VC3-VC12-channel	WAN-PORT=<integer value 6:8>[NUMBER-TO-REMOVE=<integer value 1:50>]
283.	Free-VC12VC3-List	<none>
284.	Used-VC12VC3-List	<none>
285.	General	AGGREGATE-PORT=<integer value 1:2>[ADMINISTRATIVE-STATUS=<enable|disable>][DESCRIPTION=<string[0:64]>][CONNECTED-TO=<string[0:64]>]
286.	TUG3-mapping	[K=<integer value 1:3>][STRUCTURE=<tu3|tu12x21>]
287.	Show-VC3-VC12-Mapping	<none>
288.	List-VC3-VC12-Usage	[SORT-MODE=<LEX|G707>]
289.	Protection	[MSP-STATUS=<enabled|disabled>][PROTECTION-TYPE=<unidirectional|bidirectional>][REVERTING-STATUS=<enabled|disabled>][WAIT-TO-RESTORE-TIME=<integer value 0:2147483647>][SWITCHING-COMMAND=<clear|exercise|manualSwitchToProtection|manualSwitchToWorking|forcedSwitchToProtection|forcedSwitchToWorking|lockoutProtection>]
290.	VC4-Path-Trace	[PATH-TRACE=<enabled|disabled>][EXPECTED-TI=<string[1:15]>][HEX-EXPECTED-TI=<string[2:44]>][TRANSMIT-TI=<string[1:15]>][HEX-TRANSMIT-TI=<string[2:44]>]
291.	RS-Path-Trace	AGGREGATE-PORT=<integer value 1:2>[PATH-TRACE=<enabled|disabled>][EXPECTED-TI=<string[1:15]>][HEX-EXPECTED-TI=<string[2:44]>][TRANSMIT-TI=<string[1:15]>][HEX-TRANSMIT-TI=<string[2:44]>]
292.	General	[SPANNING-TREE-ENABLED=<true|false>][FORCED-PROTOCOL=<stpCompatible|rstp>][BELONG-TO-VLAN=<true|false>][PRIORITY=<integer value 0:65535>][MAX-AGE=<integer value>][HELLO-TIME=<integer value>][FORWARD-DELAY=<integer value>]
293.	Port-Table	[ETHERNET-PORT=<integer value 1:8>][PRIORITY=<integer value 0:255>][ENABLE=<enabled|disabled>][PATH-COST=<integer value 0:200000000>][EDGE-PORT=<true|false>][POINT-POINT=<forceTrue|forceFalse|auto>][PROTOCOL-MIGRATION=<true|false>]
294.	Tuning	<none>

Table 8-1 ONS 15302 - ONSCLI Command and Parameters (continued)

Command		Parameters
295.	show	<none>
296.	edit	PRIORITY=<integer value 0:7>TRAFFIC-CLASS=<integer value 0:3>
297.	GFP-Bad-Frames-Statistics	[WANX-PORT=<integer value 6:8>]
298.	Enable-GFP-Counters	WANX-PORT=<integer value 6:8>
299.	Disable-GFP-Counters	WANX-PORT=<integer value 6:8>
300.	Show-GFP-Counters	[WANX-PORT=<integer value 6:8>]
301.	Clear-GFP-Counters	<none>
302.	Parameters	<none>
303.	Clear-Event-Log	<none>
304.	VC3-Statistics	K=<integer value 1:3>[SHOW-ALL-INTERVALS=<FALSE|TRUE>]
305.	MSP-Statistics	<none>
306.	Trib-Port-Statistics	TRIB-PORT=<integer value 1:12>[SHOW-ALL-INTERVALS=<FALSE|TRUE>]

Managed Objects

9.1 Introduction

This section give an overview of the parameter related to each managed object. Table 9-1 describes the ONS 15302 managed objects.

Table 9-1 Managed Objects

Managed Object	Description
Alarm	Auxiliary alarm input (for voltage-free switches).
AU-4	Administrative Unit level 4
ONS 15302	ONS 15302 device
Bridge	Bridging of Ethernet packets including Spanning Tree Protocol.
DCC / DCC-R / DCC-M	SDH Data Communication Channel as defined by ITU-T G.784
Ethernet	Physical (LAN + Mgmt Port) and logical (WAN) Ethernet interfaces
Ethernet/VC12 Mapping	Mapping of Ethernet traffic into a number of SDH VC12s
Feature	Software feature that can be enabled in the software.
Firmware	Firmware on a module.
Interface	Logical IP interface on router.
IP/IPX Router	Routing of IP and IPX traffic including routing protocols.
LAN	Customer Ethernet interface mapped to a physical port.
LED	Customer LED indicator, and Operator LED indicator
Mgmt Port	Ethernet management port.
MS	SDH signal Multiplexer Section
OSI Stack	Forwarding and routing of CLNP traffic including routing protocols.
Port	Generalization of all logical and physical interfaces.
Protection	SDH protection according to ITU.
QoS	Quality of Service
RS	SDH signal Regenerator Section
RTC	Real-Time Clock

Table 9-1 Managed Objects (continued)

Managed Object	Description
SDH	Optical or electrical SDH port
SNMP User	Registered SNMP user
Software	Software.
Trib.	PDH port (2Mbit/s).
TU-12	Tributary Unit level 12.
Tunnel	Tunnel for encapsulation of IP packets in CLNP. This object covers both encapsulation/decapsulation and address mapping.
User Channel	Transparent serial communication channel.
User Traffic Ethernet	Ethernet interface for user traffic, i.e. LAN + WAN (specialization the Ethernet managed object).

9.2 Alarm

The following section defines the managed object attributes, and their associated alarms. Note that all alarms are associated with a severity level, i.e. WARNING, MINOR, MAJOR, and CRITICAL. This is not shown in the tables.

Table 9-2 Alarm Attributes

Attribute	Access	Type	Description
MODE	R/W	choice	ENABLED or DISABLED
TRIGGERED WHEN	R/W	choice	OPENS or CLOSES. Defines whether contact opening or contact closure is the alarm situation.
TRIGGERED	R	string	Indicates if an alarm situation is present on the port (YES or NO).
PERSISTENCY FILTER ALARM ON	R/W	integer	Filtering of transient alarms. Defines the number of seconds an alarm must be on to be registered.
PERSISTENCY FILTER ALARM OFF	R/W	integer	Filtering of transient alarms. Defines the number of seconds an alarm must be off to be registered.

Table 9-3 Alarm Input Port Alarm

Alarm ID	Description
AUX	Alarm situation on alarm input port.

9.2.1 AU-4

This section give an overview of the parameter related to AU-4 managed object.AU-4 attributes are described in Table 9-4. AU-4 alarms are described in Table 9-5.

Table 9-4 AU-4 Attributes

Attribute	Access	Type	Description
AIS FILTER	R/W	choice	ON/OFF filtering of AIS
PERSISTENCY FILTER ALARM ON	R/W	integer	Filtering of transient alarms. Defines the number of seconds an alarm must be on to be registered.
PERSISTENCY FILTER ALARM OFF	R/W	integer	Filtering of transient alarms. Defines the number of seconds an alarm must be off to be registered.
ALARM REPORTING	R/W	choice	ENABLED or DISABLED. Set the alarm reporting capability for this object. The alarms are listed below

Table 9-5 AU-4 Alarms

Alarm ID	Description
AIS	Alarm indication signal
LOP	Loss of pointer

9.3 ONS 15302

This section give an overview of the parameter related to ONS 15302 managed object.ONS 15302 attributes are described in Table 9-6. Related alarms are described in Table 9-7.

Table 9-6 ONS 15302 Attributes

Attribute	Access	Type	Description
DESCRIPTION	R	string	Device type
NAME	R/W	string	User defined device name
LOCATION	R/W	string	User defined address
CONTACT	R/W	string	User defined responsible person(s)
TIME	R/W	hh:mm:ss	Current Device Time
DATE	R/W	dd/mm/yy	Current Device Date
SYSTEM UP-TIME	R	integer	Seconds since last restart

Table 9-6 ONS 15302 Attributes (continued)

Attribute	Access	Type	Description
ADMINISTRATIVESYNC SOURCE	R/W	choice	List of desired SDH synchronization source in prioritized order. Legal values are EXTERNAL (sync port), LOCAL (free-running), ACTIVE PORT, any SDH port in the system, or any E1 interface configured in PRA mode.
OPERATIONALSYNC SOURCE	R	string	Actual SDH synchronization source. For legal values, see ADMINISTRATIVE SYNC SOURCE.
REMOTE DEVICE	R/W	IP address	IP address of the remote ONS 15302.
ALARM REPORTING	R/W	choice	ENABLED or DISABLED. Set the alarm reporting capability for this object. The alarms are listed below.
GALNET MODE	R	choice	Current mode supported by the device.
GALNET MODE AFTER RESET	R/W	choice	New mode supported by the device after the next reset. Legal values are BASE or EXTENDED.

Table 9-7 ONS 15302 Alarms

Alarm ID	Description
HWFAIL	Hardware failure
LOSSY	Loss of external synchronization (Sync port)
TEMP	Temperature exceeded threshold
FAN	FAN failure

9.4 Bridge

Table 9-8 gives an overview of the parameter related to Bridge managed object.

9.4.1 General Bridge Parameters

Table 9-8 General Bridge Attributes

Attribute	Access	Type	Description
BRIDGE-ADDRESS	R	MAC	The device MAC address

Table 9-8 General Bridge Attributes (continued)

Attribute	Access	Type	Description
BRIDGE-TYPE	R	text	Bridge Type, always Transparent only for ONS 15302.
FORWARDING TABLE AGING TIME	R/W	integer	User-defined number of seconds the learned entries remain in the Forwarding Table(s) (minimum = 10 sec.).

9.4.2 Unicast Forwarding Table Attributes

Table 9-9 shows attributes that exist for each node or interface known to the bridge (Unicast Forwarding Table).

Table 9-9 Unicast Forwarding Table attributes

Attribute	Access	Type	Description
PORT	R/W	integer	Port through which the MAC has been learned.
MAC-ADDRESS	R/W	MAC	MAC address of the node.
IF-INDEX	R/W	integer	VLAN identifier (> 100 000) to which the MAC address applies.
STATUS	R	choice	Learned or manually configured addr. Possible values are LEARNED (the entry was automatically learned), SELF (the entry is a port on the device), MGMT (the entry is a static set by the operator), or OTHER.
COUNT	R	integer	Current Unicast Forwarding Table size (per VLAN)

9.4.3 Multicast Forwarding Table Attributes

The following attributes exist for each multicast MAC address / VLAN-ID pair known to the bridge, (Table 9-10).

Table 9-10 Multicast Forwarding Table Attributes

Attribute	Access	Type	Description
VLAN-ID	R	integer	VLAN identifier to which the multicast MAC address applies.
MAC-ADDRESS	R	MAC	Destination multicast MAC address.
EGRESS PORTS	R	list	Indicates a list of ports in a VLAN to be used to send frames to the multicast MAC address.
LEARNT	R	choice	Indicates the subset of ports from the list in EGRESS PORTS which were identified by IGMP snooping.

9.4.4 Multicast Forward All Table Attributes

The following attributes exist for each VLAN-ID, (Table 9-11).

Table 9-11 Multicast Forward All Table Attributes

Attribute	Access	Type	Description
VLAN-ID	R	integer	VLAN identifier of the Forward All Group.
EGRESS PORTS	R	list	Indicates a list of ports in a VLAN to be used to send frames to the multicast MAC address.
STATIC PORTS	R/W	list	Indicates a list of ports in a VLAN which can participate in a Forward All group.
FORBIDDEN PORTS	R/W	list	Indicates a list of ports in a VLAN which cannot participate in a Forward All group.

9.4.5 Multicast Forward Unregistered Table Attributes

The following attributes exist for each VLAN-ID, (Table 9-12).

Table 9-12 Multicast Forward Unregistered Table Attributes

Attribute	Access	Type	Description
VLAN-ID	R	integer	VLAN identifier of the Forward Unregistered group.
EGRESS PORTS	R	list	Indicates a list of ports in a VLAN to be used to send frames to the multicast MAC address.
STATIC PORTS	R/W	list	Indicates a list of ports in a VLAN which can participate in a Forward All group.
FORBIDDEN PORTS	R/W	list	Indicates a list of ports in a VLAN which cannot participate in a Forward Unregistered group.

9.4.6 Multicast Static Table Attributes

The following attributes exist for each multicast MAC address / VLAN-ID pair known to the bridge, (Table 9-13).

Table 9-13 Multicast Static Table Attributes

Attribute	Access	Type	Description
VLAN-ID	R/W	integer	VLAN identifier to which the multicast MAC address applies.
MULTICAST MAC ADDRESS	R/W	MAC	Destination multicast MAC address.

Table 9-13 Multicast Static Table Attributes (continued)

Attribute	Access	Type	Description
RECEIVE PORTS	R/W	choice	Indicates the port number of the port from which a packet must be received in order for this entry's filtering information to apply.
STATIC PORTS	R/W	list	Indicates a list of ports to which packets received from, and destined to, are always forwarded. This is regardless of the IGMP snooping setting.
FORBIDDEN PORTS	R/W	list	Indicates a list of ports to which packets received from, and destined to, must not be forwarded. This is regardless of the IGMP snooping setting.
STATUS	R/W	choice	Possible values are PERMANENT, DELETE ON RESET (the entry is deleted after a bridge reset), or DELETE ON TIMEOUT (the entry is deleted when it has timed out - aging mechanism).

9.4.7 MAC Multicast Parameters (IGMP Snooping)

MAC Multicast General attributes are shown in Table 9-14.

Table 9-14 MAC Multicast General Attributes

Attribute	Access	Type	Description
MAC MULTICAST FILTERING ENABLE	R/W	choice	Enables multicast on a device. Legal values are TRUE or FALSE.
IGMP SNOOPING MIB VERSION	R/W	integer	Indicates the software version of IGMP that is running on the device.
IGMP SNOOPING ENABLE	R/W	choice	Enables IGMP learning on a device. Legal values are TRUE or FALSE.
IGMP SNOOPING HOST AGING TIME	R/W	integer	Indicates the amount of time (in seconds) before aging out an entry in the MAC Multicast Group Table.
IGMP SNOOPING ROUTER AGING TIME	R/W	integer	Indicates the amount of time (in seconds) before aging out an entry in the MAC Multicast Router Table.

9.4.8 MAC Multicast Group Table Attributes

The following attributes exist for per VLAN (tag), per port and per MAC multicast address, (Table 9-15).

Table 9-15 MAC Multicast Group Table Attributes

Attribute	Access	Type	Description
TAG	R	integer	Identifies the VLAN.
PORT	R	integer	Port number in the VLAN from which multicast group information was learned.
ADDRESS	R	MAC	MAC multicast group address.
EXPIRY TIME	R	integer	Indicates the (minimum) amount of time before the entry is aged out.

9.4.9 MAC Multicast Router Table Attributes

The following attributes exist for per VLAN (tag), and per port, (Table 9-16).

Table 9-16 MAC Multicast Router Table Attributes

Attribute	Access	Type	Description
TAG	R	integer	Identifies the VLAN.
PORT	R	integer	Port number in the VLAN for which this entry contains information for an IP multicast Router.
EXPIRY TIME	R	integer	Indicates the (minimum) amount of time before the entry is aged out.

9.5 General Spanning Tree Parameters

This section describes General Spanning Tree parameters.

9.5.1 General STP Attributes

General STP attributes are shown in Table 9-17.

Table 9-17 General STP Attributes

Attribute	Access	Type	Description
STATUS	R/W	choice	Enabling/disabling of the Spanning Tree Protocol. Legal values are TRUE/FALSE.
PROTOCOL	R	string	Always IEEE 802.1d
STP-TYPE	R	string	per Device or per VLAN
MUST-BELONG-TO-VLAN	R/W	choice	Defines if STP shall be enabled on VLAN ports only or on all ports. Legal values are TRUE (VLAN only) or FALSE (all).
PRIORITY	R/W	integer	Bridge priority in the STP network (low numerical value makes it more likely to become the root) 0-65535

Table 9-17 General STP Attributes (continued)

Attribute	Access	Type	Description
BRIDGE-MAX-AGE	R/W	integer	The maximum age (in seconds) of STP-information learned from the network on any port before it is discarded
BRIDGE-HELLO-TIME	R/W	integer	Time (in seconds) between transmission of config. messages through a given port
BRIDGE-FORWARD-DELAY	R/W	integer	Amount of time a bridge remains in a listening and learning state before forwarding the packets.
STP-MIB-VERSION	R	integer	STP MIB version
ROOT-PORT	R	integer	Port number offering the lowest cost to the root node.
ROOT-ADDRESS	R	MAC	Current root node MAC address
ROOT-PRIORITY	R	integer	Current root node priority
ROOT-PATH-COST	R	integer	Cost from this bridge to the current root node (0 if this bridge is root)
TIME-SINCE-TOPOLOGY-CHANGE	R	integer	Time (in seconds) since last reconfiguration of STP-topology
TOPOLOGY-CHANGE-COUNT	R	integer	Number of STP reconfigurations since last restart
MAX-AGE	R	integer	The maximum age (in seconds) currently in use by all the bridges within the spanning tree.
HELLO-TIME	R	integer	Time (in seconds) between transmission of config. messages through a given port currently in use by all the bridges within the spanning tree.
HOLD-TIME	R	integer	Minimum time (in seconds) between transmission of config. messages through a given port (hard coded = 100 hundredths of sec., i.e. 1 sec.).
FORWARD-DELAY	R	integer	Amount of time a bridge remains in a listening and learning state before forwarding the packets (value currently in use by all the bridges within the spanning tree).

9.5.2 STP Port Attributes

Table 9-18 shows attributes that exists for each port of the bridge (port specific Spanning Tree Parameters).

Table 9-18 STP Port Attributes

Attribute	Access	Type	Description
PRIORITY	RW	integer	Port priority. 0-255
PORT-STATE	R	choice	STP state. Legal values are DISABLED, BLOCKING, LISTENING, LEARNING, FORWARDING.
PORT-ENABLE	R/W	choice	Defines whether the STP is enabled on a port or not. Legal values are ENABLED or DISABLED.
COST	R/W	integer	The cost added to the root path field. Used to determine the cost of the path to the root through this port. 0-65535.
DESIGNATED-ROOT	R	bridgeidentifier	Designated Bridge transmits a unique Bridge Identifier as the Root in the configuration messages (CMs) with priority and MAC address of the Designated Bridge being included.
DESIGNATED-COST	R	integer	The Designated Port path cost of network segments connected to this port. This value is compared to the Root Path Cost field in received configuration messages (CMs).
DESIGNATED-BRIDGE	R	bridgeidentifier	The Bridge Identifier, which this port considers to be the Designated Bridge for this port segment, with priority being included.
DESIGNATED-PORT	R	portIdentifier	The Port Identifier on the Designated Bridge for this port LAN segment.
FORWARD-TRANSITIONS	R	integer	The number of times this port has transitioned from the Learning state to the Forwarding state.

9.5.3 Rapid STP Port Attributes

Table 9-19 shows attributes that exists per VLAN and per port of the bridge (port specific Rapid Spanning Tree Parameters):

Table 9-19 Rapid STP Port Attributes

Attribute	Access	Type	Description
VLAN	R	integer	VLAN ID.
PORT	R	integer	Port number.
STATUS	R/W	choice	Indicates if the port is an edge port. Legal values are FALSE or TRUE.

9.5.4 Rapid Spanning Tree Force Software Version Attributes

Table 9-20 shows attributes that exists per VLAN (Rapid Spanning Tree Force Software Version Table).

Table 9-20 Rapid Spanning Tree Force Software Version Attributes

Attribute	Access	Type	Description
VLAN	R	integer	VLAN ID.
STATE	R/W	choice	Specifies whether this Bridge uses the normal RSTP algorithm, or the STP Compatibility algorithm. Legal values are: STP COMPATIBILITY, or NORMAL RSTP.

9.5.5 Traffic Control Port Priority Attributes

The following attributes exists per port, (Table 9-21).

Table 9-21 Traffic Control Port Priority Attributes

Attribute	Access	Type	Description
PORT	R	integer	Port number.
DEFAULT PRIORITY	R/W	integer	Indicates the default priority assigned to the ingress port. Packets are assigned this default priority if they are not tagged. Legal values are [0:7].
NUMBER OF TRAFFIC CLASSES	R/W	integer	Indicates the number of traffic classes to which received packets can be mapped. Legal values are [1:8].

9.5.6 Traffic Class Attributes

The following attributes exists per port and per priority, (Table 9-22).

Table 9-22 Traffic Class Attributes

Attribute	Access	Type	Description
PORT	R	integer	Port number.
PRIORITY	R	integer	Priority level. Legal values are [0:7].
TRAFFIC CLASS	R/W	integer	Indicates the traffic class to which received packets with specified PRIORITY are mapped. Legal values are [0:3].

9.5.7 Priority Group Attributes

The following attributes exists per port, (Table 9-23).

Table 9-23 Priority Group Attributes

Attribute	Access	Type	Description
PORT	R	integer	Port number.
PRIORITY GROUP	R	integer	Indicates the group to which the PORT belongs. All ports belonging to a same group have the same User Priority to Traffic Class mapping (Table 9-22)

9.6 DCC

There are two DCC objects per SDH port, one for DCCR and one for DCCM. Both have the following attributes.Attributes are shown in Table 9-24.

Table 9-24 DCC Attributes

Attribute	Access	Type	Description
ENABLED	R/W	choice	Defines whether this DCC is enabled. Legal values are TRUE/FALSE.
MODE	R/W	choice	Defines the use of the DCC. Legal values are: NONE IP BROADCAST PPP
LAPD ROLE	R/W	choice	Defines the LAPD role on the DCC. Legal values are: NETWORK USER

9.7 Ethernet

Abstract object, no attribute defined.

9.8 Ethernet/VC-12 Mapping

The following subsections describes attributes related to Ethernet/VC-12 Mapping.

9.8.1 Ethernet/VC-12 Mapping Attributes

Table 9-25shows attributes that exist for each WAN port.

Table 9-25 Ethernet/VC-12 Mapping Attributes

Attribute	Access	Type	Description
ADMINISTRATIVE-CAPACITY	R/W	integer	Bandwidth allocated by operator (0-100 in steps of 2 MBit/s (Mbps))
OPERATIONAL-CAPACITY	R	integer	Current real bandwidth (0-100)
KLM	R	string	Identification of the allocated SDH VC-12 containers. Allocation of VC-12s takes place according to the mapping scheme defined in section SDH multiplexing and mapping
OPERATIONAL-STATUS	R	choice	Operational status per VC-12 (UP or DOWN)
PATH-TRACE	R/W	choice	Enabling/disabling of path trace mechanism (for all allocated VC-12s). Legal values are ENABLE/DISABLE.
EXPECTED-TI	R/W	string	Rx VC-12 path trace identifier pattern (15 char). Equal for all VC-12s.
TRANSMIT-TI	R/W	string	Tx VC-12 path trace identifier pattern (15 char). Equal for all VC-12s.
CHANNEL-TI	R/W	choice	Represents the VC-12 (1-50) for which the received path trace identifier pattern is displayed in RECEIVED-TI.
RECEIVED-TI	R/W	string	Received trace identifier pattern for the VC-12 of the channel selected by RECEIVED-TI KLM.

9.8.2 WAN Port Alarms

WAN port alarms are shown in Table 9-26.

Table 9-26 WAN Port Alarms

Alarm ID	Description
WANDELAY	Differential VC-12 delay for the WAN port is greater than +/– 2ms

9.9 Feature

Feature attributes are shown in Table 9-27.

Feature Attributes

Table 9-27 Feature Attributes

Attribute	Access	Type	Description
ENABLED FEATURES	R	list	List of enabled features on object.

9.10 Firmware

Firmware attributes are shown in Table 9-28.

Firmware Attributes

Table 9-28 Firmware Attributes

Attribute	Access	Type	Description
PRODUCT NUMBER	R	string	Product number
ICS	R	string	Item Change Status (revision)

9.11 LAN

See Ethernet.

9.12 LED

LED attributes are given in Table 9-29.

LED Attributes

Table 9-29 LED Attributes

Attribute	Access	Type	Description
SEVERITY THRESHOLD	R/W	choice	Defines which alarm severity shall turn on the LED.Legal values are: WARNING, MINOR, MAJOR, or CRITICAL.

9.13 Management Port (MGMT)

Management port attributes are shown in Table 9-30.

Mgmt Port Attributes

Table 9-30 Mgmt Port Attributes

Attribute	Access	Type	Description
MODE	R/W	choice	Defines the use of the Management Port. Legal values are:NONEIP MANAGEMENT PORTIP BROADCAST
MAC FRAME FILTER	R/W	choice	ENABLED or DISABLED. Defines whether the filtering mechanism for MAC frames coming from the Management Port shall be used or not. Valid only for IP BROADCAST mode.

9.14 Multiplex Section (MS)

Multiplex Section attributes are shown in Table 9-31 and relevant alarms in Table 9-32.

MS Attributes

Table 9-31 MS Attributes

Attribute	Access	Type	Description
AIS FILTER	R/W	choice	ON/OFF filtering of AIS
RDI FILTER	R/W	choice	ON/OFF filtering of RDI
PERSISTENCY FILTER ALARM ON	R/W	integer	Filtering of transient alarms. Defines the number of seconds an alarm must be on to be registered.
PERSISTENCY FILTER ALARM OFF	R/W	integer	Filtering of transient alarms. Defines the number of seconds an alarm must be off to be registered.
SIGNAL DEGRADE TRESHOLD	R/W	integer	Threshold for signal degraded alarm, 10E-n where n is the threshold. Legal values are 6, 7, 8 and 9.
BBE	R	integer	Background Block Errors
ES	R	integer	Errored Seconds
SES	R	integer	Severe Error Seconds

Table 9-31 MS Attributes (continued)

Attribute	Access	Type	Description
UAS	R	integer	Unavailable Seconds
ALARM REPORTING	R/W	choice	ENABLED or DISABLED. Set the alarm reporting capability for this object. The alarms are listed below.

MS Alarms

Table 9-32 MS Alarms

Alarm ID	Description
AIS	Alarm Indication signal.
EXC	Excessive error defect.
DEG	Degraded signal defect.
RDI	Remote Defect indication.
CSF	Communication subsystem failure, DCCM communication failure.

9.15 The Point-to-Point Protocol (PPP)

The PPP interface parameters are not manageable via ONSCLI. However, the implementation is based on standard MIBs, RFC 1471 (PPP) and RFC 1473 (NCP).

Data Link Layer - PPP

In IP/PPP mode PPP is used as the Data Link Layer Protocol on the DCC channel. The ONS 15302 uses RFC 1662: PPP in HLDC like framing with the CRC-32 option. The CRC-16 option is not supported.

Link Control Protocol - LCP

The ONS 15302 uses RFC 1661: The Point-to Point-Protocol with the following options:

- Magic Number
- MRU = 1500

Once the LCP reach the opened state, Echo-Request and Echo-Reply messages are used as keep alive messages. The Echo-Request messages are sent with the negotiated Magic Number, zero if not negotiated. The ONS 15302 uses an Echo-Request interval of 10 seconds. The ONS 15302 will turn the interface down after missing 5 Echo-Reply messages.

After the LCP is established the ONS 15302 will initiate NCP for IP, i.e. IPCP.

Internet Protocol Control Protocol - IPCP

The ONS 15302 uses RFC 1332: The PPP Internet Protocol Control Protocol, with the following options:

- IP-Address

The ONS 15302 uses the IPCP negotiation phase to inform its peer of its own IP address. The peer must access this address.

The ONS 15302 will accept any IP Address negotiated by the peer.

Once the IPCP reach the opened state, IP communications can take place.

9.16 Port

Common parameters for Ethernet, SDH, tributary, and alarm ports is described in Table 9-33.

Table 9-33 Port Attributes

Attribute	Access	Type	Description
PORT NUMBER	R	integer	Port number on the module.
DESCRIPTION	R/W	string	User defined name of port

9.17 Protection

The protection mode supported is 1 + 1 Multiplex Section Protection (MSP). Attributes are described in Table 9-34 with relevant alarms shown in Table 9-35.

Protection Attributes

Table 9-34 Protection Attributes

Attribute	Access	Type	Description
MSP Enabled	R/W	choice	ENABLED or DISABLED
Switching Type	R/W	choice	UNIDRECTIONAL or BIDIRECTIONAL
Operation Type	R/W	choice	REVERTIVE or NON-REVERTIVE
Wait-to-restore time	R/W	integer	Number of seconds to wait before switching back to the preferred link after it has been restored (default 300 s)
Preferred Link	R	string	Identifier of the preferred working link (always LINK A for ONS 15302).
Commands	R/W	choice	CLEAR, LOCKOUT-OF-PROTECTION, FORCED-SWITCHED-TO-PROTECTION, FORCED-SWITCHED-TO-WORKING, MANUAL-SWITCHED-TO-PROTECTION, MANUAL-SWITCHED-TO-WORKINGEX ERCISE, or NO-COMMAND
Active Link	R	string	Identifier of the active link
Local Request	R	integer	Local request contained in K1 byte

Table 9-34 Protection Attributes (continued)

Attribute	Access	Type	Description
Remote Request	R	integer	Remote request contained in K1 byte
PERSISTENCY FILTER ALARM ON	R/W	integer	Filtering of transient alarms. Defines the number of seconds an alarm must be on to be registered.
PERSISTENCY FILTER ALARM OFF	R/W	integer	Filtering of transient alarms. Defines the number of seconds an alarm must be off to be registered.
ALARM REPORTING	R/W	choice	ENABLED or DISABLED. Set the alarm reporting capability for this object. The alarms are listed below.

Protection Alarm

Table 9-35 Protection Alarm

Alarm ID	Description
MSP	Problem with MSP signalling with another NE across K1/K2 bytes.

9.18 Regenerator Section

Regenerator Section attributes are described in Table 9-36 with relevant alarms in Table 9-37.

RS Attributes

Table 9-36 RS Attributes

Attribute	Access	Type	Description
PERSISTENCY FILTER ALARM ON	R/W	integer	Filtering of transient alarms. Defines the number of seconds an alarm must be on to be registered.
PERSISTENCY FILTER ALARM OFF	R/W	integer	Filtering of transient alarms. Defines the number of seconds an alarm must be off to be registered.
SIGNAL DEGRADE TRESHOLD	R/W	integer	Threshold for signal degraded alarm, 10E-n where n is the threshold. Legal values are 6, 7, 8 and 9.
BBE	R	integer	Background Block Errors
ES	R	integer	Errored Seconds
SES	R	integer	Severe Error Seconds

Table 9-36 RS Attributes (continued)

Attribute	Access	Type	Description
UAS	R	integer	Unavailable Seconds
RS TRACE	R/W	choice	Enabling/disabling of trace mechanism. Legal values are ENABLE/DISABLE.
RS RECEIVED TI	R	string	Actual Received Regenerator Section Trace Identifier, string (15 octets).
RS EXPECTED TI	R/W	string	Expected Regenerator Section Trace Identifier, string (15 octets).
RS TRANSMIT TI	R/W	string	Actual Transmitted Regenerator Section Trace Identifier, string (15 octets).
ALARM REPORTING	R/W	choice	ENABLED or DISABLED. Set the alarm reporting capability for this object. The alarms are listed below.

RS Alarms

Table 9-37 RS Alarms

Alarm ID	Description
EXC	Excessive error defect.
DEG	Degraded signal defect.
CSF	Communication subsystem failure, DCCR communication failure.
TIM	Trace Identifier mismatch.

9.19 RTC

RTC attributes are described in Table 9-38.

RTC Attributes

Table 9-38 RTC Attributes

Attribute	Access	Type	Description
TIME SERVER IP ADDRESS	R/W	IP address	IP address of a host acting as a server for the Time Protocol (RFC 868)

Table 9-38 RTC Attributes (continued)

Attribute	Access	Type	Description
TIME SYNC INTERVAL	R/W	integer	Frequency at which the date/time on the ONS 15302 should be synchronized with the date/time on the server. Setting this parameter to 0 means use manual setting time.
TIME ZONE	R/W	integer	Used to adjust the GMT time received from the server to the local time, and to possibly take into account the Day-Light Saving Time.

9.20 SDH

SDH attributes are described in Table 9-39 with relevant alarms in Table 9-40.

SDH Attributes

Table 9-39 SDH Attributes

Attribute	Access	Type	Description
ADMINISTRATIVE STATUS	R/W	choice	Desired operational status. ENABLED or DISABLED.
OPERATIONAL STATUS	R	string	Actual status on interface. UP or DOWN
RX Level	R	integer	Received optical signal level in dBm (Not applicable with electrical interface).
CONNECTED TO	R/W	list of 100 integers	This attribute is added in order to enable network level management applications to discover the physical network topology. Use of the list entries is user defined and may be variable according to type of network element connected in the other end. Typically the first entry defines which type of NE this port is connected to. The next entries may contain e.g. rack, subrack, IP address, NSAP, module, port.
PERSISTENCY FILTER ALARM ON	R/W	integer	Filtering of transient alarms. Defines the number of seconds an alarm must be on to be registered.

Table 9-39 SDH Attributes (continued)

Attribute	Access	Type	Description
PERSISTENCY FILTER ALARM OFF	R/W	integer	Filtering of transient alarms. Defines the number of seconds an alarm must be off to be registered.
ALARM REPORTING	R/W	choice	ENABLED or DISABLED. Set the alarm reporting capability for this object. The alarms are listed below.

SDH Alarms

Table 9-40 SDH Alarms

Alarm ID	Description
LOS	Loss of STM-1 signal
LOF	Loss of frame alignment on the STM-1 signal.
TD	Transmit Degrade on laser (Not applicable with electrical interface).
TF	Transmit fail on laser (Not applicable with electrical interface).

9.21 SNMP User

SNMP User attributes are described in Table 9-41.

SNMP User Attributes

The SNMP User object contains a table of SNMP users. Each entry of the table contains the following parameters.

Table 9-41 SNMP User Attributes

Attribute	Access	Type	Description
IP ADDRESS	R/W	IP address	IP address of authorized manager
TRAPS ENABLE	R/W	choice	Defines if traps shall be sent to this manager. Legal values are YES and NO.
ACCESS RIGHT	R/W	choice	Defines the access rights of the user. Legal values are SUPER, READ-WRITE and READ-ONLY.
PASSWORD	R/W	string	Password use to access the NE (SNMP community string).

9.22 Software

Software attributes are described in Table 9-42.

Table 9-42 Software Attributes

Attribute	Access	Type	Description
PRODUCT NUMBER	R	string	Product number
ICS	R	string	Item Change Status (revision)

9.23 Tributary

Tributary attributes are described in Table 9-43 with relevant alarms in Table 9-44.

Tributary Port Attributes

Table 9-43 Tributary Port Attributes

Attribute	Access	Type	Description
ADMINISTRATIVE STATUS	R/W	choice	Defines if port is ENABLED or DISABLED
OPERATIONAL STATUS	R	choice	Actual port status UP or DOWN
PERSISTENCY FILTER ALARM ON	R/W	integer	Filtering of transient alarms. Defines the number of seconds an alarm must be on to be registered.
PERSISTENCY FILTER ALARM OFF	R/W	integer	Filtering of transient alarms. Defines the number of seconds an alarm must be off to be registered.
TRIBUTARY MODE	R/W	choice	Tributary port mode, TRA (G.703 Transparent mode) or PRA (ISDN Primary Rate Access)
LOOP MODE	R/W	choice	Loop mode, possible values are:NONE, No loop activated on this tribLL2, Local Loop 2 is activeLL3, Local Loop 3 is active
PATH TRACE	R/W	choice	Enabled or disabled
RECEIVED TI	R	string	Actual Received Path Trace Identifier, string (15 octets).
EXPECTED TI	R/W	string	Expected Path Trace Identifier, string (15 octets).

Table 9-43 Tributary Port Attributes (continued)

Attribute	Access	Type	Description
TRANSMIT TI	R/W	string	Actual Transmitted Path Trace Identifier, string (15 octets).
ALARM REPORTING	R/W	choice	ENABLED or DISABLED. Set the alarm reporting capability for this object. The alarms are listed below.

Tributary Port Alarms

Table 9-44 Tributary Port Alarms

Alarm ID	Description
LOSTX	Loss of signal
AISRX	Alarm indication signal network side
LFARX	Loss of frame alignment customer side
LFATX	Loss of frame alignment customer side
UNASS	Trib activated without mapping to an available VC-12

9.24 TU-12

TU-12 attributes are described in Table 9-45 with relevant alarms in Table 9-46.

TU-12 Attributes

Table 9-45 TU-12 Attributes

Attribute	Access	Type	Description
AIS FILTER	R/W	choice	ON/OFF filtering of AIS
PERSISTENCY FILTER ALARM ON	R/W	integer	Filtering of transient alarms. Defines the number of seconds an alarm must be on to be registered.
PERSISTENCY FILTER ALARM OFF	R/W	integer	Filtering of transient alarms. Defines the number of seconds an alarm must be off to be registered.
ALARM REPORTING	R/W	choice	ENABLED or DISABLED. Set the alarm reporting capability for this object.

TU-12 Alarms

Table 9-46 TU-12 Alarms

Alarm ID	Description
AIS	Alarm indication signal
LOP	Loss of pointer

9.25 User Channel

User Channel attributes are described in Table 9-47.

User Channel Attributes

Table 9-47 User Channel Attributes

Attribute	Access	Type	Description
ADMINISTRATIVE STATUS	R/W	choice	Defines if user channel is ENABLED or DISABLED.
AGGREGATE PORT	R/W	choice	Identifies the aggregate port used to carry user channel data. Legal values are A, B, or ACTIVE PORT.
DESCRIPTION	R/W	string	User defined name.
MODE	R/W	choice	Speed. Legal values are 64 kbit/s and 19.2 kbit/s

9.26 User Traffic Ethernet

User Traffic Ethernet attributes are described in Table 9-48. Port Mirroring attributes are found in Table 9-49.

User Traffic Ethernet Attributes

Table 9-48 User Traffic Ethernet Attributes

Attribute	Access	Type	Description
CONNECTOR-TYPE	R	string	RJ45 or LC.
PORT-DESCRIPTOR	R	string	Always Ethernet in ONS 15302
MAX-CAPACITY	R	string	Highest possible port speed.
MAC-ADDRESS	R	MAC	Port's MAC address

Table 9-48 User Traffic Ethernet Attributes (continued)

Attribute	Access	Type	Description
ASSIGN-PHYSICAL-ADDRESS	R/W	choice	Defines if the common bridge MAC address or a dedicated port address assigned by the system shall be used. Legal values are DEFAULT/RESERVE.
ADMINISTRATIVE-STATUS	R/W	choice	Enables/disables the port. Legal values are ON/OFF.
PORT-STATUS	R	string	Actual port status. UP or DOWN.
SPEED-ADMIN-MODE	R/W	choice	Desired port speed. Legal values are 0, 10 and 100; 0 means port speed not assigned 10 means force speed manually to 10 Mbit/s 100 means force speed manually to 100 Mbit/s
AUTONEGOTIATION-MODE	R/W	choice	Defines whether speed and duplex mode shall be set manually or automatically. Legal values are ENABLE (automatic), DISABLE (manual).
PORT-SPEED	R	string	Current real speed on the port
DUPLEX-ADMIN-MODE	R/W	choice	Desired duplex mode. Legal values are NONE (mode not set), HALF or FULL.
DUPLEX-OPERATION-MODE	R	choice	Actual duplex mode (HALF or FULL).
BACK-PRESSURE-MODE	R/W	choice	ENABLE/DISABLE
FLOW-CONTROL-MODE	R/W	choice	ON/OFF/AUTO

Port Mirroring Attributes

Table 9-49 Port Mirroring Attributes

Attribute	Access	Type	Description
MIRRORED PORT	R/W	choice	Indicates the port number from which all outgoing and incoming traffic is copied. Legal values are DISABLED, or a port number.
COPY PORT	R/W	choice	Indicates the port number to which all outgoing and incoming traffic from/to MIRRORED PORT is mirrored. Legal values are DISABLED, or a port number.

9.27 VC-12

VC-12 attributes are described in Table 9-50 with relevant alarms in Table 9-51.

VC-12 Attributes

Table 9-50 VC-12Attributes

Attribute	Access	Type	Description
RDI FILTER	R/W	choice	ON/OFF filtering of RDI
PERSISTENCY FILTER ALARM ON	R/W	integer	Filtering of transient alarms. Defines the number of seconds an alarm must be on to be registered.
PERSISTENCY FILTER ALARM OFF	R/W	integer	Filtering of transient alarms. Defines the number of seconds an alarm must be off to be registered.
SIGNAL DEGRADE TRESHOLD	R/W	integer	Threshold for signal degraded alarm, 10E-n where n is the threshold. Legal values are 6, 7, 8 and 9.
BBE	R	integer	Background Block Errors
ES	R	integer	Errored Seconds
SES	R	integer	Severe Error Seconds
UAS	R	integer	Unavailable Seconds
ALARM REPORTING	R/W	choice	ENABLED or DISABLED. Set the alarm reporting capability for this object.

VC-12 Alarms

Table 9-51 VC-12 Alarms

Alarm ID	Description
UNEQ	Unequipped
TIM	Trace identifier mismatch
PLM	Payload mismatch
EXC	Excessive error defect.
DEG	Degraded signal defect.
RDI	Remote defect indication

9.28 VC-4

VC-4 attributes are described inTable 9-52 with relevant alarms in Table 9-53.

VC-4 Attributes

Table 9-52 VC-4 Attributes

Attribute	Access	Type	Description
RDI FILTER	R/W	choice	ON/OFF filtering of RDI
PERSISTENCY FILTER ALARM ON	R/W	integer	Filtering of transient alarms. Defines the number of seconds an alarm must be on to be registered.
PERSISTENCY FILTER ALARM OFF	R/W	integer	Filtering of transient alarms. Defines the number of seconds an alarm must be off to be registered.
SIGNAL DEGRADE TRESHOLD	R/W	integer	Threshold for signal degraded alarm, 10E-n where n is the threshold. Legal values are 6, 7, 8 and 9.
BBE	R	integer	Background Block Errors
ES	R	integer	Errored Seconds
SES	R	integer	Severe Error Seconds
UAS	R	integer	Unavailable Seconds
PATH TRACE	R/W	choice	Enabled or disabled
RECEIVED TI	R	string	Actual Received Path Trace Identifier, string (15 octets).
EXPECTED TI	R/W	string	Expected Path Trace Identifier, string (15 octets).
TRANSMIT TI	R/W	string	Actual Transmitted Path Trace Identifier, string (15 octets).
ALARM REPORTING	R/W	choice	ENABLED or DISABLED. Set the alarm reporting capability for this object. The alarms are listed below.

VC-4 Alarms

Table 9-53 VC-4 Alarms

Alarm ID	Description
LOM	Loss of multiframe alignment
UNEQ	Unequipped
TIM	Trace identifier mismatch

Table 9-53 VC-4 Alarms (continued)

Alarm ID	Description
PLM	Payload mismatch
EXC	Excessive error defect
DEG	Degraded signal defect
RDI	Remote defect indication

9.29 VLAN

This section described VLAN attributes.

VLAN Attributes

VLAN attributes is described in Table 9-54.

Table 9-54 VLAN Attributes

Attribute	Access	Type	Description
SUPPORTED-TYPE	R	string	Indicates the type of VLAN currently supported.
SUPPORTED-TYPE-AFTER-RESET	R/W	choice	Indicates the type of VLAN supported after the device is reset. Legal values are “Per Port” or “Per Port And Per Protocol”

Attributes for each VLAN

Table 9-55 describe attributes that exist for each VLAN.

Table 9-55 VLAN Attributes

Attribute	Access	Type	Description
NAME	R/W	string	User defined VLAN name.
PRIORITY	R/W	integer	Indicates the value of the priority tag. Legal values are [0:7].
MAC-ADDRESS	R	MAC	Permanent VLAN MAC address (depends on ADDRESS-TYPE).
ADDRESS-TYPE	R/W	choice	DEFAULT or RESERVE.
TAG	R/W	integer	VLAN tag for encapsulation of traffic in a remote bridge. Legal values are 0-4000.

Table 9-55 VLAN Attributes (continued)

Attribute	Access	Type	Description
PROTOCOL-TYPE	R/W	choice	Indicates the type of protocol used to define the VLAN. Legal values are PREDEFINED or USER DEFINED. This parameter applies only for per Port and per Protocol VLANs.
PROTOCOL	R/W	choice	Indicates the type of protocol used to define the VLAN. If PROTOCOL-TYPE = PREDEFINED, legal values are: IP, IPX RAW, IPX Ethernet, IPX LLC, IPX SNAP, DECNET, NETBIOS, SNA, or OTHER. If PROTOCOL-TYPE = USER DEFINED, legal values are defined by the user via the Ethernet User Defined Protocols (see). This parameter applies only for per Port and per Protocol VLANs.

Attributes for each Port being Member of a VLAN.

Table 9-56 describes attributes that exist for each port being member of a VLAN.

Table 9-56 VLAN Port Attributes

Attribute	Access	Type	Description
VLAN PORT NUMBER	R/W	integer	Defines an Ethernet port on the device.
VLAN PORT TYPE	R	choice	
TAGGING	R/W	choice	Defines whether tagging shall be enabled on this port. Legal values are ENABLE/DISABLE.
FORBIDDEN EGRESS PORT	R/W	list	Indicates the ports which are forbidden to be included in the egress port list for this VLAN.

Attributes for each Ethernet User defined Protocol

Table 9-57 describes attributes that exist for each Ethernet user defined protocol.

Table 9-57 Ethernet User defined Protocol Attributes

Attribute	Access	Type	Description
PROTOCOL NAME	R/W	string	User defined name.
ETHERNET TYPE	R/W	octet string	User defined Ethernet type.

GVRP Attributes

GVRP attributes are described in Table 9-58.

Table 9-58 GVRP Attributes

Attribute	Access	Type	Description
GVRP STATUS	R/W	choice	Indicates if GVRP is enabled on the device. Legal values are ENABLED or DISABLED.

GVRP Port Attributes

Table 9-59 describes attributes that exist for each User Traffic Ethernet port.

Table 9-59 GVRP Port Attributes

Attribute	Access	Type	Description
PORT GVRP STATUS	R/W	choice	Indicates if GVRP is enabled on the port. Legal values are ENABLED or DISABLED.
JOINT TIME	R/W	integer	Maximum interval in milliseconds between GVRP PDUs.
LEAVE TIME	R/W	integer	Period of time in milliseconds that the device will wait in the Leaving state before transiting to the Empty state.
LEAVE ALL TIME	R/W	integer	Interval in milliseconds between Leave All PDUs.
FAILED REGISTRATIONS	R	integer	Indicates the total number of failed GVRP registrations, for any reason, on this port.
LAST PDU ORIGIN	R	octet string	Indicates the Source MAC Address of the last GVRP message received on this port.

9.30 VT100 User

The VT100 User object contains the password for the VT100 port and for TELNET access.Attributes are described in Table 9-60.

Table 9-60 VT100 User Attributes

Attribute	Access	Type	Description
VT100 PASSWORD	R/W	string	Password
TELNET PASSWORD	R/W	string	Password

9.31 WAN

See Ethernet.

A

ABER Bit Error Rate switching threshold

AC Alternate Current

ADM Add Drop Multiplexer

AIS Alarm Indication Signal (1111...)

APS Automatic Protection Switching

AU Administrative Unit

AUXP Auxiliary Pattern (1010...)

B

B2B Back-to-back

BAT Battery

BER Bit Error Ratio

BIDL Bi-Directional Loopback Alarm

C

CLI Command Line Interface

CLNP Connection less Network Protocol

CO Central Office

CRC-4 Method for detection of bit errors (ITU-T Rec. G.704)

D

DC Direct Current

DCC Data Communications Channel

DCE Data Circuit-terminal Equipment

DCN Data Communications Network

DL Downlink (towards user)

DLAS Degraded Laser

DQUI Degraded Quality on User Interface

DTE Data Terminal Equipment

E

ECT Equipment Craft Terminal

EOW Engineering Order Wire

EEPROM Electrical Erase Programmable Read Only Memory

EMC Electromagnetic Compatibility

EPROM Erase Programmable Read Only Memory

ES End System

ES Errored Seconds

ET Exchange Termination

ETSI European Telecommunication Standards Institute

F

F1 Optical line interface

F2 Electrical 2 Mbit/s interface

FA Frame Alignment

FC Failure Condition

FC/PC Optical Connector

FP Fabry Perot

FPGA Field Programmable Gate Array

FTP File Transfer Protocol

G

GFP	Generic Frame Procedure
GUI	Graphical User Interface

H

HBER	High Bit Error Rate
HDB3	High Density Binary Code
HDLC	High-level Data Link Control
HW	Hardware

I

ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IS	Intermediate System
ISDN	Integrated Services Digital Network
ITU-T	International Telecommunication Union Standardization Bureau

K

KLM	Numbering scheme for container in SDH

L

LAP-D	Link Access Procedure on the D channel
LAN	Local Area network
LBER	Low Bit Error Rate
LCAS	Link Capacity Adjustment Scheme

LCT VT.100 compatible Local Craft Terminal

LD Laser Diode

LED Light Emitting Diode

LFA Loss of Frame (BF) Alignment

LL2/LL3 Local Loop 2/3

LMF Loss of Multiframe Alignment

LOS Loss of Signal

LPS Line Protection Switching

LTE Line Termination Equipment

M

MAC Medium Access

MD Mediation Device

MF Multiframe (G.704)

MIB Management Information Base

MS Multiplex Section

N

NC Not Connected

NE Network Element

NET Network

NSAP Network Service Access Point

NTE Network Termination Equipment

NV Non-Volatile

O

OC Operating Center

OCT Office Craft Terminal

ODF	Optical Distribution Frame
OFDLS	Optical Fibre Digital Line System (Associated LTE, NTE and fibre route)
OLOS	Optical LOS
OPOL	Optical Power out of Limit
ORX	Optical interface module RX
OSI	Open Systems Interconnection
OTX	Optical interface module TX

P

PABX	Private Automatic Branch Exchange
PC	Personal Computer
PCB	Printed Circuit Board
PDH	Plesiochronous Digital Hierarchy (ITU-T Rec. G.702)

R

RAL	Restricted Access Location
Rx	optical receiver

T

TAC	Technical Assistance Center
TCP	Transport Control Protocol
TIA	Telecommunication Industry Association
Tx	optical transmitter

W

www	World Wide Web