



Cisco Edge Craft Software Guide

Release 1.2
February 2004

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-5383-01



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.

CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0401R)



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](#)
- [Audience](#)
- [Document Organization](#)
- [Related Documentation](#)
- [Document Conventions](#)
- [Where to Find Safety and Warning Information](#)
- [Obtaining Documentation](#)
- [Documentation Feedback](#)
- [Obtaining Technical Assistance](#)
- [Obtaining Additional Publications and Information](#)

Document Objectives

This Software Guide explains the functionality of the Cisco Edge Craft for the Cisco ONS 15302 and ONS 15305 systems. It contains installation and user information for the Cisco ONS 15302 and ONS 15305 systems. Use this Software Guide in conjunction with the appropriate publications listed in the [Related Documentation](#) section.

Audience

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

Document Organization

This Cisco Edge Craft Software Guide, R1.2 is organized into the following chapters:

- [Chapter 1, “Installing Cisco Edge Craft”](#) provides information how to install the Cisco Edge Craft Software.
- [Chapter 2, “Software Description”](#) provides details about the features of the Cisco Edge Craft.
- [Chapter 3, “Using Cisco Edge Craft”](#) provides information how to use the Cisco Edge Craft.
- [Chapter 4, “General Management”](#) provides information about the configuration operations supported by the Management Interfaces managed object.
- [Chapter 5, “Traffic Port Management”](#) provides information about the configuration of the four different port types (SDH, PDH, LAN, and WAN)
- [Chapter 6, “Link Aggregation”](#) provides details how to manage the link aggregation functionality of the network element.
- [Chapter 7, “Layer 2 Configuration”](#) provides information to manage the bridging service (L2 forwarding) on the network element.
- [Chapter 8, “Performance Management”](#) provides information about the performance of the system.
- [Appendix A, “Troubleshooting and FAQ”](#) provides information in case of problems with the system.

Related Documentation

Use this Cisco Edge Craft Software Guide, R1.2 in conjunction with the following referenced publications:

- *Cisco ONS 15302 Installation and Operation Guide*
Provides information how to install the system and how to initial the system.
- *Cisco ONS 15305 Installation and Operation Guide*
Provides information how to install the system and how to initial the system.

Document Conventions

This publication uses the following conventions:

Convention	Application
boldface	Commands and keywords in body text.
<i>italic</i>	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.

Convention**Application**`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. To see translations of the warnings that appear in this publication, refer to the translated safety warnings that accompanied this device.

Note: SAVE THESE INSTRUCTIONS

Note: This documentation is to be used in conjunction with the specific product installation guide that shipped with the product. Please refer to the Installation Guide, Configuration Guide, or other enclosed additional documentation for further details.

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 on the World Wide Web at this URL:

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

You can access the Cisco website at this URL:

<http://www.cisco.com>

International Cisco websites can be accessed from this URL:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpk/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/index.shtml>
- 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 800 553-NETS (6387).

Cisco Optical Networking Product Documentation CD-ROM

Optical networking-related documentation, including Cisco Edge Craft 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.

Documentation Feedback

You can submit e-mail 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.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides 24-hour-a-day, award-winning technical support services, online and over the phone. Cisco.com features the Cisco TAC website as an online starting point for technical assistance. If you do not hold a valid Cisco service contract, please contact your reseller.

Cisco TAC Website

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

<http://www.cisco.com/tac>

Accessing all the tools on the Cisco TAC website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:

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

Opening a TAC Case

Using the online TAC Case Open Tool is the fastest way to open P3 and P4 cases. (P3 and P4 cases are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using the recommended resources, your case will be assigned to a Cisco TAC engineer. The online TAC Case Open Tool is located at this URL:

<http://www.cisco.com/tac/caseopen>

For P1 or P2 cases (P1 and P2 cases are those in which your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

To open a case 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 listing of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

Priority 1 (P1)—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.

Priority 2 (P2)—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.

Priority 3 (P3)—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.

Priority 4 (P4)—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. Go to this URL to visit the company store:
<http://www.cisco.com/go/marketplace/>
- The Cisco *Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:
<http://cisco.com/univercd/cc/td/doc/pcat/>
- *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 online at this URL:
<http://www.ciscopress.com>
- *Packet* magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access Packet magazine at this URL:
<http://www.cisco.com/packet>
- *iQ Magazine* is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. 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>
- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:
<http://www.cisco.com/en/US/learning/index.html>



About This Guide iii

Document Objectives	iii
Audience	iii
Document Organization	iii
Related Documentation	iv
Document Conventions	iv
Where to Find Safety and Warning Information	v
Obtaining Documentation	v
Cisco.com	vi
Ordering Documentation	vi
Cisco Optical Networking Product Documentation CD-ROM	vi
Documentation Feedback	vi
Obtaining Technical Assistance	vii
Cisco TAC Website	vii
Opening a TAC Case	vii
TAC Case Priority Definitions	vii
Obtaining Additional Publications and Information	viii

CHAPTER 1

Installing Cisco Edge Craft 1-1

1.1 Install Cisco Edge Craft Using the Install Wizard	1-1
1.2 Un-install Cisco Edge Craft	1-2
1.3 Commission IP Address via the VT100 Interface	1-2
1.3.1 Invoke ONSCli	1-3
1.3.2 Configure Community-Handler	1-5
1.3.2.1 ONS 15305	1-5
1.3.2.2 ONS 15302	1-5
1.3.3 Assign an IP Address	1-6
1.3.3.1 ONS 15305	1-6
1.3.3.2 ONS 15302	1-7
1.3.4 Change Passwords	1-7
1.3.4.1 ONS 15305	1-7
1.3.4.2 ONS 15302	1-7
1.4 Connect to a Network Element	1-8

1.5 Configure the VT100 Terminal 1-9

CHAPTER 2

Software Description 2-1

2.1 Introduction 2-1

2.2 Product Features 2-2

2.2.1 Network Element Access 2-2

2.2.2 Information Model 2-2

2.2.3 Single User 2-3

2.2.4 Single Network Element 2-3

2.2.5 Graphical User Interface Types 2-3

2.2.6 No Persistency 2-3

2.2.7 List of Possible Network Element IP Addresses 2-3

2.2.8 Configuration Download and Upload 2-3

2.2.9 Software, Firmware and Licenses Download 2-3

2.2.10 User Access 2-4

2.2.11 Alarm and Event Notifications Presentation 2-4

2.2.12 Presentation of Performance Data 2-4

2.2.13 Management Configuration 2-4

2.2.14 Physical Inventory 2-4

2.2.15 Logical Inventory 2-4

2.2.16 Global Settings 2-4

2.2.17 Alarm and Event Filtering Configuration 2-5

2.2.18 SDH Ports Configuration 2-5

2.2.19 PDH Ports Configuration 2-5

2.2.20 MSP and SNCP Configuration 2-5

2.2.21 SDH Synchronization Configuration 2-5

2.2.22 LAN Ports Configuration 2-5

2.2.23 WAN Ports Configuration 2-5

2.2.24 Test Loops Configuration 2-5

2.2.25 Cross-Connect (XC) Configuration 2-5

2.2.26 Bridge Configuration 2-6

2.2.27 VLAN Configuration 2-6

2.2.28 Security 2-6

2.2.29 Data Communication 2-6

2.2.30 Reliability 2-6

2.2.31 Maintenance 2-6

2.2.31.1 Debugging 2-6

2.2.31.2 System Logging 2-6

2.2.31.3 New Releases and Patches 2-7

CHAPTER 3**Using Cisco Edge Craft 3-1**

- 3.1 Cisco Edge Craft Desktop 3-1
 - 3.1.1 Toolbar Buttons 3-2
 - 3.1.2 Menu Items 3-5
 - 3.1.2.1 File 3-5
 - 3.1.2.2 Edit 3-5
 - 3.1.2.3 View 3-6
 - 3.1.2.4 Equipment 3-7
 - 3.1.2.5 Bridge 3-8
 - 3.1.2.6 Tools 3-8
 - 3.1.2.7 Help 3-8
 - 3.1.2.8 Log Viewer 3-9
 - 3.1.3 Copy and Paste 3-11
 - 3.1.4 Cell Selection Mode 3-11
 - 3.1.5 Navigate in Tables Using the Keyboard 3-11
 - 3.1.6 Auto Fit Column Width 3-12
- 3.2 Topology Browser 3-12
- 3.3 Alarm Display 3-12
 - 3.3.1 Subscribe Cisco Edge Craft to Alarms 3-13
 - 3.3.2 View Alarms 3-13
 - 3.3.2.1 Refresh 3-14
 - 3.3.2.2 History 3-14
 - 3.3.2.3 Select Alarm 3-14
 - 3.3.2.4 Copy Alarms 3-16
 - 3.3.2.5 Alarm Lifecycle 3-16
 - 3.3.3 View the Events Reported from the Network Element 3-16
 - 3.3.3.1 Current Events 3-16
 - 3.3.3.2 Event History 3-17
 - 3.3.3.3 Visible Columns 3-17
 - 3.3.3.4 Change Column Order 3-18
 - 3.3.3.5 Resize Columns 3-19
 - 3.3.3.6 Sort Columns 3-19
 - 3.3.4 Alarm and Event Notification 3-20
 - 3.3.4.1 Alarm Notification 3-20
 - 3.3.4.2 Event Notification 3-21
 - 3.3.4.3 Trap-to-Notification Mapping 3-21
 - 3.3.4.4 Unknown Traps 3-22

CHAPTER 4**General Management 4-1**

- 4.1 Management Modes and Configuration 4-1
 - 4.1.1 Management Port Configuration 4-2
 - 4.1.1.1 Mode: Not Used 4-2
 - 4.1.1.2 Mode: IP 4-3
 - 4.1.2 DCC Configuration 4-4
 - 4.1.2.1 Mode: Not Used 4-4
 - 4.1.2.2 Mode: IP 4-4
 - 4.1.3 IP Default Gateway Configuration 4-5
- 4.2 ONS 15305 Scenarios 4-6
 - 4.2.1 Notations Used 4-6
 - 4.2.2 Scenario 1: Cisco Edge Craft and ONS 15305 on the Same Subnet 4-7
 - 4.2.3 Scenario 2: Cisco Edge Craft and ONS 15305 on Different Subnets 4-8
 - 4.2.4 Scenario 3: IP over DCC 4-9
 - 4.2.5 Scenario 4: IP over PPP 4-10
- 4.3 Manage Common Parameters 4-11
 - 4.3.1 View Common Parameters 4-11
 - 4.3.2 Identify the Network Element 4-12
 - 4.3.3 Time Settings 4-12
 - 4.3.4 Users 4-14
 - 4.3.4.1 Add a New User 4-14
 - 4.3.4.2 VT 100 Password (ONS 15302 only) 4-15
 - 4.3.5 Available Features (Licenses) 4-15
 - 4.3.6 Physical Inventory - ONS 15305 4-16
 - 4.3.7 Physical Inventory - ONS 15302 4-17
 - 4.3.8 Restart the ONS 15305 4-17
 - 4.3.9 Restart the ONS 15302 4-18
 - 4.3.10 Logs (Alarm Logs, Performance Data Logs) 4-18
 - 4.3.10.1 Clear Alarm History 4-18
 - 4.3.10.2 Clear PM Data 4-18
 - 4.3.10.3 LEDs and Alarm Output 4-19
 - 4.3.10.4 Ping Mechanism 4-19
 - 4.3.10.5 Alarm Ports 4-20
 - 4.3.10.6 AUX Port - ONS 15305 4-20
 - 4.3.10.7 Power Module - ONS 15305 4-21
- 4.4 Synchronization Management 4-22
 - 4.4.1 SDH Synchronization 4-22
 - 4.4.1.1 Synchronization Networks 4-22
 - 4.4.1.2 Selecting the Best Synchronization Reference 4-23

4.4.1.3 Synchronizing the SDH Equipment	4-24
4.4.2 ONS 15305	4-24
4.4.2.1 Signal Monitoring	4-24
4.4.2.2 Candidate Selection and Configuration	4-24
4.4.2.3 QL-Monitoring and Switching	4-25
4.4.2.4 SEC	4-25
4.4.2.5 Synchronizing External Equipment	4-25
4.4.2.6 Rules	4-26
4.4.2.7 Synchronization Alarms	4-27
4.4.3 View the Synchronization Data (T0 or T4)	4-27
4.4.4 Add Synchronization Source Candidate (T0 or T4)	4-28
4.4.5 Modify Synchronization Source Candidate (T0 or T4)	4-29
4.4.6 Delete Synchronization Source Candidate (T0 or T4)	4-29
4.4.7 Operate Synchronization Switch (T0 or T4)	4-30
4.4.8 View Synchronization Switch (T0 or T4)	4-31
4.4.9 Activate Synchronization on the ONS 15302	4-31
4.5 Download Software to a Network Element	4-32
4.5.1 Network Release	4-32
4.5.2 Operational and Administrative Software Bank	4-33
4.5.3 Effect of Software Upgrades on Traffic	4-33
4.5.4 Download an ONS 15305 Network Release	4-34
4.5.5 Download Software to the ONS 15305	4-34
4.5.5.1 Switch Banks Manually	4-35
4.5.6 Download Software to the ONS 15302	4-36
4.6 Back Up and Restore Configuration Data	4-36
4.6.1 Back Up Configuration Data	4-36
4.6.2 Restore Configuration Data	4-37
4.7 Alarm and Event Configuration	4-38
4.7.1 Event Forwarding	4-39
4.7.2 Configure General Alarm Reporting	4-39
4.7.2.1 Device Alarm Enabling	4-40
4.7.2.2 Slot Alarm Enabling	4-40
4.7.2.3 Traffic Port Alarm Enabling	4-40
4.7.2.4 Alarm Port Alarm Enabling	4-40
4.7.2.5 Aux Port Alarm Enabling	4-40
4.7.3 Suppress Specific Alarms	4-41
4.7.3.1 Suppress RDI, EXC, DEG, SSF Alarms	4-41
4.7.3.2 Suppress AIS Alarms from SDH Ports	4-41
4.7.3.3 Suppress AIS Alarms from E1 Ports	4-41

4.7.3.4	Suppress AIS Alarms from AUX Port	4-41
4.7.4	Modify Alarm Severity and Description	4-42
4.7.5	Set Signal Degrade Threshold	4-42
4.7.6	Modify Alarm Persistency	4-42
4.7.6.1	Persistency Group 1 (HighOrderLevel)	4-42
4.7.6.2	Persistency Group 2 (Unfiltered)	4-43
4.7.6.3	Persistency Group 3 (LowOrderLevel)	4-43
4.7.7	Modify ONS 15302 Alarm Configuration Attributes	4-43
4.7.7.1	View all Alarm Reporting Instances	4-44
4.7.7.2	Enable Alarm Reporting	4-44
4.7.7.3	Modify Ais Rdi Alarm Reporting	4-45
4.7.7.4	Modify Alarm Persistency	4-45
4.7.7.5	Modify Signal Degraded (Sd) Threshold	4-46
4.8	Manage ONS 15305 Slots	4-46
4.8.1	View a Slot	4-47
4.8.2	Modify a Slot	4-48
CHAPTER 5	Traffic Port Management	5-1
5.1	Select a Traffic Port	5-1
5.2	SDH Ports	5-1
5.2.1	Configure ONS 15305 SDH Port Structure (Channelization)	5-2
5.2.1.1	AU4 Termination Points for Cross-connection	5-2
5.2.1.2	Tu3 Termination Points for XC	5-2
5.2.1.3	Tu12 Managed Objects for XC	5-3
5.2.2	Modify or Remove ONS 15305 SDH Port Structure	5-3
5.2.2.1	Modify Between Tu12 and Tu3 Objects	5-3
5.2.2.2	Modify Between Au4 and Tu3 or Tu12 Objects	5-3
5.2.3	Set and Read Path Trace Identifiers	5-4
5.2.3.1	Set or Read RS Path Trace Identifiers	5-4
5.2.3.2	Set or Read VC-4 Path Trace Identifiers	5-5
5.2.4	Monitor SDH Port Performance	5-5
5.2.4.1	Read RS PM Counters	5-5
5.2.4.2	Read MS PM Counters	5-6
5.2.4.3	Read VC-4 PM Counters	5-6
5.2.5	Enable the SDH Port to Carry Traffic and Report Alarms	5-6
5.2.6	Set ONS 15305 SDH Port Synchronization Quality Output Signaling	5-7
5.2.7	SDH Port as a Synchronization Source Input	5-7
5.2.8	DCC Channels on the SDH Port Carrying Management Traffic	5-7
5.3	PDH Ports	5-7

5.3.1	Set the Port Mode for ONS 15305	5-7
5.3.2	Set a Loop in a ONS 15305 PDH Port	5-8
5.3.3	Set a Loop in a ONS 15302 PDH Port	5-9
5.3.4	Release a Loop in a PDH Port	5-9
5.3.5	Assign VC12s in the ONS 15302	5-9
5.3.6	Set and Read Path Trace Identifiers	5-10
5.3.7	Monitor PDH Port Performance	5-11
5.3.8	Enable the PDH Port to Carry Traffic and Report Alarms	5-12
5.3.9	Cross-Connect the ONS 15305 PDH Port to Another Port	5-12
5.4	LAN Ports	5-12
5.4.1	ONS 15305 - LAN Port Attributes	5-12
5.4.2	ONS 15302 LAN Port Attributes	5-14
5.5	WAN Ports - ONS 15305	5-14
5.5.1	WAN Ports and Mapping	5-14
5.5.2	Add Initial WAN Port Capacity	5-16
5.5.3	Modify WAN Port Capacity	5-19
5.5.3.1	Increase Capacity in the SDH Server Layer	5-19
5.5.3.2	Decrease Capacity in the SDH Server Layer	5-20
5.5.4	Protect a WAN Port	5-20
5.5.5	Modify Protection Parameters on the WAN Port	5-22
5.5.6	Command a WAN Port Protection Switch	5-23
5.5.7	Set Path Trace Identifiers for a WAN Port	5-24
5.5.8	Read Path Trace Identifiers for a WAN Port	5-24
5.5.9	Monitor WAN Port Performance	5-25
5.5.10	Advanced WAN Port Operations	5-25
5.5.10.1	Select and Insert Multiple Termination Points	5-25
5.5.10.2	Manually Enter Termination Points	5-26
5.6	WAN Ports - ONS 15302	5-26
5.6.1	WAN ports and the Mapping	5-26
5.6.2	Differences Between the ONS 15305 and ONS 15302	5-27
5.6.3	Add Initial WAN Port Capacity	5-27
5.6.3.1	Set the Administrative Capacity (Optional)	5-28
5.6.3.2	Cross-Connect the WAN Channels	5-28
5.6.4	Increase Capacity in the SDH Server Layer	5-30
5.6.5	Decrease Capacity in the SDH Server Layer	5-30
5.6.6	Set Path Trace Identifiers for a WAN Port	5-31
5.6.7	Read Path Trace Identifiers for a WAN Port	5-32
5.6.8	Monitor WAN Port Performance	5-32
5.6.9	Advanced WAN Port Operations	5-33

5.7	ONS 15305 SDH Layer Network and Cross-Connections	5-33
5.7.1	SDH Port Structuring	5-34
5.7.1.1	C.B.K.L.M Value Usage	5-35
5.7.1.2	Cross-Connection Management	5-36
5.7.1.3	8-Port STM-1 Module Example	5-37
5.7.1.4	XC Fabric	5-40
5.7.2	Open the Cross-Connection GUI	5-40
5.7.3	Browse Existing Cross-Connections	5-42
5.7.3.1	Browse all Cross-Connections	5-42
5.7.3.2	Browse Cross-Connections of a Port	5-42
5.7.3.3	Filter the Content of the Cross-Connection List	5-43
5.7.3.4	Synchronize or Refresh the Cross-Connect Window	5-43
5.7.4	Set Up Cross-Connections from a 2 Mbps E1 Port to a Timeslot in an SDH Port	5-44
5.7.5	Set Up Cross-Connections from a 45 Mbps E3 (T3) Port to a Timeslot in an SDH Port	5-45
5.7.6	Create a Pass-through Cross-Connection	5-45
5.7.7	Modify Cross Connections	5-46
5.7.8	Protect Cross Connections	5-46
5.7.8.1	Enable SNC Protection	5-47
5.7.8.2	Modify Protection Parameters of a Cross-Connection	5-48
5.7.8.3	Command a Cross-Connection Protection Switch	5-48
5.7.9	Delete Cross-Connections	5-49
5.7.10	Advanced Cross-Connection Operations	5-49
5.7.10.1	Set Up Multiple Cross-Connections by Multiple Selection	5-49
5.7.10.2	Set Up Multiple Cross-Connections by Repeated Operations	5-50
5.7.10.3	Enter Termination Points Manually	5-50
5.8	ONS 15305 SDH Protection Management	5-50
5.8.1	Multiplex Section Protection	5-50
5.8.2	Protect Section by MSP	5-52
5.8.3	Modify MSP	5-53
5.8.4	Delete MSP	5-53
5.8.5	Command an MSP Switch	5-54
5.8.6	Legal Combinations of SNCP and MSP	5-55
5.8.7	SubNetwork Connection Protection	5-55
5.8.7.1	Protect Connection by SNCP	5-55
5.8.7.2	Modify SNCP	5-55
5.8.7.3	Command an SNCP Switch	5-55
5.9	ONS 15302 SDH Protection Management	5-56
5.9.1	Modify MSP Parameters	5-56

CHAPTER 6**Link Aggregation 6-1**

- 6.1 View Link Aggregation - ONS15305 6-1
- 6.2 Modify Link Aggregation - ONS 15305 6-2
 - 6.2.1 Assign a Port to a Trunk 6-3
 - 6.2.2 Trunk Elements used by Management are Named ifindex 6-4

CHAPTER 7**Layer 2 Configuration 7-1**

- 7.1 Bridge 7-1
 - 7.1.1 Configuration of Static Unicast Forwarding Information Example 7-1
 - 7.1.2 Configure Static Multicast Forwarding Information 7-3
 - 7.1.3 Enable IGMP Snooping 7-4
- 7.2 Spanning Tree Protocol (STP) Configuration 7-5
 - 7.2.1 Configure the STP Algorithm per Device 7-5
 - 7.2.2 Configure the STP Algorithm per VLAN 7-6
- 7.3 Rapid Spanning Tree Protocol Configuration 7-6
 - 7.3.1 Configure RSTP on a Port 7-7
- 7.4 MAC Multicast 7-7
 - 7.4.1 Configuring MAC Multicast 7-7
 - 7.4.1.1 MulticastForwarding 7-8
 - 7.4.1.2 MulticastForwardingAll 7-8
 - 7.4.1.3 MulticastForwardUnregistered 7-8
 - 7.4.1.4 MulticastStatic 7-8
- 7.5 Traffic Control 7-9
 - 7.5.1 PortPriority 7-9
 - 7.5.2 PriorityGroup 7-9
 - 7.5.3 TrafficClass 7-10
- 7.6 Manage VLANs 7-10
 - 7.6.1 Virtual Local Area Networks (VLAN) 7-10
 - 7.6.2 Tagged/Untagged LAN Ports 7-11
- 7.7 VLAN Provisioning 7-11
 - 7.7.1 Configure a New VLAN Per Port 7-12
 - 7.7.2 Configure a New VLAN Per Protocol and Per Port 7-13
 - 7.7.3 Configure an Ethernet User Defined Protocol 7-14
 - 7.7.3.1 Use the Ethernet User Defined Protocol 7-14
 - 7.7.3.2 Use Pre-defined Protocols 7-16
 - 7.7.4 Configure VLAN Port members 7-16
 - 7.7.5 GVRP 7-18
- 7.8 Examples 7-19

7.8.1	Configuration of an IP Interface	7-19
7.8.2	Configuration of a Static Route	7-21
7.8.2.1	Create a Static Route	7-21
7.8.2.2	Static Route Example	7-22
7.8.2.3	Configuration of a Default Route	7-23
7.8.2.4	Default Route Example	7-23
7.8.3	Configuration of a RIP Filter	7-24
7.8.3.1	Create an IP RIP Global Filter	7-24
7.8.3.2	IP RIP Global Filter Examples	7-24
7.9	Open Shortest Path First	7-25
7.9.1	Supported OSPF Areas: Transit and Stub Areas	7-25
7.9.2	Configure an OSPF Area	7-25
7.9.3	Configure an OSPF Interface	7-26
7.9.4	Enable OSPF on the Network Element	7-26
7.10	DHCP	7-27
7.10.1	Configure the Range of IP Addresses for the DHCP Server	7-27
7.10.1.1	Configure the DHCP Server for Manual Allocation	7-27

CHAPTER 8

Performance Management 8-1

8.1	G.826 Performance Monitoring Data	8-1
8.2	Counters	8-2
8.3	Criteria for Counting Valid-data in the ONS 15305	8-2

APPENDIX A

Troubleshooting and FAQ A-1

Question 1	A-1
Question 2	A-1
Question 3	A-1
Question 4	A-2
Question 5	A-2
Question 6	A-2
Question 7	A-2
Question 8	A-3
Question 9	A-3
Question 10	A-5
Question 11	A-5

GLOSSARY



FIGURES

Figure 1-1	Install Shield preparing Installation Wizard	1-1
Figure 1-2	Install Wizard - Introduction	1-2
Figure 1-3	Logon Window	1-4
Figure 1-4	Start Window	1-4
Figure 1-5	Starting Cisco Edge Craft	1-8
Figure 1-6	Selection of IP Address - Logon Window	1-8
Figure 1-7	Cisco Edge Craft Logon Window	1-9
Figure 1-8	VT 100 available from Cisco Edge Craft Desktop	1-10
Figure 2-1	Cisco Edge Craft Connection Possibilities	2-1
Figure 2-2	Cisco Edge Craft in Co-existence with Other Management Systems	2-2
Figure 3-1	Cisco Edge Craft Desktop	3-2
Figure 3-2	Up Icon	3-2
Figure 3-3	Stop Icon	3-3
Figure 3-4	Refresh Icon	3-3
Figure 3-5	Copy Icon	3-3
Figure 3-6	Forward Icon	3-3
Figure 3-7	Backward Icon	3-3
Figure 3-8	Save Icon	3-3
Figure 3-9	Add Icon	3-3
Figure 3-10	Delete Icon	3-4
Figure 3-11	Cell Mode Icon	3-4
Figure 3-12	Lock Toolbars	3-4
Figure 3-13	Move Toolbars	3-5
Figure 3-14	File Pull-Down Menu	3-5
Figure 3-15	Edit Pull-Down Menu	3-6
Figure 3-16	View Pull-Down Menu	3-6
Figure 3-17	Equipment Pull-Down Menu	3-7
Figure 3-18	Bridge Pull-Down menu	3-8
Figure 3-19	Tools Pull-Down Menu	3-8
Figure 3-20	Help Pull-Down Menu	3-8
Figure 3-21	The About Dialog Box	3-9

Figure 3-22	Error Icon	3-9
Figure 3-23	Warning Icon	3-9
Figure 3-24	Info Icon	3-10
Figure 3-25	Unmapped Severity Icon	3-10
Figure 3-26	Note Icon	3-10
Figure 3-27	Log Viewer	3-10
Figure 3-28	Log Viewer Tool tip	3-11
Figure 3-29	Example Copy and Paste	3-11
Figure 3-30	Editable Types and Tables - Hyperlinks	3-12
Figure 3-31	Setting the TrapsEnable Attribute	3-13
Figure 3-32	Current Tab - Alarm List	3-13
Figure 3-33	Latest Alarm	3-14
Figure 3-34	Notification History	3-14
Figure 3-35	Select Single Alarm	3-15
Figure 3-36	Select All Alarms	3-15
Figure 3-37	Select Alarms - Continuous Range	3-15
Figure 3-38	Select Alarms - None Continuous Range	3-15
Figure 3-39	Lifecycle Instance of Alarm Point	3-16
Figure 3-40	Select Events	3-17
Figure 3-41	Current Events	3-17
Figure 3-42	Event History	3-17
Figure 3-43	Visible Columns 1	3-18
Figure 3-44	Visible Columns 2	3-18
Figure 3-45	Column Order	3-19
Figure 3-46	Column Resize	3-19
Figure 3-47	Column Sorting	3-20
Figure 3-48	Trap to Notification Mapping	3-22
Figure 4-1	Management Interfaces - Managed Object	4-2
Figure 4-2	ManagementPort - Attributes	4-2
Figure 4-3	ManagementPort - Mode Selector	4-3
Figure 4-4	ManagementPort - IP Address Attribute	4-3
Figure 4-5	ManagementPort - Add IP Address	4-3
Figure 4-6	Management Interfaces - Dcc Attribute	4-4
Figure 4-7	IPEncapsulation - Encapsulation Selector	4-5
Figure 4-8	Cisco Edge Craft and ONS 15305 on the Same Subnet	4-7

Figure 4-9	Cisco Edge Craft and ONS 15305 on Different Subnets	4-8
Figure 4-10	IP over DCC	4-9
Figure 4-11	IP over PPP	4-10
Figure 4-12	Identification of Network Element	4-12
Figure 4-13	Time Settings - Time Attribute	4-13
Figure 4-14	Time Attribute - Values	4-13
Figure 4-15	Time Attributes - System Time	4-13
Figure 4-16	Add a New User - Overview	4-14
Figure 4-17	Available Features	4-15
Figure 4-18	Physical Inventory - Overview	4-16
Figure 4-19	Restart of Network Element - Overview	4-17
Figure 4-20	Clear Alarm- and Performance Data Log	4-18
Figure 4-21	LEDs - Severity Selector	4-19
Figure 4-22	Ping Mechanism	4-19
Figure 4-23	Alarm Ports	4-20
Figure 4-24	AUX Port	4-20
Figure 4-25	AUX port - Timeslots	4-21
Figure 4-26	Power Module - Attributes	4-21
Figure 4-27	Synchronization Network Example	4-23
Figure 4-28	T0 Selection	4-24
Figure 4-29	T4 Selection	4-26
Figure 4-30	Synchronization - Selecting Managed Object	4-28
Figure 4-31	Synchronization - T0 SynchSources attribute	4-28
Figure 4-32	Add Synchronization Source	4-29
Figure 4-33	Operate Synchronization Switch 1	4-30
Figure 4-34	Operate Synchronization Switch 2	4-30
Figure 4-35	View Synchronization Switch	4-31
Figure 4-36	Select Synchronization	4-31
Figure 4-37	Select AdministrativeSynchSource	4-32
Figure 4-38	Example of Switching Software Banks	4-33
Figure 4-39	Download of Release Files	4-34
Figure 4-40	Select Device	4-35
Figure 4-41	Select ConfigData	4-36
Figure 4-42	Select Device	4-38
Figure 4-43	General Alarm Reporting Filters.	4-39

Figure 4-44	Select Device	4-44
Figure 4-45	Select Alarm Config	4-44
Figure 4-46	Select AlarmReportingAll	4-44
Figure 4-47	Select AlarmReporting	4-45
Figure 4-48	Select AlarmreportingAisRdi	4-45
Figure 4-49	Select AIS Attributes	4-45
Figure 4-50	Set Alarm Persistency Attributes	4-46
Figure 4-51	Select SDTreshold	4-46
Figure 4-52	Set SDTreshold	4-46
Figure 4-53	ONS 15305 Slots	4-47
Figure 4-54	Select Slot	4-47
Figure 4-55	Slot Module - Port Concept	4-47
Figure 4-56	Relation Between Installed and Expected Module in a Slot.	4-48
Figure 4-57	Select Target Slot	4-49
Figure 4-58	Set View Mode to Children	4-50
Figure 5-1	Select the Aug1 Managed Object	5-2
Figure 5-2	Set the Structure Attribute	5-2
Figure 5-3	Set the E1 Mode Attribute	5-8
Figure 5-4	Set Loop Mode Attributes	5-8
Figure 5-5	Assign VC 12 Port	5-10
Figure 5-6	Select Interval24Hour	5-11
Figure 5-7	Set Interval24Hour Attributes	5-12
Figure 5-8	LAN Port Attributes	5-13
Figure 5-9	LAN Port Attributes - ONS 15302	5-14
Figure 5-10	The 8 x STM-1 Module with WAN Ports	5-15
Figure 5-11	View of one WAN Port and its Logical View	5-15
Figure 5-12	Sequence Numbers for Correct Order of TU-12 to VC-12 Cross Connects.	5-16
Figure 5-13	Set Bandwidth	5-17
Figure 5-14	Select WAN Port Attributes	5-17
Figure 5-15	Set WAN Port Attributes	5-18
Figure 5-16	Select Available VC/TU12	5-18
Figure 5-17	Select WAN Channels	5-20
Figure 5-18	Select Protected Mode	5-21
Figure 5-19	Set SNCP Properties Enabled	5-22
Figure 5-20	Set SNCP Properties Protection	5-23

Figure 5-21	Set SNCP Properties Command	5-23
Figure 5-22	View of the WAN Ports and their Logical View	5-27
Figure 5-23	Set Bandwidth	5-28
Figure 5-24	Select a WAN port	5-28
Figure 5-25	Set WAN Attributes	5-29
Figure 5-26	Select Available VC/TU12 Container	5-29
Figure 5-27	Delete WAN Port	5-31
Figure 5-28	SDH Layer Network	5-34
Figure 5-29	SDH Multiplexing Structure	5-35
Figure 5-30	Slot - Port - CTP Relations	5-37
Figure 5-31	Largest Possible Cross Connect Matrix	5-37
Figure 5-32	Unidirectional XC, Unprotected	5-38
Figure 5-33	Unidirectional XC, Protected	5-38
Figure 5-34	Bidirectional XC, Unprotected	5-39
Figure 5-35	Bidirectional, Protected	5-39
Figure 5-36	Example of Bidirectional, Unprotected, Point-to-Point XC	5-39
Figure 5-37	Example of Bidirectional, Protected, Point-to-Point XC	5-40
Figure 5-38	XC Fabric	5-40
Figure 5-39	Select Cross Connect	5-41
Figure 5-40	Select SDH Port Cross Connect	5-41
Figure 5-41	Select XCFabric Cross Connect	5-41
Figure 5-42	Cross-Connection GUI - Overview	5-42
Figure 5-43	Example of Filtering Criteria - Cross-Connections	5-43
Figure 5-44	Select Synchronize	5-44
Figure 5-45	Select the VC/TU12 Tab	5-44
Figure 5-46	Select the VC/TU12 Tab	5-45
Figure 5-47	Select Enabled Attributes	5-47
Figure 5-48	Select SNCP Command	5-48
Figure 5-49	1+1 MSP Between two ONS 15305	5-51
Figure 5-50	Protection Switching Scenarios	5-51
Figure 5-51	Select SDH Port	5-52
Figure 5-52	Select MSP Object	5-52
Figure 5-53	Select Protection Port Attributes	5-52
Figure 5-54	Select MspCommands Attribute	5-54
Figure 5-55	Select SDH1/MSP1 Attributes	5-56

Figure 5-56	Set MSP Command	5-57
Figure 6-1	Attributes Related to Link Aggregation	6-2
Figure 6-2	Creating and Editing a Trunk to a VLAN	6-4
Figure 6-3	VLAN settings for a Trunk with GE	6-5
Figure 7-1	Configuration of Static Unicast Forwarding Information	7-2
Figure 7-2	Configuration of Static Multicast Forwarding Information	7-3
Figure 7-3	Enabling IGMP Snooping	7-5
Figure 7-4	VLAN GUI - Overview	7-12
Figure 7-5	VLAN Settings	7-12
Figure 7-6	Add a VLAN	7-13
Figure 7-7	Set VLAN Attributes	7-13
Figure 7-8	Add a VLAN	7-14
Figure 7-9	Configure a VLAN	7-14
Figure 7-10	Configuration of an Ethernet User Defined Protocol	7-15
Figure 7-11	Configuration of VLAN Port members	7-17
Figure 7-12	Edit the Bridge Port Number	7-17
Figure 7-13	GVRP Attributes	7-18
Figure 7-14	Select Legal Time Values	7-19
Figure 7-15	Configuration of an IP Interface	7-20
Figure 7-16	Create a Static Route	7-22
Figure 7-17	Figure - Static Route in Router R1	7-23
Figure 8-1	View PM - Example	8-2
Figure A-1	VLAN Calculation	A-2
Figure A-2	IEEE 802.1Q Tag header (VLAN tag)	A-3
Figure A-3	Adjustment of VLAN/GVRP entries	A-4
Figure A-4	Definition of a Set of Ports Through an Octet String	A-5
Figure A-5	Common UDP Ports	A-6



Table 1-1	CLI Connector Pinout (RJ-45 to DS-9)	1-3
Table 2-1	Cisco Edge Craft Capabilities	2-2
Table 3-1	File Menu	3-5
Table 3-2	Edit Menu	3-6
Table 3-3	ViewMenu	3-6
Table 3-4	Equipment Menu	3-7
Table 3-5	Bridge Menu	3-8
Table 3-6	Tools Menu	3-8
Table 3-7	Help Menu	3-9
Table 3-8	Alarm Notification Types and their Attributes	3-20
Table 3-9	Event Notification Types and their Attributes	3-21
Table 4-1	Management Modes Versus Management Interface	4-1
Table 4-2	Cisco Edge Craft and ONS 15305 on the Same Subnet - Settings	4-7
Table 4-3	Cisco Edge Craft and ONS 15305 on Different Subnet - Settings	4-8
Table 4-4	IP Over DCC - Settings	4-9
Table 4-5	IP Over PPP- Settings	4-10
Table 4-6	Alarms Related to SDH Synchronization Events	4-27
Table 4-7	Persistency Group 1 (HighOrderLevel)	4-42
Table 4-8	Persistency Group 2 (Unfiltered)	4-43
Table 4-9	Persistency Group 3 (LowOrderLevel)	4-43
Table 5-1	CBKLM Value Usage	5-35
Table 7-1	VLAN Protocol	7-16
Table 8-1	Managed Objects	8-1
Table A-1	Octet String and Corresponding Set of Ports	A-5
Table A-2	Link State Type (according to RFC2328, Appendix A.4.1)	A-6



Installing Cisco Edge Craft

This chapter describes how to install the Cisco Edge Craft and how to start the VT100 terminal.

1.1 Install Cisco Edge Craft Using the Install Wizard

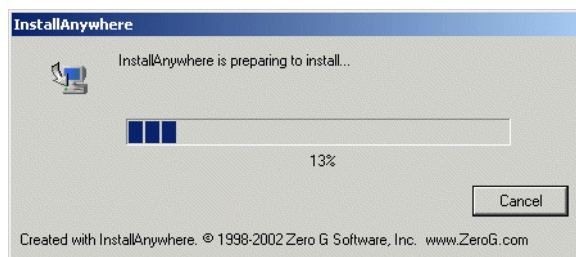
Step 1 Insert the Cisco Edge Craft SW CD in desired drive on target PC.



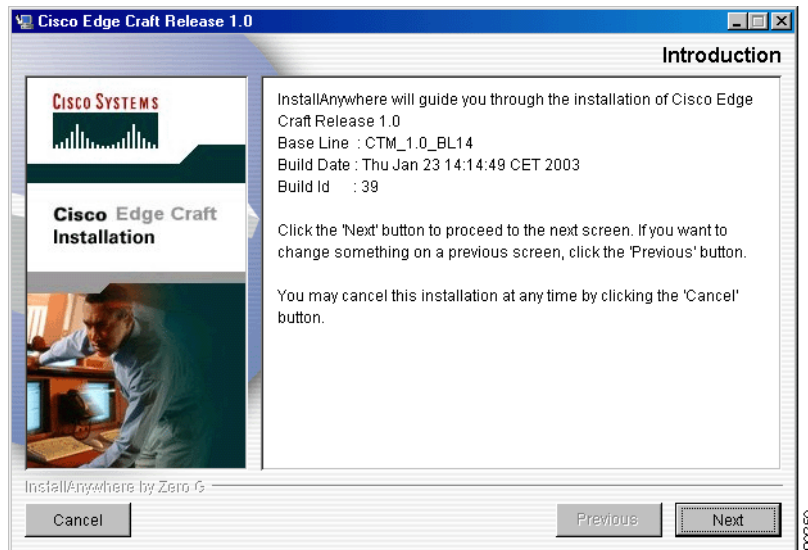
Note Required diskspace for the Cisco Edge Craft installation is minimum 65 Mb.

Step 2 Run `ciscocraft.exe`; the Cisco Edge Craft Install shield launches ([Figure 1-1](#)).

Figure 1-1 *Install Shield preparing Installation Wizard*



Step 3 Follow the instructions given in the Install wizard ([Figure 1-2](#)).

Figure 1-2 Install Wizard - Introduction

1.2 Un-install Cisco Edge Craft

-
- Step 1** Select Start > Programs > Cisco Edge Craft > uninstall and follow the instructions given on the screen.
- or
- Step 2** Select Start > Settings > Control Panel > Add/Remove Programs and choose Cisco Edge Craft.
-

1.3 Commission IP Address via the VT100 Interface

A local terminal with VT100 emulation is required during the first commission of the network element to set up the necessary communications parameters enabling access to the NE via Cisco Edge Craft over the management port. After the first commission, the VT100 interface can be used for modifying the communications parameters and to perform status checks of the network element. The VT100 interface is password protected.

ONSCLI is a line-oriented ASCII-based management interface embedded in the Cisco network element. The ONSCLI is accessed via the VT100-port. The serial connection communications parameters are fixed:

- 19200 bits
- no parity
- 8 bits
- 1 stop bit
- no hardware flow control

VT100 terminal codes are used.

The VT100-port (Console port) for the Cisco network element is provided using a RJ-45 connector. A cable for connecting the VT100-port to the serial-port on the PC is available. [Table 1-1](#) provides the pinouts.

Table 1-1 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

**Note**

Pins 4, 5 and 7 are used only for debugging purposes.

1.3.1 Invoke ONSCLI

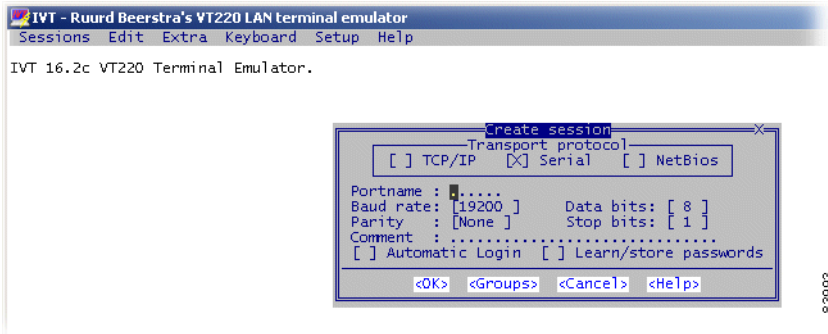
- Step 1** Connect the VT100 interface of the network element to a free COM port of the PC running the Cisco Edge Craft application.
- Step 2** A VT100 terminal application is available from the Cisco Edge Craft Logon window. Select Program > Cisco Edge Craft > Cisco Edge Craft.
- Step 3** Double-click the VT100 icon in the lower right corner of the Logon window ([Figure 1-3](#)).

Figure 1-3 Logon Window



The terminal application launches (Figure 1-4).

Figure 1-4 Start Window



Step 4 Enter the **COM port** name and click **OK**.

Step 5 An ONSCLI session is invoked by typing **onscli** in terminal window. User authentication (a password, 6 to 12 ASCII characters) is required, as the following session start-up sequence shows. The default password is ONSCLI.

```
>ONSCLI
-----
ONS 15305 Command Line Interface
-----

Enter ONSCLI password: *****
ONSCLI>
```

Step 6 When access has been granted, you can define the following parameters:

```
IP-Configuration(Management-Port):
Show-Current-Alarms:
Community-handler:
```

Exit:

It is sufficient to type leading characters of the command name to avoid ambiguity – the same applies to keywords.



Note The backspace or delete key can be used to edit the command line. Commands and keywords are not case-sensitive.

The management port IP address is a compulsory parameter, and must be specified by the user. All the other parameters (except default gateway) default to pre-defined values if they are not specified.

1.3.2 Configure Community-Handler

The following parameters settings are shown for both the Cisco ONS 15305 and the Cisco ONS 15302.

The following example shows how to set the community handler for a default user. When setting community handler for a specific user, the corresponding IP address must be entered instead of 0.0.0.0.

1.3.2.1 ONS 15305

-
- Step 1** Enter the following command:
- ```
ONSCLI>com
```
- Step 2** Press **Enter**.
- Step 3** Enter the following command:
- ```
ONSCLI>Community-handler\ll
```
- Step 4** Press **Enter**. The following text appears:
- ```
Add: Add Community entry
Edit: Edit Community entry
Remove: Remove Community entry
Show: Show Community entry
Exit:
ONSCLI>Community-handler\
```
- Step 5** Enter the following command:
- ```
ONSCLI>Community-handler\add man=0.0.0.0 com=public acc=super traps=disable
```
- Step 6** Press **Enter**. The following text appears:
- ```
MANAGER: 0.0.0.0
COMMUNITY: public
ACCESS: super
TRAPS: disable
ONSCLI>Community-handler\
```
- 

### 1.3.2.2 ONS 15302

The pre-configured factory community appears as follows:

```

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

```

This is an insecure community, meaning it enables all managers, regardless of the IP-address, to access the device with the public community string.

- 
- Step 1** To add your own community string, enter the following command:  
*ONSCli>Security\Community-Table\add manager=10.0.0.20 community=admin access=super traps=enable*
- Step 2** Press **Enter**.
- 

## 1.3.3 Assign an IP Address

This section explains how to assign an IP address to an ONS 15305 or ONS 15302.

### 1.3.3.1 ONS 15305

ONSCli>**ip ?**

Usage:

IP-Configuration(Management-Port)

```

[IP-ADDRESS=<IP address>]
[SUBNET-MASK=<IP address>]
[DEFAULT-GATEWAY=<IP address>]

```

Available independent of router license

```
[MODE=<notUsed|ip|clnp|ipAndClnp>]
```

Management mode for the management port

lclnplipAndClnpl only with OSI license

```

ONSCli>ip
IP-ADDRESS: 10.20.47.131
SUBNET-MASK: 255.255.254.0
DEFAULT-GATEWAY: 10.20.47.254
MODE: ip
STATUS: up
Management port Status

```

ONSCli>

To configure the device by setting the IP address to the management port, complete the following steps.

- 
- Step 1** Enter the following command: *ONSCli>ip ip=192.168.2.2 sub=255.255.255.252 def=192.168.2.1.*



```
--- Change IP address, are you sure (y/n)? y
IP-ADDRESS: 192.168.2.2
SUBNET-MASK: 255.255.255.252
DEFAULT-GATEWAY: 192.168.2.1
```

**Step 2** Press **Enter**.

---

### 1.3.3.2 ONS 15302

---

**Step 1** Enter the following command:

```
ONSCLI>Device\Management-Configuration\Custom\Management-Port\IP-Configuration
ip-address=10.0.0.1 subnet-mask=255.255.255.0 default-gateway=10.0.0.254
```

**Step 2** Press **Enter**.

**Step 3** Verify the intention of the operation by pressing **y**. The following text appears:

```
IP-ADDRESS: 10.0.0.1
SUBNET-MASK: 255.255.255.0
DEFAULT-GATEWAY: 10.0.0.254
```

**Step 4** Type **exit** to terminate the session.

---

## 1.3.4 Change Passwords

This section explains how to change passwords for the ONS 15305 or ONS 15302.

### 1.3.4.1 ONS 15305

---

**Step 1** Enter the following command:

```
ONSCLI>ch ?
```

The following text appears.

```
[ONSCLI -PASSWORD=<string[6:12]>]
[TELNET-PASSWORD=<string[6:12]>]
```

**Step 2** Use this command to change TELNET and ONSCLI passwords. Both passwords can be changed in the same command or they can be changed one by one.

---

### 1.3.4.2 ONS 15302

---

**Step 1** Enter the following command:

```
ONSCLI>Security\Community-Table>ch ?
```

The following text appears:

```
[ONSCLI -PASSWORD=<string[6:12]>]
```

[TELNET-PASSWORD=<string[6:12]>]

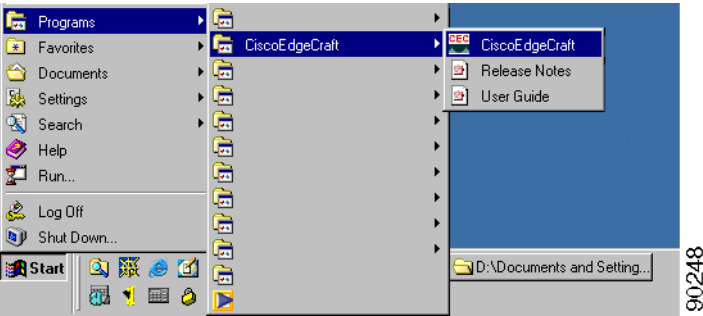
- Step 2** Use this command to change TELNET and ONSCLI passwords. Both passwords can be changed in the same command or they can be changed one by one.

# 1.4 Connect to a Network Element

The purpose of this section is to describe the tasks involved in setting up a connection between the craft terminal and any Cisco network element. See also the “1.3 Commission IP Address via the VT100 Interface” section on page 1-2.

- Step 1** Select Program > Cisco Edge Craft > Cisco Edge Craft (Figure 1-5).

Figure 1-5 Starting Cisco Edge Craft



A logon window appears.

- Step 2** Enter the community password.
- Step 3** If it is present, select the desired network element from the **Ip** pull-down menu (Figure 1-6).

Figure 1-6 Selection of IP Address - Logon Window



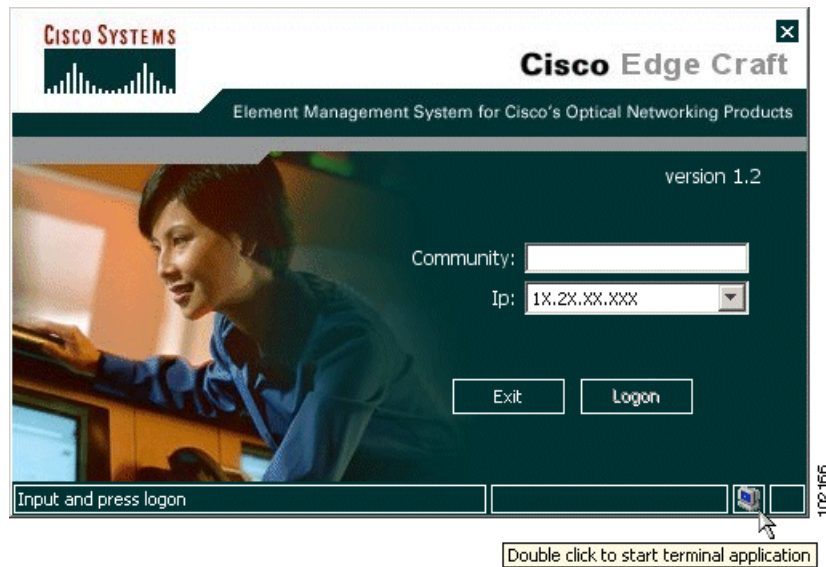
The system adds the selected IP address to the logon window. You can also fill in the IP address manually (Figure 1-7).

**Step 4** Click **Logon** to continue.

The network element supports three community access levels

- ReadOnly - only read access to the whole MIB
- ReadWrite - read and write to the MIB, but can not change community strings
- Super - read and write to the complete MIB.

**Figure 1-7 Cisco Edge Craft Logon Window**



**Step 5** The system validates the community string and IP address combination. If it is valid, meaning the combination is correct and the SNMP community string is valid, the craft terminal sets up a connection to the specified IP address. The desktop of the craft terminal with its working windows appears.

You can now browse the network element topology and perform the required management tasks.

If the community string is invalid, access to the network element is not granted and an error message is presented.

If the IP address you entered manually or selected in the list is not reachable/non-existent or does not belong to an Cisco network element, the system generates an error message and asks for a new IP address.

## 1.5 Configure the VT100 Terminal

The VT100 terminal can be launched from the Cisco Edge Craft desktop (Figure 1-8) or the logon window (Figure 1-7).

**Figure 1-8** VT 100 available from Cisco Edge Craft Desktop

You can change the terminal software that will be launched by editing the VT 100 path description in the ExternalApplications.xml file, found in the install\dir\CISCOEDGE CRAFT\res\config\folder:.

The following is an example of the ExternalApplications.xml file:

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
- <ExternalApplications>
 <vt100 file="../external/IVT VT220 Telnet/ivt.exe" />
 <exec file="rundll32 url.dll,FileProtocolHandler" />
 <editor file="notepad.exe" />
 <fileexplorer file="explorer.exe" />
 <web file="rundll32 url.dll,FileProtocolHandler" />
 <ciscoweb file="rundll32 url.dll,FileProtocolHandler" params
 ="http://www.cisco.com" />
 <help file="rundll32 url.dll,FileProtocolHandler" params="
 ../res/help/CEC1-0.pdf" />
 <releasenotes file="rundll32 url.dll,FileProtocolHandler" params="
 ../res/help/CECRN10.pdf" />
</ExternalApplications>
```



# Software Description

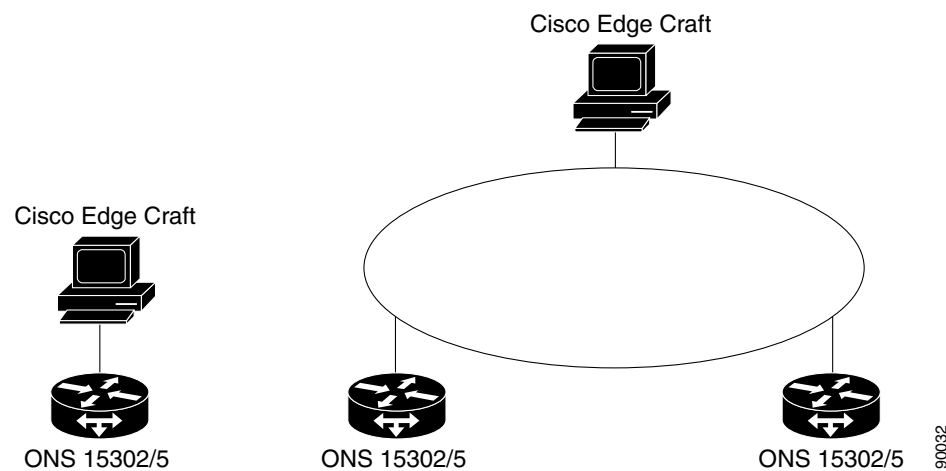
This section gives an overview of the Cisco Edge Craft.

## 2.1 Introduction

Cisco Edge Craft is used to operate a single network element and provides a real-time snapshot of the network element. Cisco Edge Craft can only present and work on information that is stored on the network element. A user must be logged into the Cisco Edge Craft graphical user interface (GUI) for it to function. The GUI presents alarms if Cisco Edge Craft is connected to the network element. Performance data can be loaded from the network element.

Cisco Edge Craft is a single user system. It is a standalone application running on Windows or Solaris platforms. Cisco Edge Craft is not dependent on any other system to be able to perform its tasks. The laptop or a PC where Cisco Edge Craft is running can be attached to the network element directly through the management port or through a LAN ([Figure 2-1](#)).

**Figure 2-1 Cisco Edge Craft Connection Possibilities**



Cisco Edge Craft can co-exist with other management products from Cisco ([Figure 2-2](#)). The SNMP Agent used by Cisco Edge Craft for communication with the network element handles multiple SNMP managers.

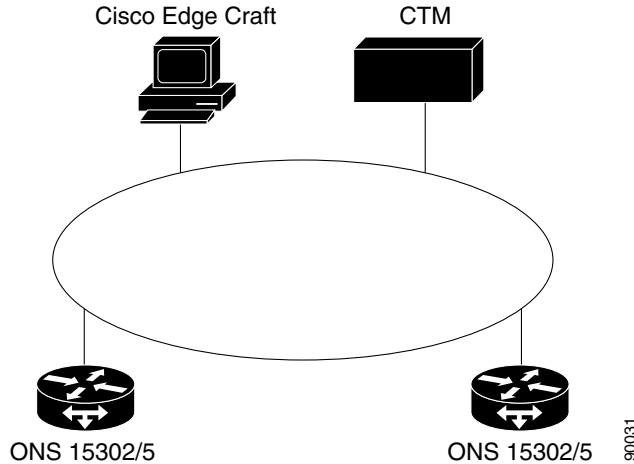
**Figure 2-2 Cisco Edge Craft in Co-existence with Other Management Systems**

Table 2-1 displays the capabilities of the Cisco Edge Craft.

**Table 2-1 Cisco Edge Craft Capabilities**

Customer Benefit	Supporting Features
Support for configuration of network element for no extra cost, to get it into operation quickly.	All necessary configuration of network element can be done by Cisco Edge Craft.
Part of Cisco Family of products and therefore easy to upgrade to EMS or NMS level.	Cisco Edge Craft has the same look and feel as the other products in the family and uses a sub-set of components from the Cisco component collection.
Easy access to network element	Can run on a laptop.
Can access network elements both locally and remote.	Communication on management port (IP) to the embedded SNMP Agent in the network element.

## 2.2 Product Features

Some of the feature listed here are only applicable to Cisco Edge Craft (CEC) if the feature is available on the network element.

### 2.2.1 Network Element Access

CEC communicates with the network element through the embedded SNMP Agent. To establish this communication line the network element must have an IP address. If an IP address has not been assigned, a separate communication line on the serial port can assign the IP address and other related parameters.

### 2.2.2 Information Model

CEC has its own internal representation (information model) of the network elements. This is an object-oriented model and is identical to the information model used by all Cisco products.

## 2.2.3 Single User

Only one user can be logged into CEC at one time.

## 2.2.4 Single Network Element

CEC can only communicate with one network element at a time. The user must close the connection to one NE before connecting to a new NE.

## 2.2.5 Graphical User Interface Types

The GUI presents the network element in accordance with the information model and has no knowledge about the SNMP MIBs used by the embedded Agent.

The GUI cannot be customized by the user.

CEC has two different types of graphical user interfaces (GUI):

- The Network Element Topology Browser (NETB) is a hierarchical presentation of the managed objects in the network element.
- The custom GUI is developed to support a specific task or function.

## 2.2.6 No Persistency

CEC has no persistent storage of operations and notifications.

## 2.2.7 List of Possible Network Element IP Addresses

CEC stores the IP address of accessed network elements. The operator can choose the IP address of the current network element in the start up window for CEC.

## 2.2.8 Configuration Download and Upload

CEC can initiate upload of the complete configuration from one network element and store it on the local or remote computer. The remote computer is identified by its IP address.

CEC can initiate download of the complete configuration from a local or remote computer to the network element. The remote computer is identified by its IP address.

The uploaded configuration cannot be edited.

## 2.2.9 Software, Firmware and Licenses Download

CEC can initiate download of software, firmware, and licenses on the network element. The location of the software, firmware, and licenses can either be on the same computer as CEC or on a remote computer. The remote computer is identified by its IP address; both the local and remote computers must be TFTP servers.

The restart of the equipment that uses new downloaded software/firmware can be scheduled.

## 2.2.10 User Access

CEC supports user authentication through user identification (community string).

Initial access of the network element is through public access.

## 2.2.11 Alarm and Event Notifications Presentation

CEC presents all alarms and events that are generated while the user is logged into CEC. The alarms are presented in a tabular view. If the received traps from the network element cannot be mapped to an alarm or an event, the trap is still presented to the operator.

CEC presents the alarm history stored on the network element. The alarm history is presented in a tabular view.

## 2.2.12 Presentation of Performance Data

CEC has no analysis of performance management data.

The user can read the current registered performance data on the network element, view it in a GUI, and copy it to file. The file can be read or edited in any word processing tool, such as Microsoft Excel.

Supported performance data are: G.826, MIB-II (RFC1213), and RMON counters.

## 2.2.13 Management Configuration

CEC supports configuration of the DCN management traffic settings.

## 2.2.14 Physical Inventory

The physical inventory gives an overview of the installed parts on the network element and the currently running software or firmware. Software and firmware packages that have been downloaded but not activated are also presented.

## 2.2.15 Logical Inventory

The logical inventory gives an overview of the managed entities in the network element. The logical entities may agree with the physical parts, but not necessarily.

## 2.2.16 Global Settings

The network element has some configurations that are not related to the user traffic on the network element. These are parameters such as location, owner, time server, LED settings, power modules.



## 2.2.17 Alarm and Event Filtering Configuration

The alarm reporting from some managed entities on the network elements can be filtered out.

## 2.2.18 SDH Ports Configuration

CEC supports configuration of the SDH ports. The SDH ports have two main configuration areas.

- Properties of the ports. The properties can be viewed and edited.
- Structuring of the ports

## 2.2.19 PDH Ports Configuration

CEC supports configuration of PDH port properties. The properties can be viewed and edited.

## 2.2.20 MSP and SNCP Configuration

CEC supports MSP and SNCP set up, which means the user can view, create, modify, and delete.

## 2.2.21 SDH Synchronization Configuration

The network element can have more than one synchronization source for the SDH traffic. The sources are prioritized. CEC helps the user in the set up of these rules.

## 2.2.22 LAN Ports Configuration

CEC supports the configuration of LAN port properties. The properties can be viewed and edited.

## 2.2.23 WAN Ports Configuration

CEC supports configuration of WAN port properties. The properties can be viewed and edited. CEC also supports configuration of WAN bandwidth.

## 2.2.24 Test Loops Configuration

CEC supports configuration of test loops.

## 2.2.25 Cross-Connect (XC) Configuration

CEC supports cross connection management for the SDH ports. The cross-connects can be set, deleted, and updated. Two supported cross-connects are point-to-point and WAN to SDH mapping.

## 2.2.26 Bridge Configuration

CEC supports bridge set up.

## 2.2.27 VLAN Configuration

CEC supports VLAN configuration, meaning the user can create, remove, and update VLANs.

## 2.2.28 Security

The security of Cisco Edge Craft is based on the SNMP v.1 security (community string).

## 2.2.29 Data Communication

Cisco Edge Craft can communicate with the network elements

- Directly on the management port
- The management port connected to a VLAN
- Via the inband DCC

## 2.2.30 Reliability

This section lists the reliability requirements and know bugs on CEC.

One or more Cisco Edge Craft users can be connected to the same network element at the same time if the network element is connected to a LAN, but the users they will have no visibility to each other.

Known bugs are presented with a workaround in the release notes.

## 2.2.31 Maintenance

Debugging and system logging are realized through log4j, open source code.

### 2.2.31.1 Debugging

- All components in CEC have a debugging interface.
- The components can log different information decided by the debug level.
- The components have one debug level.

### 2.2.31.2 System Logging

- All system errors are logged.
- CEC error messages include a text description of the error, the operating system error code (if applicable), the module detecting the error condition, and a time stamp.

- If configured, all system errors are retained in the Error Log Database.

### 2.2.31.3 New Releases and Patches

The new releases or patches are available for download from the support pages on <http://www.cisco.com>.





## Using Cisco Edge Craft

---

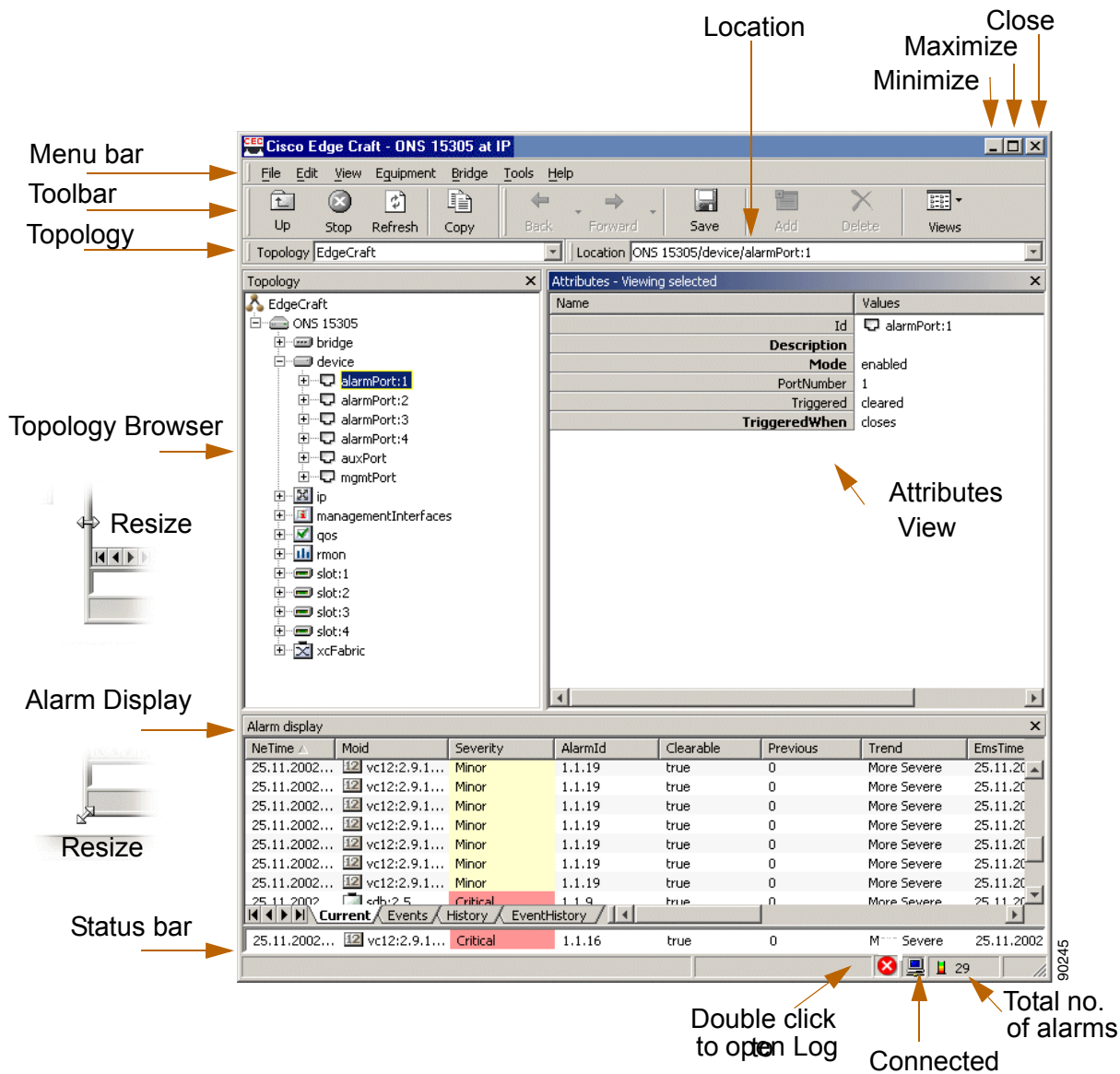
The graphical user interface of Cisco Edge Craft is built on the Cisco GUI framework and is delivered pre-customized to show a network element topology browser, attributes, and an alarm list.

The alarm list displays all alarms, events and notifications that occur while Cisco Edge Craft is connected to the network element.

### 3.1 Cisco Edge Craft Desktop

[Figure 3-1](#) gives an overview of the Cisco Edge Craft desktop with explanation of the functionality. The status bar will display a description of selected toolbar buttons or menu items.

Figure 3-1 Cisco Edge Craft Desktop



### 3.1.1 Toolbar Buttons

Figure 3-2 to Figure 3-11 show the functionality of the toolbar icons available in the Cisco Edge Craft.

Figure 3-2 Up Icon



This icon moves the topology up one level.

**Figure 3-3 Stop Icon**

This icon stops the current operation.

**Figure 3-4 Refresh Icon**

This icon refreshes the active view.

**Figure 3-5 Copy Icon**

This icon copies selected rows to the system clipboard.

**Figure 3-6 Forward Icon**

This icon moves the view forward in the Attributes Viewer.

**Figure 3-7 Backward Icon**

This icon moves the view backward in Attributes Viewer.

**Figure 3-8 Save Icon**

This icon saves the content of the Attributes View on the equipment.

**Figure 3-9 Add Icon**

This icon adds a new row to the Attributes Viewer.

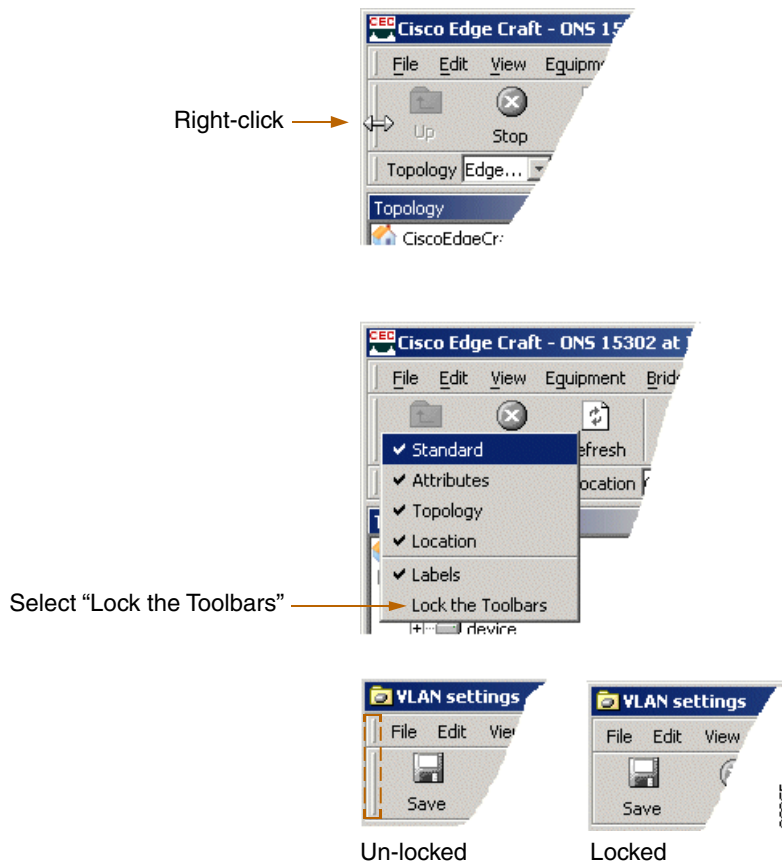
**Figure 3-10 Delete Icon**

This icon deletes selected items.

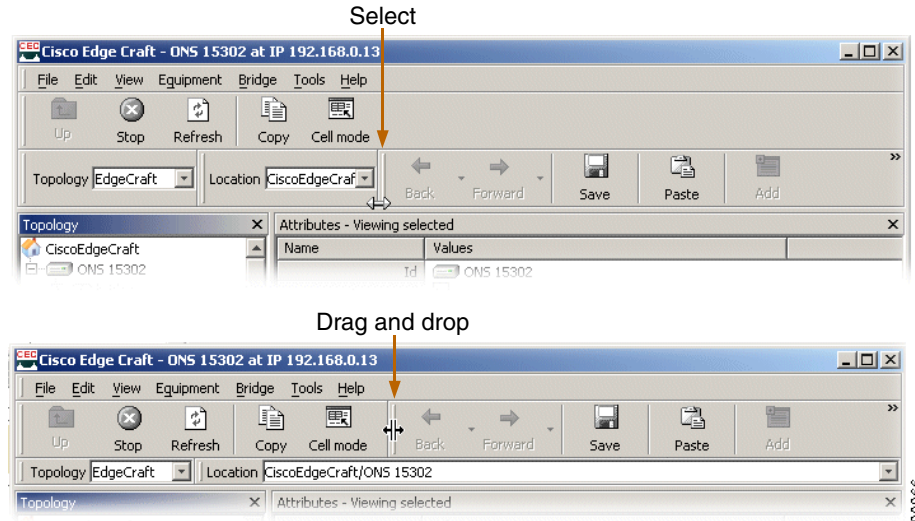
**Figure 3-11 Cell Mode Icon**

By default, entire rows are selected in the table, but single cells can easily be selected using the cell-mode toggle button.

Figure 3-12 and Figure 3-13 show how to lock and move toolbars.

**Figure 3-12 Lock Toolbars**

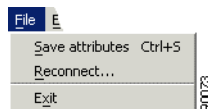


**Figure 3-13 Move Toolbars**

## 3.1.2 Menu Items

### 3.1.2.1 File

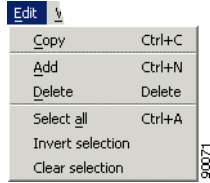
Figure 3-14 and Table 3-1 show and describe the File menu.

**Figure 3-14 File Pull-Down Menu****Table 3-1 File Menu**

Menu item	Action
Save	Save contents.
Reconnect	Reconnect to equipment.
Exit	Exit Cisco Edge Craft.

### 3.1.2.2 Edit

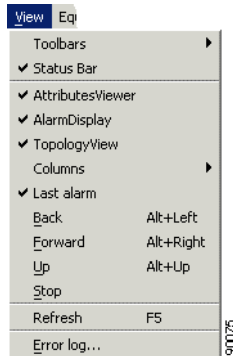
Figure 3-15 and Table 3-2 show and describe the Edit menu.

**Figure 3-15 Edit Pull-Down Menu****Table 3-2 Edit Menu**

Menu item	Action
Copy	Copy selected items to system clipboard.
Paste	Paste copied content
Add	Add row.
Delete	Delete selected item(s).
Select all	Select all items in active the active view.
Invert selection	Invert current selection in the active view.
Clear selection	Clear current selection.

### 3.1.2.3 View

Figure 3-16 and Table 3-3 show and describe the View menu.

**Figure 3-16 View Pull-Down Menu****Table 3-3 ViewMenu**

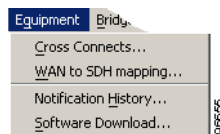
Menu item	Action
Toolbars	Standard: Check to make standard toolbar active. Attributes: Check to make attributes toolbar active. Labels: Check to make labels visible on tool buttons.
Status bar	Check to make status bar visible in the bottom of Cisco Edge Craft desktop.
Alarm Display	Check to make alarm display an active application on the desktop.

**Table 3-3 ViewMenu**

Menu item	Action
Topology View	This option makes the topology view an active application on the desktop.
Attributes	This option makes the attributes viewer an active application on the desktop.
Columns	This option toggles visible columns in the alarm display. See the <a href="#">“3.3.3.3 Visible Columns”</a> section on page 3-17.
Last Alarm	This option allows the user to view the last alarm in a separate window in the alarm display.
Back	This option moves CEC back.
Forward	This option moves CEC forward.
Up	This option moves CEC up one level.
Stop	This option stops current operation.
Refresh	This option refreshes the active view.
Error Log	<p>This option opens an error log.</p> <p>The log is also available from the status bar.</p> <p>These symbols indicate severity in the status bar; if the log contains messages see <a href="#">Figure 3-22</a> to <a href="#">Figure 3-25</a>.</p> <p>Double-click the current symbol to view the log.</p>

### 3.1.2.4 Equipment

[Figure 3-17](#) and [Table 3-4](#) show and describe the Equipment menu.

**Figure 3-17 Equipment Pull-Down Menu****Table 3-4 Equipment Menu**

Menu item	Action
Cross Connect	<p>This option opens the cross-connect.</p> <p>See the <a href="#">“5.7 ONS 15305 SDH Layer Network and Cross-Connections”</a> section on page 5-33 for details.</p>
WAN to SDH mapping	<p>This option opens the WAN to SDH mapping.</p> <p>See the <a href="#">“5.5.2 Add Initial WAN Port Capacity”</a> section on page 5-16 for details.</p>
Notification History	<p>This option opens the Notification History.</p> <p>See the <a href="#">“3.3.2.2 History”</a> section on page 3-14.</p>

### 3.1.2.5 Bridge

Figure 3-18 and Table 3-5 show and describe the Bridge menu.

**Figure 3-18 Bridge Pull-Down menu**



**Table 3-5 Bridge Menu**

Menu item	Action
VLAN Settings	This option opens the VLAN Settings. See the “ <a href="#">7.7 VLAN Provisioning</a> ” section on <a href="#">page 7-11</a> for details on VLAN Settings.

### 3.1.2.6 Tools

Figure 3-19 and Table 3-6 show and describe the Tools menu.

**Figure 3-19 Tools Pull-Down Menu**



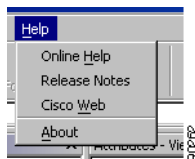
**Table 3-6 Tools Menu**

Menu item	Action
VT 100 Terminal	This option launches the VT100 terminal (if configured). See the “ <a href="#">1.5 Configure the VT100 Terminal</a> ” section on <a href="#">page 1-9</a> for details.
Text Editor	This option opens the Text Editor.

### 3.1.2.7 Help

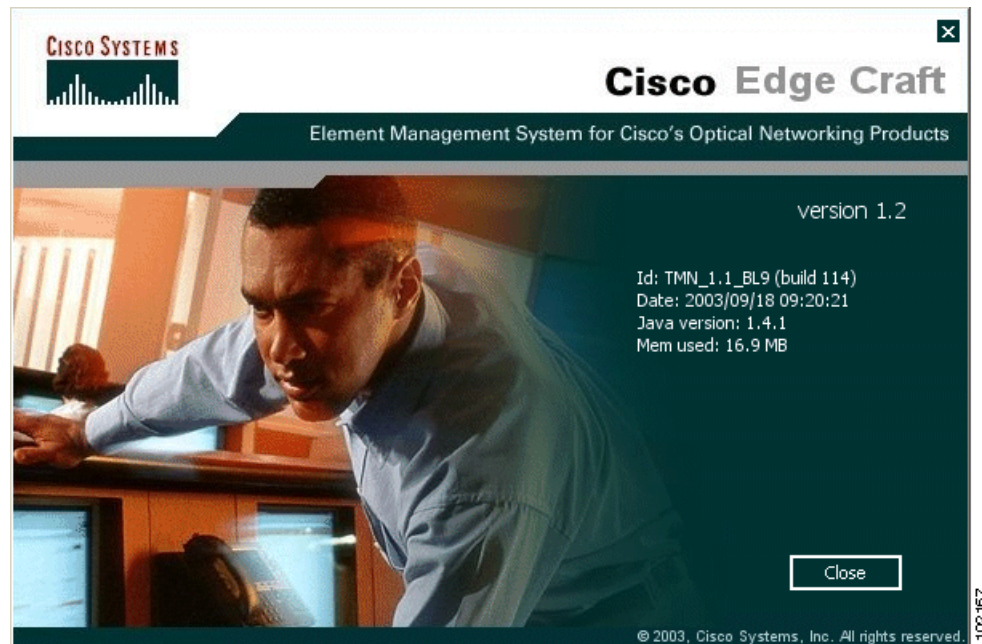
Figure 3-20 and Table 3-7 show and describe the Help menu.

**Figure 3-20 Help Pull-Down Menu**



**Table 3-7 Help Menu**

Menu item	Action
Online Help	This option launches the Cisco Edge Craft User Guide online.
About	This option launches information about the Cisco Edge Craft software ( <a href="#">Figure 3-21</a> ).

**Figure 3-21 The About Dialog Box**

### 3.1.2.8 Log Viewer

[Figure 3-22](#) and [Figure 3-26](#) show the log viewer icons.

These symbols indicate severity in the status bar if the log contains messages:

**Figure 3-22 Error Icon**

This icon indicates that an error message is present.

**Figure 3-23 Warning Icon**

This icon indicates that a warning message is present.

**Figure 3-24 Info Icon**

This icon indicates that information is available.

**Figure 3-25 Unmapped Severity Icon**

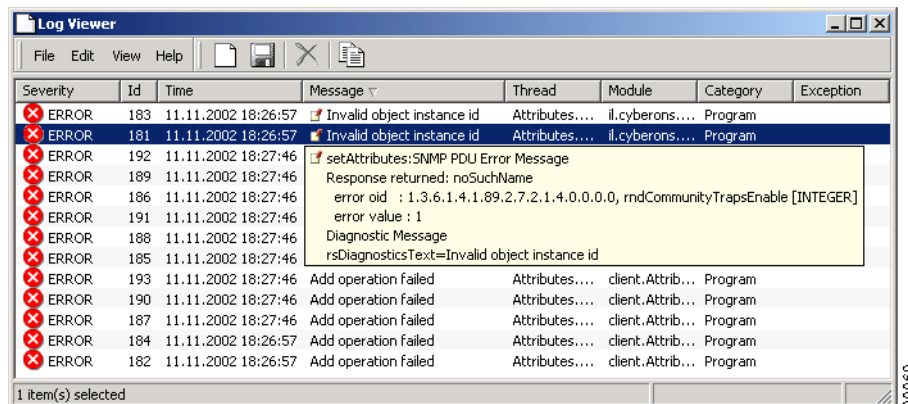
This icon indicates that unmapped severity information is available.

**Figure 3-26 Note Icon**

If this icon occurs, additional information is available.

- Step 1** Double-click the current symbol to view the log.  
Messages marked with the note icon contain additional information.
- Step 2** Click the note icon to view a hyper link.

[Figure 3-27](#) and [Figure 3-28](#) show the log viewer function.

**Figure 3-27 Log Viewer**

The Tool tip shows the entire value if it does not fit inside the cell.

**Figure 3-28 Log Viewer Tool tip**

Program	ID	Name	Action	Date	Level
client.Desktop	26	Creating desktop a...		25.11.2002...	INFO
alarm.Alarm...	13	False		25.11.2002...	INFO
ServiceStarter	0	Starting application...		25.11.2002...	INFO
ServiceStarter	1	Starting service:Sn...		25.11.2002...	INFO
ServiceStarter	2	Starting service:MB...		25.11.2002...	INFO
ServiceStarter	3	Starting service:Ma...		25.11.2002...	INFO






49 item(s) in list

Program	ID	Name	Action	Date	Level
alarm.Alarm...	13	False		25.11.2002...	INFO
ServiceStarter	0	Starting application...		25.11.2002...	INFO
ServiceStarter	1	Starting service:Sn...		25.11.2002...	INFO
ServiceStarter	2	Starting service:MB...		25.11.2002...	INFO
ServiceStarter	3	Starting service:Ma...		25.11.2002...	INFO

### 3.1.3 Copy and Paste

All Cisco Edge Craft applications supporting table entry editing have a copy and paste feature. When pasting, Cisco Edge Craft will verify that selected columns have the same data type as the copied cells. If not, you can copy the data based on the column names. Only editable columns with the same name and datatype will be pasted. This enables copying and pasting between tables with the same data but with a different column order ([Figure 3-29](#)).

**Figure 3-29 Example Copy and Paste**

				
Id	MoClass	Severity	AlarmId	Description
device	critical	ufail	device main unit failure	
device	major	temp	high temperature alarm	
fan	major	fan	fan failure	
power	critical	pwrInA	power failure input A	
power	critical	pwrInB	power failure input B	
power	critical	pwrOut	power output failure	
slot	critical	modMis	module mismatch	

### 3.1.4 Cell Selection Mode

By default, entire rows are selected in a table, but single cells can easily be selected using the cell-mode toggle button ([Figure 3-11](#)).

The feature enables you to copy one table cell, select the entire column, press Paste, and thus copy the value into all selected cells. Copy and paste of ranges is also supported, meaning you can copy values A and B and paste them into a large range to get the A and B values repeated throughout the range.

Copy and paste to external applications, for example Microsoft Excel, is also supported.

### 3.1.5 Navigate in Tables Using the Keyboard

Use the Arrow keys to move the cursor (applies for editable tables only). Use the Enter key or the F2 key to edit a selected cell. Use the Tab key to move the cursor to the next editable cell (from left to right and top to bottom). The selection is circular, meaning when the last editable cell on the last row is reached, the cursor moves to the first editable cell in the first row.

To move to the first editable cell in a table, activate the window and press the Tab key twice.

### 3.1.6 Auto Fit Column Width

Double-clicking the resize-area in the column header will resize the column so that it is wide enough to show all values in the column. By default, the column name is not taken into consideration, but to do so hold down the Shift key while double-clicking.

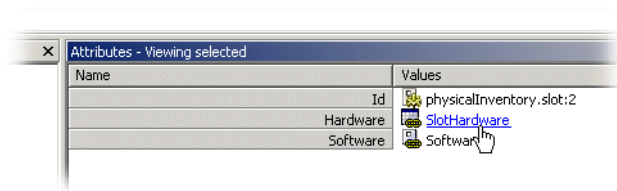
## 3.2 Topology Browser

The topology browser shows the hierarchy of managed entities, for example, LAN ports, VLANs, and bridges on the current network element. You can view the entire hierarchy, or use any of the pre-defined views to view only managed entities of a certain type, for example only view the LAN ports. Whenever an item in the topology is selected, the attributes view will list the child objects under it.

Clicking the device folder in the topology browser (Figure 3-1) will display all alarm-, aux- and management ports. Clicking alarmport:1 will show that specific port's attributes. Attributes that are editable (shown as bold), can be edited directly in the table or through custom user interfaces.

The combination of topology and attribute panes works similar to Windows Explorer, only it shows the contents of a network element instead of files in the file system.

**Figure 3-30 Editable Types and Tables - Hyperlinks**



All links to editable complex types and tables appear as hyperlinks (Figure 3-30).

Although changing attribute values can carry all necessary configurations, more complex configurations are handled using wizards or custom user interfaces.

By selecting a managed object instance and right clicking it, you can choose **Open in new window**. A new Attributes Viewer displaying selected managed object opens. This enables you to easily compare values on different managed objects.

The different configuration tasks using the topology browser are shown in the following chapters.

## 3.3 Alarm Display

The purpose of the alarm display is to present the current alarm and event notifications.

The history of all alarms also appears. The history list in the network element can be cleared. Alarms report failures in the network element. They can be clearable or not clearable. Clearable alarms have a duration. Events report other situations in the network element that are not failures. Figure 3-1 shows an event with a status.

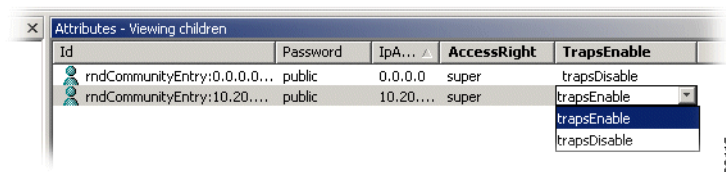


### 3.3.1 Subscribe Cisco Edge Craft to Alarms

You must manually register Cisco Edge Craft as a subscriber to alarms and events from the network element.

- Step 1** Log into the target network element. See the [“1.1 Install Cisco Edge Craft Using the Install Wizard” section on page 1-1](#).
- Step 2** Set the device > users > snmp > **TrapsEnable** attribute to trapsEnable ([Figure 3-31](#)).

**Figure 3-31 Setting the TrapsEnable Attribute**



- Step 3** Click **Save**.

When the registration is complete, Cisco Edge Craft polls the element for all current alarms and starts sending alarms and events to the Cisco Edge Craft IP address.

The SNMP traps are mapped to notifications in Cisco Edge Craft. The mapping philosophy is described in the [“3.3.4 Alarm and Event Notification” section on page 3-20](#).

You can view the list of current alarm notifications by selecting current alarm in the notification list.

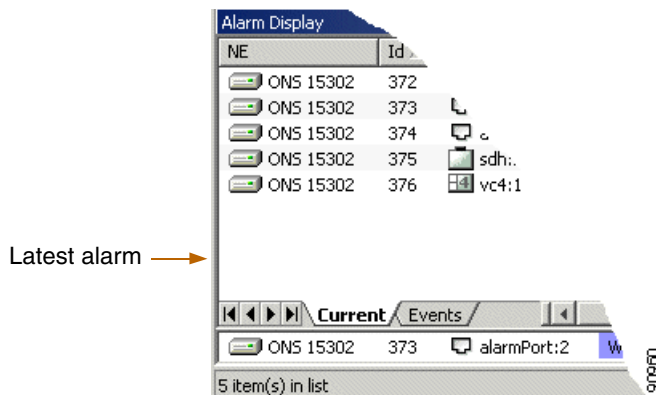
### 3.3.2 View Alarms

Click the **Current** tab to view current alarms ([Figure 3-32](#)).

**Figure 3-32 Current Tab - Alarm List**



The latest alarm is visible in lower part of the Alarm List ([Figure 3-33](#)).

**Figure 3-33 Latest Alarm**

### 3.3.2.1 Refresh

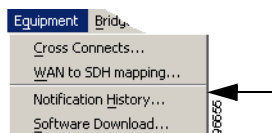
Click **Refresh** in the tool bar to update the Alarm List.

### 3.3.2.2 History

Use the following procedure to obtain a list of all alarm notifications reported on the network element since the last restart of the network element or the last clearing of the history list in the network element.

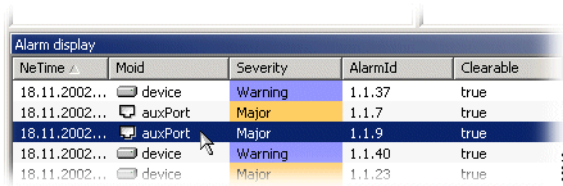
The history log on the network element can be cleared through an action on the log administration attribute of the device. See “[4.3 Manage Common Parameters](#)” section on page 4-11.

- 
- Step 1** From the Equipment menu, choose **Notification History** ([Figure 3-34](#)).
- This will provide a list of all alarm notifications reported on the network element since the last restart of the network element or the last clearing of the history list in the network element.
- Step 2** Click **Refresh**.
- You must explicitly do a refresh for Cisco Edge Craft to collect the alarm history from the network element. Before the refresh is selected the notification list might be empty because a load has not been performed yet.

**Figure 3-34 Notification History**

### 3.3.2.3 Select Alarm

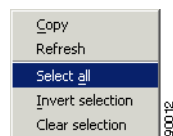
Click on desired single alarm ([Figure 3-35](#)).

**Figure 3-35 Select Single Alarm**


NeTime	Moid	Severity	AlarmId	Clearable
18.11.2002...	device	Warning	1.1.37	true
18.11.2002...	auxPort	Major	1.1.7	true
18.11.2002...	auxPort	Major	1.1.9	true
18.11.2002...	device	Warning	1.1.40	true
18.11.2002...	device	Major	1.1.23	true

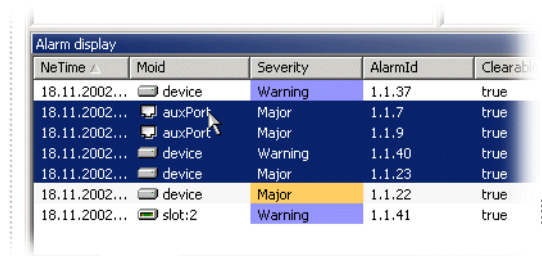
To select multiple alarms, complete the following procedure.

- Step 1** Right click and choose **Select all** (Figure 3-36).

**Figure 3-36 Select All Alarms**

or

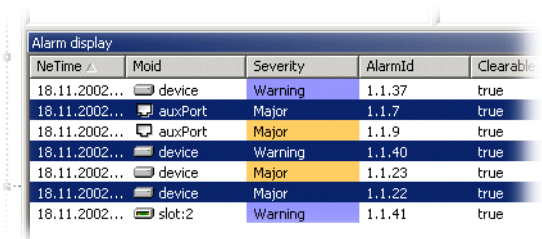
- Step 2** Click the first alarm in a continuous range, hold the Shift key, and click the last alarm in a range (Figure 3-37).

**Figure 3-37 Select Alarms - Continuous Range**


NeTime	Moid	Severity	AlarmId	Clearable
18.11.2002...	device	Warning	1.1.37	true
18.11.2002...	auxPort	Major	1.1.7	true
18.11.2002...	auxPort	Major	1.1.9	true
18.11.2002...	device	Warning	1.1.40	true
18.11.2002...	device	Major	1.1.23	true
18.11.2002...	device	Major	1.1.22	true
18.11.2002...	slot:2	Warning	1.1.41	true

or

- Step 3** Click the first alarm, hold the Ctrl key, and click on alarms to make one continuous selection (Figure 3-38)

**Figure 3-38 Select Alarms - None Continuous Range**


NeTime	Moid	Severity	AlarmId	Clearable
18.11.2002...	device	Warning	1.1.37	true
18.11.2002...	auxPort	Major	1.1.7	true
18.11.2002...	auxPort	Major	1.1.9	true
18.11.2002...	device	Warning	1.1.40	true
18.11.2002...	device	Major	1.1.23	true
18.11.2002...	device	Major	1.1.22	true
18.11.2002...	slot:2	Warning	1.1.41	true

**Step 4** You can also choose **Invert selection** or **Clear selection**.

### 3.3.2.4 Copy Alarms

**Step 1** Select the alarms.

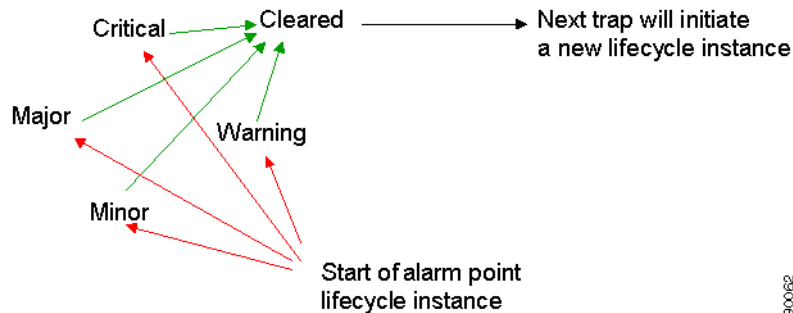
**Step 2** Click **Copy**.

The content of your selection is copied to the clipboard and can be pasted to other applications, for example Notepad.

### 3.3.2.5 Alarm Lifecycle

The notification list presents one row for each alarm point, that is, an alarm source and an alarm identification combination. When a new alarm notification for the same alarm point appears, the row is updated with the severity of the new alarm and new timestamps unless the alarm has been cleared. A new row is created if the alarm point starts a new lifecycle instance (Figure 3-39). Each new alarm notification might cause a transition from one severity to another or to the cleared severity, which ends the lifecycle.

**Figure 3-39 Lifecycle Instance of Alarm Point**



No traps are sent to the Cisco Edge Craft IP address if you have de-registered as a trap receiver.

## 3.3.3 View the Events Reported from the Network Element

This section explains how to view current events and event history, and how to view, resize, and sort columns.

### 3.3.3.1 Current Events

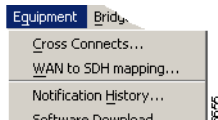
To view current events reported from the network element, select **Event** in the notification list (Figure 3-40 and Figure 3-41).

**Figure 3-40 Select Events****Figure 3-41 Current Events**

Alarm display			
Id ▲	Moid	Description	EventType
985	mgmtPort	Link Up	equip
986	dccR:1.1.1	Link Down	equip
987	dccM:1.1.2	Link Down	equip
988	dccR:1.2.1	Link Down	equip
989	dccM:1.2.2	Link Down	equip
990	dccR:1.3.1	Link Down	equip
991	dccM:1.3.2	Link Down	equip
992	dccR:1.4.1	Link Down	equip

### 3.3.3.2 Event History

- Step 1** From the Equipment Menu, choose **Notification History**.
- Step 2** Click the **Event** tab to view event history ()[Figure 3-42](#).

**Figure 3-42 Event History**

Details about the attributes of the event notifications are provided in [Table 3-8 on page 3-20](#).

### 3.3.3.3 Visible Columns

You can decide which columns will be visible in the alarm display.

- Step 1** From the View menu choose **Columns**.
- Step 2** Uncheck a column to remove it from the alarm display.
- Current alarms and alarm history appear in [Figure 3-43](#).
- Events and event history appear in [Figure 3-44](#).

Figure 3-43 Visible Columns 1

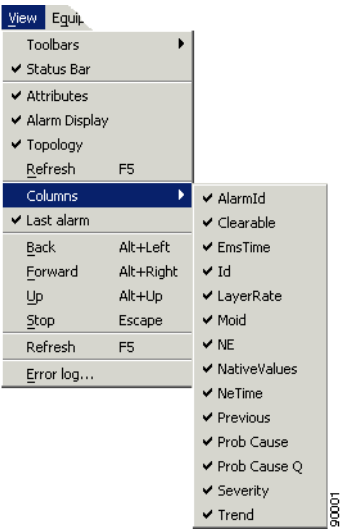
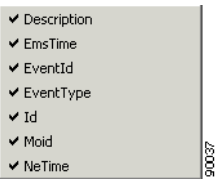


Figure 3-44 Visible Columns 2



### 3.3.3.4 Change Column Order

Use this procedure to change the order of columns (Figure 3-45).

- Step 1** Click a column heading.
- Step 2** Drag and drop the column to a new position.

**Figure 3-45 Column Order**

Alarm display

d	Severity	_Description ▾	_AlarmId
2109	Major	T0 in holdover mode	39
2110	Major	High temperature alarm	3

Alarm display

_Description ▾	Severity	_AlarmId	d
T0 in holdover mode	Major	39	2109
High temperature alarm	Major	3	2110

Alarm display

_Description	Severity	_AlarmId	d
T0 in holdover mode	Major	39	109
High temperature alarm	Major	3	110

### 3.3.3.5 Resize Columns

- Step 1** Rest the mouse pointer to the right of a column header. The mouse pointer turns into a double-arrow (Figure 3-46).
- Step 2** Drag the column to a suitable column size.

**Figure 3-46 Column Resize**

Alarm display

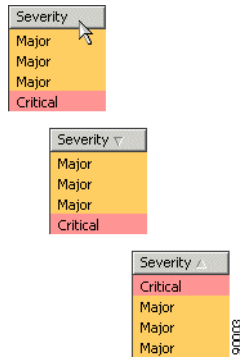
NetTime ▲	Moid	Severity	_AlarmId	Clear
25.11.2002...	vc12:2.9.1...	Minor	1.1.19	true
25.11.2002...	vc12:2.9.1...	Minor	1.1.19	true
25.11.2002...	vc12:2.9.1...	Minor	1.1.19	true
25.11.2002...	vc12:2.9.1...	Minor	1.1.19	true
25.11.2002...	vc12:2.9.1...	Minor	1.1.19	true
25.11.2002...	vc12:2.9.1...	Minor	1.1.19	true

Alarm display

NetTime ▲	Moid	Severity	_AlarmId	Clear
25.11.2002...	vc12:2.9.1...	Minor	1.1.19	true
25.11.2002...	vc12:2.9.1...	Minor	1.1.19	true
25.11.2002...	vc12:2.9.1...	Minor	1.1.19	true
25.11.2002...	vc12:2.9.1...	Minor	1.1.19	true
25.11.2002...	vc12:2.9.1...	Minor	1.1.19	true
25.11.2002...	vc12:2.9.1...	Minor	1.1.19	true

### 3.3.3.6 Sort Columns

- Step 1** Click a column to sort it in ascending order (Figure 3-47).
- Step 2** Click the column again to sort it in descending order.

**Figure 3-47 Column Sorting**

## 3.3.4 Alarm and Event Notification

The notification types with attributes supported by Cisco Edge Craft are:

- Alarm notification, shown in [Table 3-8](#).
- Event notification, shown [Table 3-9](#).

### 3.3.4.1 Alarm Notification

The severity of an alarm notification can either be reported from the network element or must be defined in the notification mapping.

**Table 3-8 Alarm Notification Types and their Attributes**

Notification	Attribute	Legal Values
Moid	Identification of the network element that contains the source of the alarm.	Depends on NE type. Has to be a M.O for the NE.
Id	Sequence number	
Previous	Sequence number of previous notification	
AlarmId	Unique identification of alarm	
NeTime	Timestamp from network element if available	Number of seconds since 1.1.1970
Ems Time	Timestamp set by Cisco Edge Craft	Number of seconds since 1.1.1970
Severity	Severity of alarm.	Critical, major, minor, warning, cleared, Indeterminate
Trend	Trend indication to report the trend in the severity change.	No change, less severe, more severe
Prob Cause	The probable cause of the alarm.	Legal values depend on the network element.



**Table 3-8 Alarm Notification Types and their Attributes (continued)**

Notification	Attribute	Legal Values
Prob Cause Q	A probable cause qualifier if the probable cause itself is not sufficient to determine the exact error and source.	Legal values depend on the network element.
Layer rate	The layer rate in which the managed object belongs if applicable.	Not Applicable, or any other layer rate supported by the network element
Clearable	Boolean value to indicate if the alarm can be cleared or not. Some alarms do not have duration and therefore no cleared severity.	false, true
Native Values	Unmapped trap data	Depends on NE

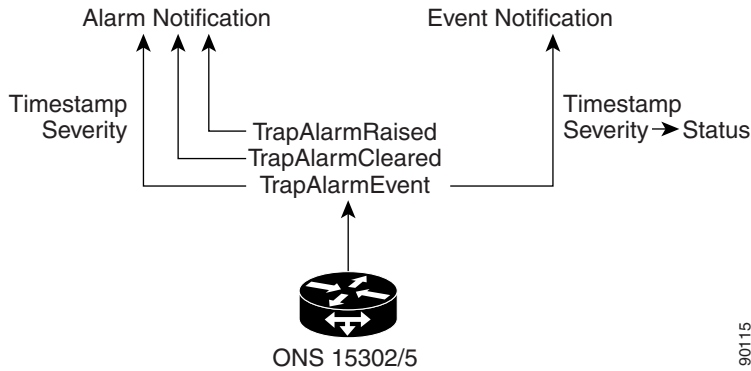
### 3.3.4.2 Event Notification

**Table 3-9 Event Notification Types and their Attributes**

Notification	Attribute	Legal Values
Moid	Identification of the network element that contains the source of the event.	A M.O in the Information Model for the equipment
EventId	Unique identification of event	
NeTime	Timestamp from network element if available	Number of seconds since 1.1.1970
Ems Time	Timestamp set by Cisco Edge Craft	Number of seconds since 1.1.1970
Description	Additional text	
EventType	Type of event	equip, comm
Id	Sequence number	

### 3.3.4.3 Trap-to-Notification Mapping

The interpretation of alarms and events is slightly different in the network element and Cisco Edge Craft. The mapping rules applied to the SNMP traps are in [Figure 3-48](#).

**Figure 3-48 Trap to Notification Mapping**

The **TrapAlarmRaised** and **TrapAlarmCleared** traps are mapped to alarm notification. The timestamp in the trap is used with the severity. ONS 15305 and ONS 15302 network elements have a severity in the trap. This severity is used in notification.

One attribute in an alarm notification is called clearable. If this attribute is set to true, it indicates that the management system should expect a **TrapAlarmCleared** for this alarm.

Those **TrapAlarmEvent** traps that indicate an error failure in the network element will be mapped to an alarm notification with the clearable attribute set to false. The severity and timestamp from the trap are used in the alarm notification.

Other **TrapAlarmEvents** will be mapped to event notifications. These have no severity, but a status defining the type of event, for example info and confirm. The severity in the trap might be used as the status in the event notification.

### 3.3.4.4 Unknown Traps

If Cisco Edge Craft receives a trap and no mapping to any type of notification is available, a notification is generated. The notification contains all the information as it was received in the trap.



# General Management

This chapter describes the configuration operations supported by the Management Interface managed object (MO).

The attributes under the management interfaces MO are not unique in the information model. Each attribute mirrors a similar attribute located under another MO. The attributes under the management interfaces MO have been put together to allow the user to set up basic configuration of the management interfaces without having to browse through many MOs in the topology browser. For advanced configuration operations, additional MOs must still be used.

## 4.1 Management Modes and Configuration

The management traffic is IP based (SNMP and TFTP messages); therefore when configuring a management path IP datagrams must carry the management traffic over the network. For the management interfaces, two main encapsulation types are available:

- IP directly carried over a layer 2 protocol (Ethernet, PPP, or proprietary).
- IP encapsulated within CLNP carried over a layer 2 protocol (IEEE 802.x or LAP-D).

In addition, each management interface can be turned off. Actual encapsulation support varies depending on the management interface type (management port or DCC). [Table 4-1](#) provides an overview of the different management modes versus the management interfaces.



**Note** This is an important feature for security purposes, especially for the management port, which is physically accessible on the network element (main card).

**Table 4-1 Management Modes Versus Management Interface**

Management Interface	Not Used	IP		
		IP/Ethernet	IP/proprietary encapsulation	IP/PPP
Management Port	X	X		
DCC	X		X	X

**Note**

The management port is able to run both IP over Ethernet and CLNP over IEEE 802.x at the same time. On the contrary, a DCC can run only one mode at a time. In addition, a maximum of eight DCCs can be used for management purposes, meaning only eight DCCs can have their management mode set to IP.

The following sections describe how to configure the management port and the DCCs by using the management interfaces MO present in the topology browser.

## 4.1.1 Management Port Configuration

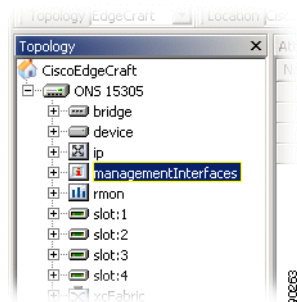
The management port can run two types of encapsulation or mode. A particular mode is selected by setting the variable mode (management interfaces >management port > mode). Required configuration for possible modes is Not Used or IP.

### 4.1.1.1 Mode: Not Used

To configure the management port mode to Not Used complete the following steps.

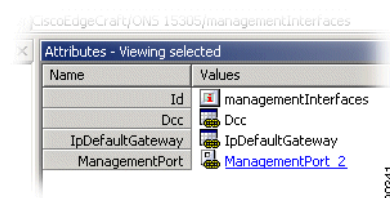
- Step 1** Click the ONS 15305 managed object, then click the **management Interfaces** managed object in the topology browser (Figure 4-1).

**Figure 4-1 Management Interfaces - Managed Object**

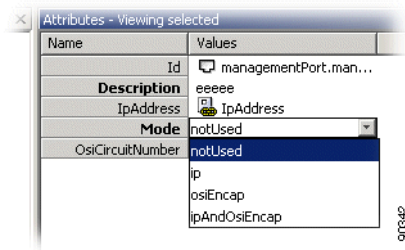


- Step 2** Click **managementPort** in the attributes window (Figure 4-2).

**Figure 4-2 ManagementPort - Attributes**



- Step 3** In the attributes window, the set mode to **Not Used** (Figure 4-3).

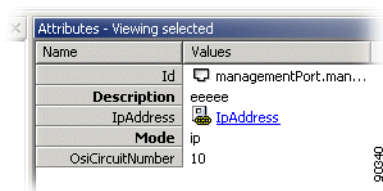
**Figure 4-3 ManagementPort - Mode Selector**

**Step 4** Click **Save** on the toolbar.

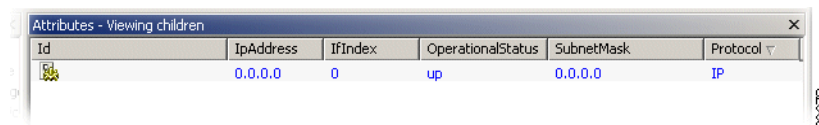
### 4.1.1.2 Mode: IP

To configure the management port with the mode set to IP, complete the following steps:

- Step 1** Click the ONS 15305 managed object, then click the **management Interfaces** managed object in the topology browser.
- Step 2** Click **managementPort** in the attributes window.
- Step 3** In the attributes window, set **mode** to **IP**.
- Step 4** Click **Save** on the toolbar.
- Step 5** Click **ipAddress** in the attributes window (Figure 4-4).

**Figure 4-4 ManagementPort - IP Address Attribute**

- Step 6** Click **Add** on the toolbar. Set **protocol** to **IP**, and set **ipAddress** and **subnetMask** according to your IP addressing scheme or plan (Figure 4-5).

**Figure 4-5 ManagementPort - Add IP Address**

- Step 7** Click **Save** on the toolbar.

Depending on your topology, additional routing information might need to be configured. You can define static routes or control dynamic protocols (RIP, OSPF) by using the IP managed object in the topology browser. Defining a default gateway can be done directly from the management interface's managed object as explained in section “4.1.3 IP Default Gateway Configuration” section on page 4-5.

## 4.1.2 DCC Configuration

A DCC can run three types of encapsulation or mode. A particular mode is selected by setting the variable mode (management interfaces > DCC > mode). The required configuration for one of the two possible modes (Not Used or IP) is further detailed in the next sections.

### 4.1.2.1 Mode: Not Used

To configure a DCC with the mode set to Not Used, complete the following steps.

- Step 1** Click the ONS 15305 managed object and then click the **management Interfaces** managed object in the topology browser.
- Step 2** Click **dcc** in the attributes window. In the attributes window, each row represents a DCC interface.
- Step 3** Set **mode** to **Not Used**.
- Step 4** Click **Save** on the toolbar.

### 4.1.2.2 Mode: IP

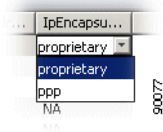
To configure a DCC with the mode set to IP, complete the following steps.

- Step 1** Click the ONS 15305 managed object and then click the **management Interfaces** managed object in the topology browser (Figure 4-6).
- Step 2** Click **dcc** in the attributes window.
- Step 3** In the attributes window, each row represents a DCC interface. Set **mode** to **IP over DCC** for the desired DCC interface.

**Figure 4-6 Management Interfaces - Dcc Attribute**

Id	Slot	PppConfig...	LapdRole	Port	UserLabel	DccType	OsiCircuit...	Mode	IpAddr...	IpEncapsu...
axx...	1	[PppCo... network		1		dccR	0	IpOverDcc		proprietary
axx...	0	[PppCo... network		0		dccR	0	notUsed		NA
axx...	0	[PppCo... network		0		dccR	0	notUsed		NA
axx...	0	[PppCo... network		0		dccR	0	notUsed		NA
axx...	0	[PppCo... network		0		dccR	0	notUsed		NA
axx...	0	[PppCo... network		0		dccR	0	notUsed		NA
axx...	0	[PppCo... network		0		dccR	0	notUsed		NA

- Step 4** In addition, when the mode is set to IP, the layer 2 encapsulation for the IP datagrams must be configured. This done by setting the ipEncapsulation variable to the desired encapsulation (proprietary or PPP) (Figure 4-7).

**Figure 4-7 IPEncapsulation - Encapsulation Selector**

- Step 5** Click **Save** on the toolbar.
- Step 6** Click **ipAddress** in the attributes window.
- Step 7** Click **Add** on the toolbar. Set **protocol** to IP, and set **ipAddress** and **subnetMask** according to your IP addressing scheme or plan.
- Step 8** Click **Save** on the toolbar.

If the mode is set to IP and ipEncapsulation is set to PPP, additional configuration for PPP can be performed via the pppConfiguration variable (management interfaces > DCC > pppConfiguration).

Depending on your topology, additional routing information might need to be configured. You can define static routes or control dynamic protocols (RIP, OSPF) by using the IP managed object in the topology browser. Defining a default gateway can be done directly from the management interfaces managed object as explained in [“4.1.3 IP Default Gateway Configuration” section on page 4-5](#).

### 4.1.3 IP Default Gateway Configuration

To configure an IP default gateway on the network element complete the following steps.

- Step 1** Click the ONS 15305 managed object, then click the **management Interfaces** managed object in the topology browser.
- Step 2** Click **ipDefaultGateway** in the attributes window.
- Step 3** Set the defaultGatewayIpAddress and defaultGatewayInterface according to your IP addressing plan.
- Step 4** Click **Save** on the toolbar.



**Note** The default gateway must be directly reachable from the network element, meaning the default gateway must belong to a subnet defined on the interface identified by defaultGatewayInterface. Modifying the default gateway results in removing the previous default gateway from the network element's routing table and adding the new (modified) gateway to the routing table.



**Note** Secure routing before removing the default gateway.

## 4.2 ONS 15305 Scenarios

This section presents four typical network topologies and describes how the management interfaces can be configured through the management interface's managed object to carry management traffic.

In the following scenarios, it is assumed that both RIP and OSPF are disabled. Although each IP network is unique, the topologies and configurations presented in this chapter can be considered basic building blocks that can be combined together to apply to a specific network.

In a real network, with a larger number of network elements, additional managed objects can be required to perform the configurations. In particular, configuration of IP and activation and configuration of dynamic routing protocols (RIP, OSPF, IS-IS) require the use of additional managed objects.

IP over DCC (with proprietary or PPP encapsulation) requires configuring a subnet per link (per DCC). Any network element configured with IP over DCC and located more than two DCC links away from Cisco Edge Craft must either have a static route to Cisco Edge Craft or must run a dynamic routing protocol. As the number of static routes increases with the number of interfaces configured to run IP over DCC, running a dynamic routing protocol can be advantageous. Depending on the network topology, care must be taken when enabling IP routing protocol over DCC to prevent the DCC network from being advertised as a path for the user traffic (as opposed to the management traffic only).

Each of the scenarios presents a figure from a typical IP topology with the parameters required in the management interface's managed object.

### 4.2.1 Notations Used

The following notations are used throughout the rest of this section:

The `/<prefix-length>` notation is used to denote the {IP address, subnet mask} pairs. As an example, the notation `192.168.0.1 / 24` refers to the following pair: {IP address 192. 168.0.1, subnet mask 255.255.255.0}.



#### Note

The prefix-length is equal to the total number of contiguous 1-bits in the traditional subnet mask.

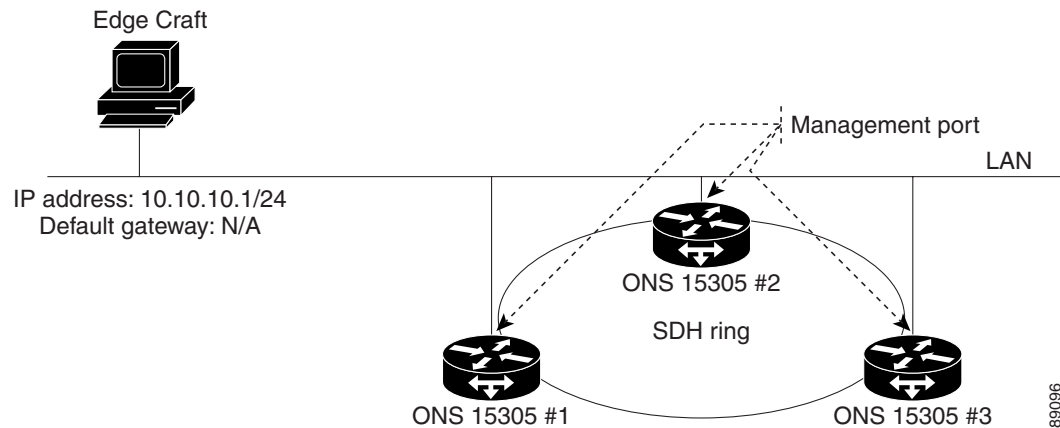
N/A (non-applicable) is used to denote that an attribute is not relevant for a particular configuration, meaning the value of the attribute will not influence the configuration.

The notation `interface (XXX)` defines the interface of the default gateway ([Figure 4-9](#) to [Figure 4-11](#)). Possible values for XXX are "MGMT Port" to the ifIndex of the management port and "DCC #n" to the ifIndex of the DCC channel. The values of the ifIndex can be found under the managed objects and DCCs.



## 4.2.2 Scenario 1: Cisco Edge Craft and ONS 15305 on the Same Subnet

**Figure 4-8 Cisco Edge Craft and ONS 15305 on the Same Subnet**



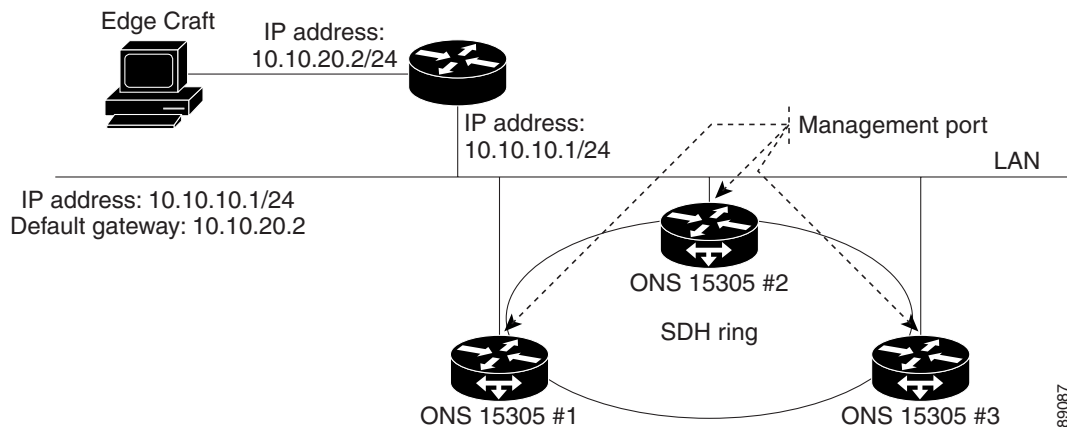
**Table 4-2 Cisco Edge Craft and ONS 15305 on the Same Subnet - Settings**

	ONS 15305 1	ONS 15305 2	ONS 15305 3
Mangement Port			
mode	IP	IP	IP
iPAddress	IP, 10.10.10.10 / 24	IP, 10.10.10.20 / 24	IP, 10.10.10.30 / 24
DCC#1			
mode	notUsed	notUsed	notUsed
ipEncapsulation	N/A	N/A	N/A
lapdRole	N/A	N/A	N/A
pppConfiguration			
initialMRU	N/A	N/A	N/A
pppIpAdminStatus	N/A	N/A	N/A
compression	N/A	N/A	N/A
ipAddress	N/A	N/A	N/A
DCC#2			
mode	not used	not used	not used
ipEncapsulation	N/A	N/A	N/A
lapdRole	N/A	N/A	N/A
pppConfiguration			
initialMRU	N/A	N/A	N/A
pppIpAdminStatus	N/A	N/A	N/A
compression	N/A	N/A	N/A
ipAddress	N/A	N/A	N/A
IP Defaulty Gateway			

**Table 4-2 Cisco Edge Craft and ONS 15305 on the Same Subnet - Settings (continued)**

	ONS 15305 1	ONS 15305 2	ONS 15305 3
ipAddress	N/A	N/A	N/A
interface	N/A	N/A	N/A

## 4.2.3 Scenario 2: Cisco Edge Craft and ONS 15305 on Different Subnets

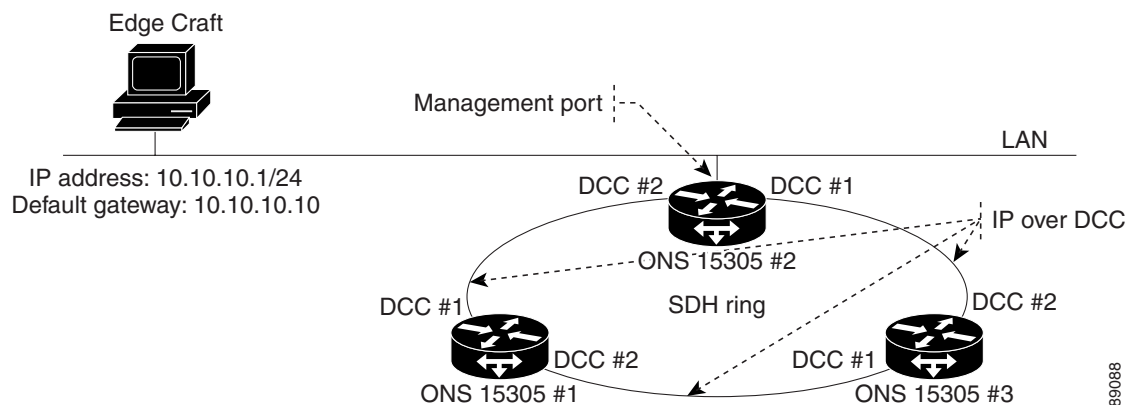
**Figure 4-9 Cisco Edge Craft and ONS 15305 on Different Subnets****Table 4-3 Cisco Edge Craft and ONS 15305 on Different Subnet - Settings**

	ONS 15305 1	ONS 15305 2	ONS 15305 3
Mangement Port			
mode	IP	IP	IP
iPAddress	IP, 10.10.10.10 / 24	IP, 10.10.10.20 / 24	IP, 10.10.10.30 / 24
DCC#1			
mode	notUsed	notUsed	notUsed
ipEncapsulation	N/A	N/A	N/A
lapdRole	N/A	N/A	N/A
pppConfiguration			
initialMRU	N/A	N/A	N/A
pppIpAdminStatus	N/A	N/A	N/A
compression	N/A	N/A	N/A
ipAddress	N/A	N/A	N/A
DCC#2			
mode	not used	not used	not used
ipEncapsulation	N/A	N/A	N/A
lapdRole	N/A	N/A	N/A

**Table 4-3 Cisco Edge Craft and ONS 15305 on Different Subnet - Settings (continued)**

	ONS 15305 1	ONS 15305 2	ONS 15305 3
pppConfiguration			
initialMRU	N/A	N/A	N/A
pppIpAdminStatus	N/A	N/A	N/A
compression	N/A	N/A	N/A
ipAddress	N/A	N/A	N/A
IP Defaulty Gateway			
ipAddress	10.10.10.1	10.10.10.1	10.10.10.1
interface	mgmt port	mgmt port	mgmt port

## 4.2.4 Scenario 3: IP over DCC

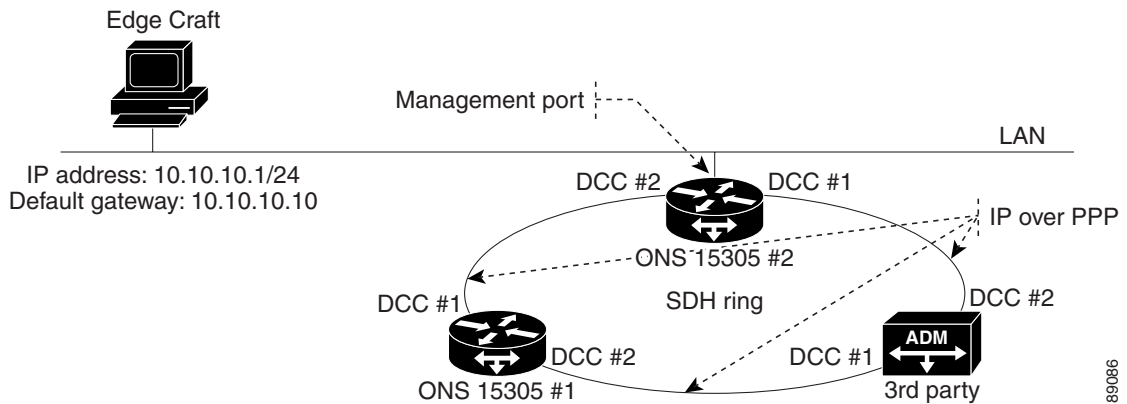
**Figure 4-10 IP over DCC****Table 4-4 IP Over DCC - Settings**

	ONS 15305 1	ONS 15305 2	ONS 15305 3
Mangement Port			
mode	IP	IP	IP
iPAddress	N/A	IP, 10.10.10.10 / 24	N/A
DCC#1			
mode	notUsed	notUsed	notUsed
ipEncapsulation	proprietary	proprietary	proprietary
lapdRole	N/A	N/A	N/A
pppConfiguration			
initialMRU	N/A	N/A	N/A
pppIpAdminStatus	N/A	N/A	N/A
compression	N/A	N/A	N/A

**Table 4-4 IP Over DCC - Settings (continued)**

	ONS 15305 1	ONS 15305 2	ONS 15305 3
ipAddress	IP, 192.168.10.1 / 24	IP, 192.168.20.1 / 24	IP, 192.168.30.1 / 24
DCC#2			
mode	not used	not used	not used
ipEncapsulation	proprietary	proprietary	proprietary
lapdRole	N/A	N/A	N/A
pppConfiguration			
initialMRU	N/A	N/A	N/A
pppIpAdminStatus	N/A	N/A	N/A
compression	N/A	N/A	N/A
ipAddress	IP, 192.168.30.2 / 24	IP, 192.168.10.2 / 24	IP, 192.168.20.2 / 24
IP Defaulty Gateway			
ipAddress	192.168.10.2	N/A	192.168.20.1
interface	DCC #1	N/A	DCC #2

## 4.2.5 Scenario 4: IP over PPP

**Figure 4-11 IP over PPP****Table 4-5 IP Over PPP- Settings**

	ONS 15305 1	ONS 15305 2	ONS 15305 3
Mangement Port			—
mode	notUsed	IP	—
iPAddress	N/A	IP, 10.10.10.10 / 24	—
DCC#1			

**Table 4-5 IP Over PPP- Settings (continued)**

	ONS 15305 1	ONS 15305 2	ONS 15305 3
mode	IP	notUsed	—
ipEncapsulation	PPP	PPP	—
lapdRole	N/A	N/A	—
pppConfiguration			
initialMRU	1500	1500	—
pppIpAdminStatus	open	open	—
compression	none	none	—
ipAddress	IP, 192.168.10.1	IP, 192.168.20.1	IP, 192.168.30.1 / 24
DCC#2			
mode	IP	IP	—
ipEncapsulation	PPP	PPP	—
lapdRole	N/A	N/A	—
pppConfiguration			—
initialMRU	1500	1500	—
pppIpAdminStatus	open	open	—
compression	none	none	—
ipAddress	IP, 192.168.30.2	IP, 192.168.10.2	IP, 192.168.20.2 / 24
IP Defaulty Gateway			
ipAddress	192.168.10.2	N/A	192.168.20.1
interface	DCC #1	N/A	DCC #2

The third-party equipment supports:

- Standard IP over PPP over DCC according IF-DN-0101-R1
- IP forwarding between its DCC interface

## 4.3 Manage Common Parameters

The purpose of this section is guide you through management of the attributes that are related to the network element sub-rack and the common hardware and software.

The section includes viewing and modifying NE parameters, time settings, users, available features, and the physical inventory, restart issues, LEDs and alarm output, and ping mechanism.

Synchronization, download of software, upload and download of configuration data, and management of NE's are described in separate sections.

### 4.3.1 View Common Parameters

Select **device** in the topology browser.

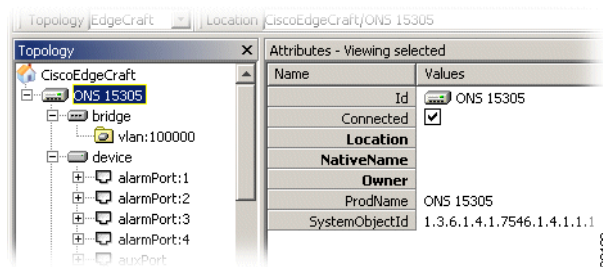
The common attributes (parameters) as defined in the information model are:

- Identification of the network element
- Time settings
- Users
- Available features (licenses)
- Physical inventory
- Network element restart
- Logs (alarm logs, performance data logs)
- LEDs and alarm output
- Ping mechanism

## 4.3.2 Identify the Network Element

- Step 1** Select the network element in the topology browser (Figure 4-12).
- Step 2** Modify the following attributes as needed:
- Location
  - NativeName
  - Owner

**Figure 4-12 Identification of Network Element**

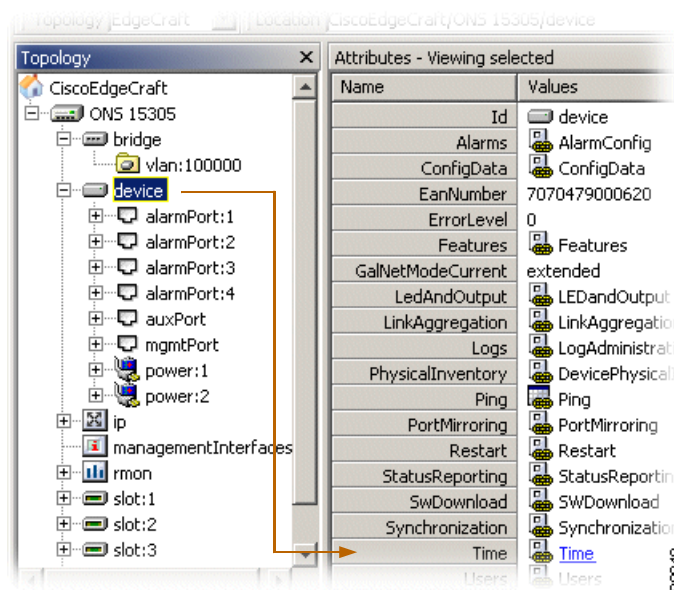


- Step 3** Click **Save** to commit changes.

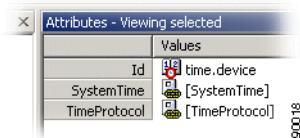
## 4.3.3 Time Settings

The following steps explain how to change time settings for an ONS 15305.

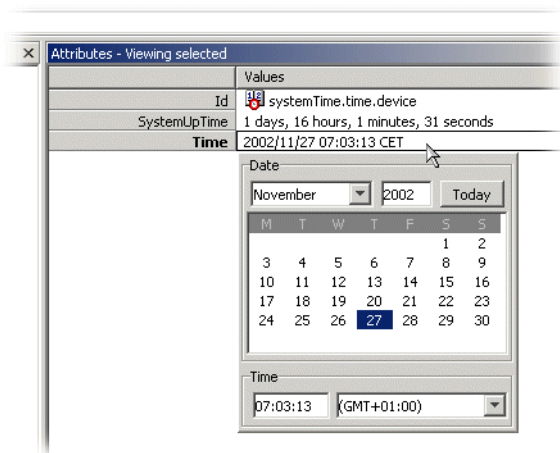
- Step 1** Select **ONS 15305** and then select the **device** managed object (Figure 4-13).

**Figure 4-13 Time Settings - Time Attribute**

**Step 2** Click **Time** (Figure 4-14).

**Figure 4-14 Time Attribute - Values**

**Step 3** Click **SystemTime>Time** to view or modify (Figure 4-15).

**Figure 4-15 Time Attributes - System Time**

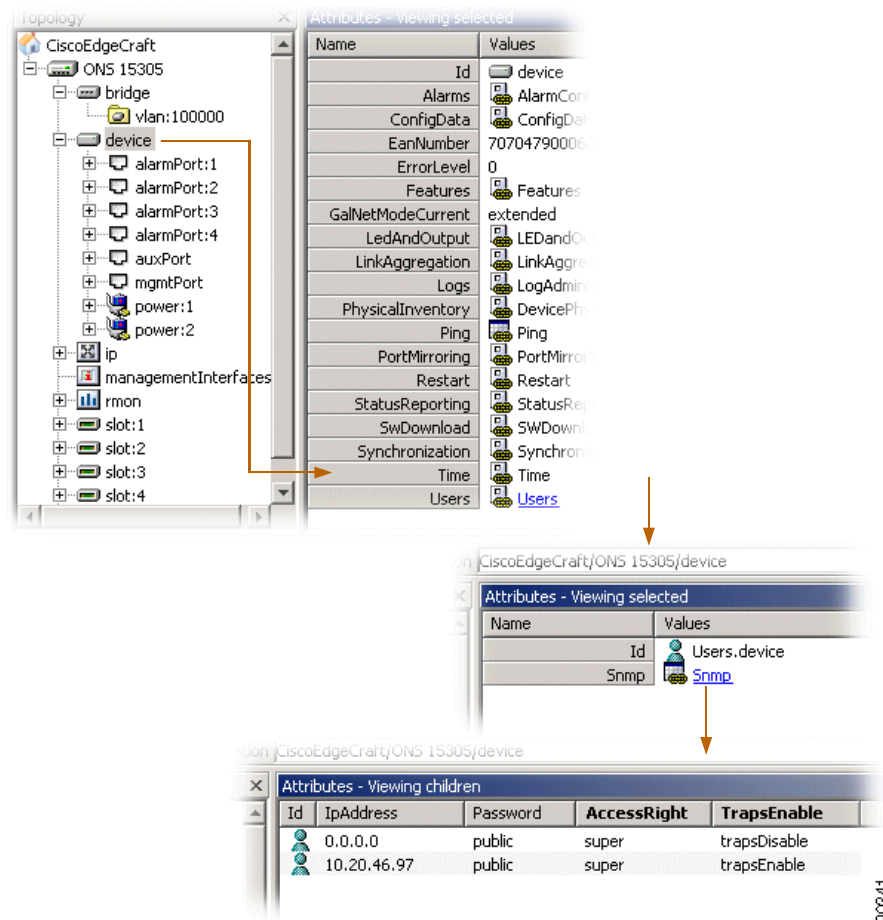
**Step 4** Click **TimeProtocol** to view or modify the following objects:

- TimeServerIpAddress
- TimeSyncInterval
- TimeZone

## 4.3.4 Users

This section explains how to add a new user (Figure 4-16) and change the VT 100 password.

**Figure 4-16 Add a New User - Overview**



### 4.3.4.1 Add a New User

- Step 1** Navigate as shown in Figure 4-16.
- Step 2** Click **Add**.



- Step 3** Enter the password or IpAddress .
- Step 4** Select the **AccessRight** from the drop-down menu.
- Step 5** Select the **TrapsEnable** state from pulldown menu.
- Step 6** Click **Save**.

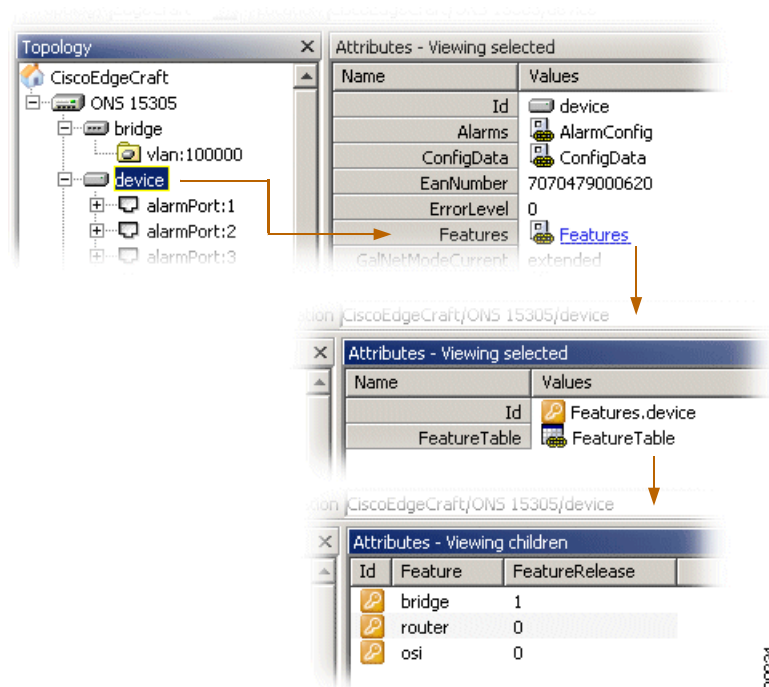
#### 4.3.4.2 VT 100 Password (ONS 15302 only)

- Step 1** In the topology browser select **device > time > VT100**.
- Step 2** Edit the **Vt100Password**.
- Step 3** Click **Save**.

### 4.3.5 Available Features (Licenses)

In the topology browser select **device > Features > FeatureTable** to view available licences (Figure 4-17).

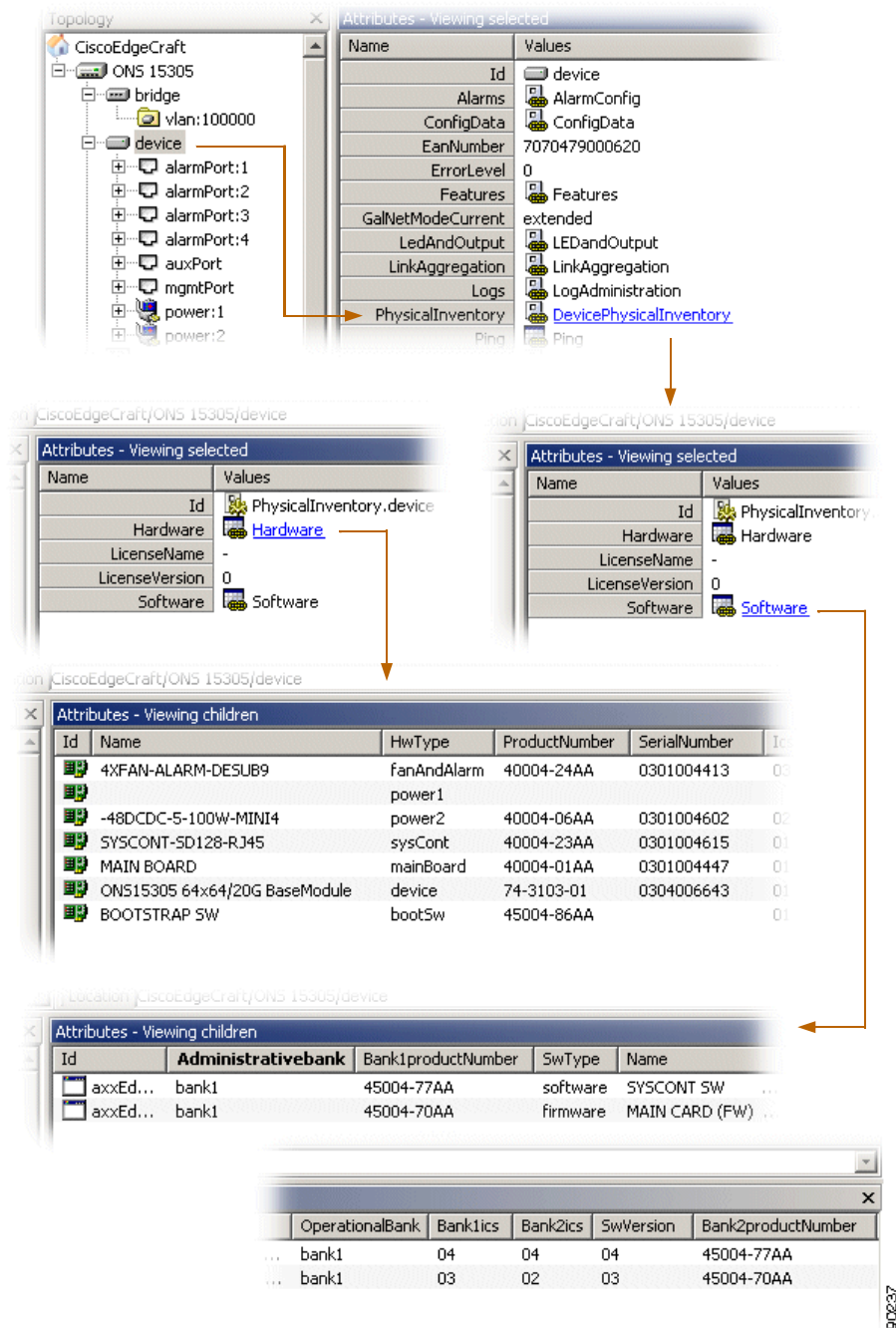
**Figure 4-17 Available Features**



## 4.3.6 Physical Inventory - ONS 15305

**Step 1** In the topology browser select **device** > **DevicePhysicalInventory** (Figure 4-18).

**Figure 4-18 Physical Inventory - Overview**



**Step 2** Select **Hardware** to list a hardware inventory.

**Step 3** Select **Software** to list a software inventory.

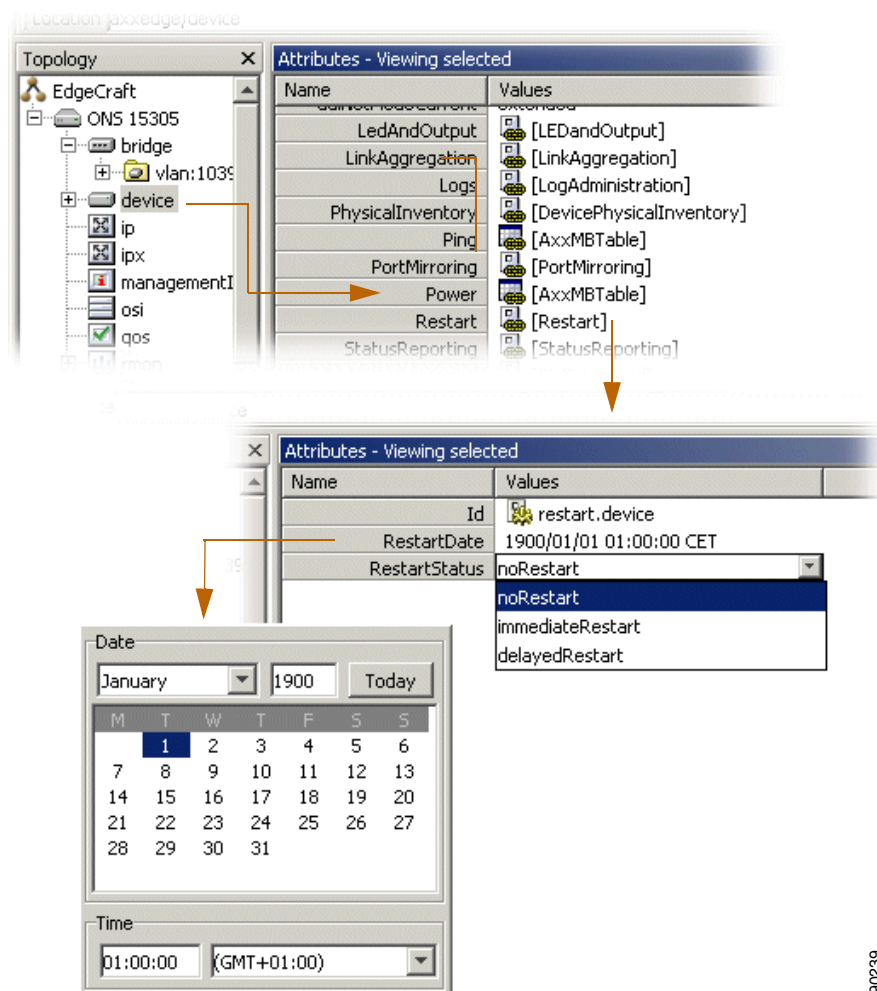
### 4.3.7 Physical Inventory - ONS 15302

In the topology browser select **device** > **inventory**.

### 4.3.8 Restart the ONS 15305

**Step 1** In the topology browser select **device** > **Restart** (Figure 4-19).

**Figure 4-19 Restart of Network Element - Overview**



**Step 2** If selecting **delayedRestart**, set **time** and **date**.

**Step 3** Select the **RestartStatus**.

90239

**Step 4** Click **Save**.

## 4.3.9 Restart the ONS 15302

- Step 1** In the topology browser select **device** > **Restart**.
- Step 2** Select **Restart**.
- Step 3** Click **Save**.

## 4.3.10 Logs (Alarm Logs, Performance Data Logs)

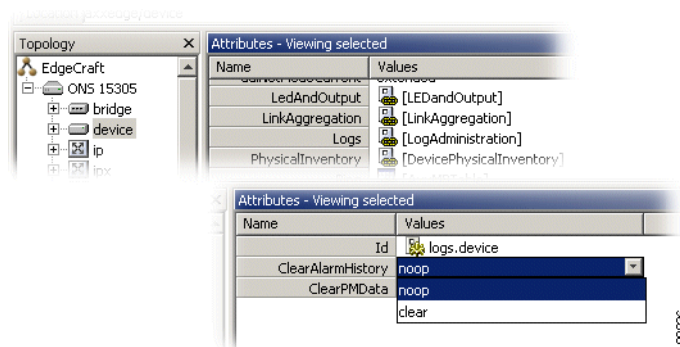
### 4.3.10.1 Clear Alarm History

- Step 1** In the topology browser select **device** > **LogAdministration**.
- Step 2** Set **ClearAlarmHistory** to **clear**.
- Step 3** Click **Save**.
- Step 4** Refresh the Alarm History in the Alarm List.

### 4.3.10.2 Clear PM Data

- Step 1** In the topology browser select **device** > **LogAdministration**.
- Step 2** Set **ClearPMDData** to **clear** (Figure 4-20).
- Step 3** Click **Save**.

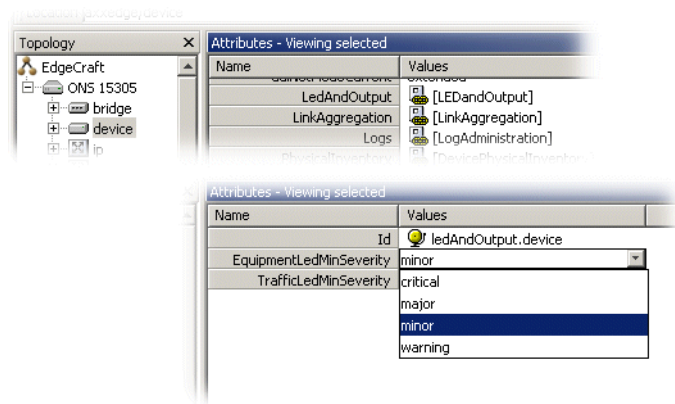
**Figure 4-20** Clear Alarm- and Performance Data Log



### 4.3.10.3 LEDs and Alarm Output

- Step 1** In the topology browser select **device** > **LEDandOutput**
- Step 2** Select **severity** to light the NE LEDs (Figure 4-21).

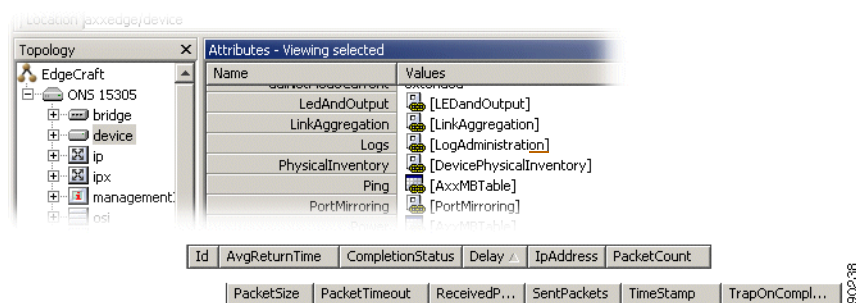
**Figure 4-21 LEDs - Severity Selector**



### 4.3.10.4 Ping Mechanism

- Step 1** In the topology browser select **device** > **Ping** hyper link (Figure 4-22).
- Step 2** Edit any of the following attributes as needed:
- Delay
  - PacketCount
  - TrapOnCompletion (true/false)
  - PacketSize
  - PacketTimeout

**Figure 4-22 Ping Mechanism**



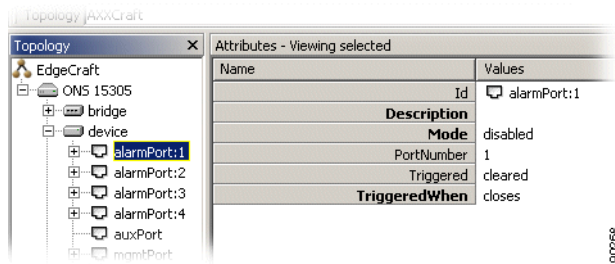
### 4.3.10.5 Alarm Ports

**Step 1** In the topology browser select **device** > **alarmPort** (Figure 4-23).

**Step 2** Edit the following attributes as needed:

- Description  
Free text description.
- Mode  
enabled or disabled
- TriggeredWhen  
opens or closes (when an alarm is to be triggered)

**Figure 4-23 Alarm Ports**

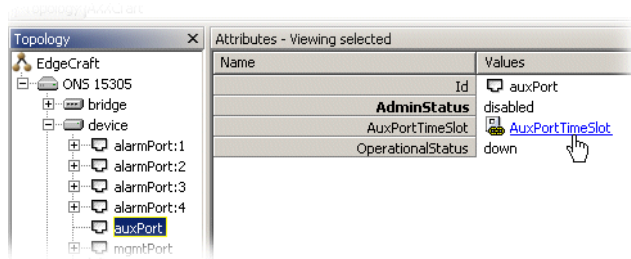


**Step 3** Click **Save**.

### 4.3.10.6 AUX Port - ONS 15305

**Step 1** In the topology browser select **device** > **auxPort** (Figure 4-24).

**Figure 4-24 AUX Port**



**Step 2** Edit the following attributes as needed:

- AdminStatus enabled or disabled
- AuxPortTimeSlot (Figure 4-25).

Figure 4-25 AUX port - Timeslots

Id	Timeslot	OhByte	Slot	Description	Port
auxEdgeAuxIntTimeSlotMapEntry:1	1	unMapped	0		0
auxEdgeAuxIntTimeSlotMapEntry:2	2	unMapped	0		0
auxEdgeAuxIntTimeSlotMapEntry:3	3	unMapped	0		0
auxEdgeAuxIntTimeSlotMapEntry:4	4	unMapped	0		0
auxEdgeAuxIntTimeSlotMapEntry:5	5	unMapped	0		0
auxEdgeAuxIntTimeSlotMapEntry:6	6	unMapped	0		0
auxEdgeAuxIntTimeSlotMapEntry:7	7	unMapped	0		0
auxEdgeAuxIntTimeSlotMapEntry:8	8	unMapped	0		0
auxEdgeAuxIntTimeSlotMapEntry:9	9	unMapped	0		0
auxEdgeAuxIntTimeSlotMapEntry:10	10	unMapped	0		0
auxEdgeAuxIntTimeSlotMapEntry:11	11	unMapped	0		0
auxEdgeAuxIntTimeSlotMapEntry:12	12	unMapped	0		0
auxEdgeAuxIntTimeSlotMapEntry:13	13	unMapped	0		0
auxEdgeAuxIntTimeSlotMapEntry:14	14	unMapped	0		0
auxEdgeAuxIntTimeSlotMapEntry:15	15	unMapped	0		0
auxEdgeAuxIntTimeSlotMapEntry:16	16	unMapped	0		0
auxEdgeAuxIntTimeSlotMapEntry:17	17	unMapped	0		0
auxEdgeAuxIntTimeSlotMapEntry:18	18	unMapped	0		0
auxEdgeAuxIntTimeSlotMapEntry:19	19	unMapped	0		0
auxEdgeAuxIntTimeSlotMapEntry:20	20	unMapped	0		0
auxEdgeAuxIntTimeSlotMapEntry:21	21	unMapped	0		0
auxEdgeAuxIntTimeSlotMapEntry:22	22	unMapped	0		0
auxEdgeAuxIntTimeSlotMapEntry:23	23	unMapped	0		0
auxEdgeAuxIntTimeSlotMapEntry:24	24	unMapped	0		0
auxEdgeAuxIntTimeSlotMapEntry:25	25	unMapped	0		0
auxEdgeAuxIntTimeSlotMapEntry:26	26	unMapped	0		0
auxEdgeAuxIntTimeSlotMapEntry:27	27	unMapped	0		0
auxEdgeAuxIntTimeSlotMapEntry:28	28	unMapped	0		0
auxEdgeAuxIntTimeSlotMapEntry:29	29	unMapped	0		0
auxEdgeAuxIntTimeSlotMapEntry:30	30	unMapped	0		0
auxEdgeAuxIntTimeSlotMapEntry:31	31	unMapped	0		0

**Step 3** Edit the following attributes as needed for AuxPortTimeSlot:

- OhByte: e1, e2, f1 or unmapped
- Slot:
- Description:
- Port:

### 4.3.10.7 Power Module - ONS 15305

**Step 1** In the topology browser select **device > power** (Figure 4-26).

Figure 4-26 Power Module - Attributes

Name	Values
Id	power:1
AlarmReporting	disabled
AlarmReportingInputA	disabled
AlarmReportingInputB	disabled
Description	PowerModule
	1

**Step 2** Edit the following attributes as needed:

- AlarmReporting  
disabled or enabled
- AlarmReportingInputA  
disabled or enabled
- AlarmReportingInputB

disabled or enabled

- Description

free text description

## 4.4 Synchronization Management

The purpose of this section is to select the synchronization source for internal SDH timing (T0) and external synchronization output (T4).

The ONS 15305 T0 and T4 automatic selection processes can select the source from a short list of available inputs. This selection is based on quality and priority.

You can override the automatic selection process by manual commands.

The first part of this section gives a short introduction to SDH synchronization which is meant to help the reader in understanding the requirements specified in this document. The synchronization is G.781 compliant.



### Note

For further reading on SDH synchronization, see *ETSI ETS 300 417-6-1*, *ITU-T Recommendation G.781*, *G.812 ("Timing requirements of slave clocks suitable for use as node clocks in synchronization networks")* and *G.813 ("Timing characteristics of SDH equipment slave clocks (SEC)")*

### 4.4.1 SDH Synchronization

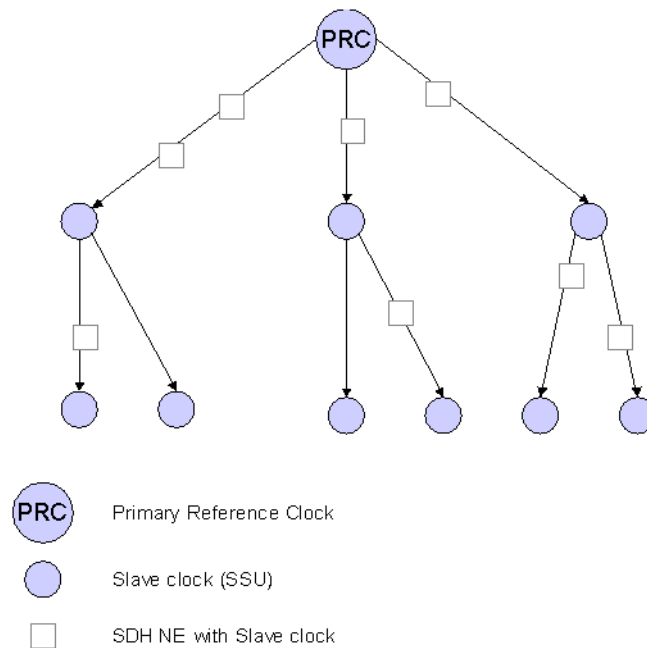
#### 4.4.1.1 Synchronization Networks

A synchronization network is a set of clock nodes that are maintained in synchronization with one another. Synchronization networks require accurate transfer of synchronization reference information between nodes so that their relative synchronization can be monitored and maintained.

Since it is difficult to synchronize all international nodes from the same master clock, each network operator typically has a primary reference clock (PRC) as defined in ITU-T Recommendation G.811.

From the PRC the synchronization reference information is distributed to all nodes in the SDH network in a tree-type network topology ([Figure 4-27](#)).



**Figure 4-27 Synchronization Network Example**

Intermediate slave clocks can enter holdover conditions if their connection to the master clock is lost. Slave clocks called Synchronization Supply Units (SSUs) will continue to serve their branch of the network until the connection with the PRC is reestablished. There may be several SSUs concatenated in a large network.

Intermediate SDH NEs will also contain slave clocks, the SDH equipment Clock (SEC). Their quality is not sufficient for providing synchronization reference information to other parts of the network, but they can serve the SDH NE itself in holdover mode if all high-quality incoming references are lost.

As shown in [Figure 4-27](#), the SDH NEs have a dual role since they need a synchronization reference to operate properly in a network and they are important for distribution of synchronization reference information to other networks.

#### 4.4.1.2 Selecting the Best Synchronization Reference

To reinforce the reliability of the synchronization network, alternative routes are often used between the clocks. The slave clock can then be switched to another synchronization reference manually, or automatically by monitoring the signal at the physical interface.

An improvement to simple signal monitoring is to send the synchronization status message (SSM) along with the synchronization signal to indicate the quality level (clock type) of the source clock. The next clock in the chain can now select the best clock based on this quality level.

Not all connections used for synchronization can send the SSM along with its synchronization reference. In this case it is possible to manually indicate the quality level for this interface in ONS 15305. This ensures that also references without SSM can be part of the automatic selection process that is based on quality level.

To avoid timing loops in the network it may be necessary to indicate in SSM that a synchronization reference should not be used. To do so, send the do not use (DNU) message.

### 4.4.1.3 Synchronizing the SDH Equipment

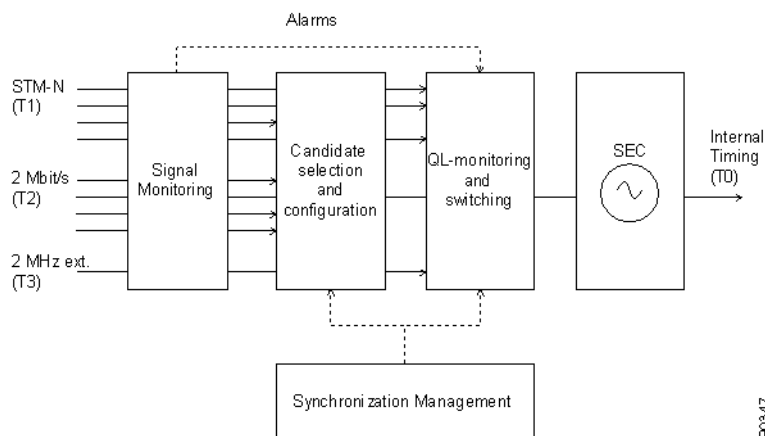
All SDH equipment contains a clock for the SDH pointer adjustments, cross-connection matrix operations, and the outgoing line signal (STM-N). It is normally operating as a slave clock and locked to a high quality incoming reference, but can run in holdover mode if the reference is lost.

This section describes how the internal timing (T0) is derived from the available synchronization references in ONS 15305.

Synchronization reference information can be extracted from any of the incoming STM-N SDH interfaces (T1), 2 Mbps PDH interfaces (T2), or the external 2 MHz synchronization input (T3) as indicated in Figure 4-28.

The figure shows that only one the available synchronization references will be used as a reference for the SEC. SEC is the clock used for internal timing (T0). When no reference is available it will run in Hold-over mode.

**Figure 4-28 T0 Selection**



## 4.4.2 ONS 15305

### 4.4.2.1 Signal Monitoring

All interfaces are monitored for signal level and framing errors. The failure will be reported to the candidate selection and QL-monitoring and switching processes.

### 4.4.2.2 Candidate Selection and Configuration

In the ONS 15305 up to five synchronization reference candidates can be selected to participate in the selection process.

For each synchronization source candidate the following parameters can be read or configured:

- Type (T1, T2, or T3 where T2 must be a 2 Mbps PDH Port in PRA mode).
- Identification of the synchronization source candidate (via its slot number, port number, etc.)
- Whether SSM usage is enabled (T1 only).

- Assigned quality level (QL). If SSM usage is disabled, the operator is free to assign a fixed QL.
- Current quality level. If SSM usage is enabled (T1) the quality level of the incoming signal is seen here. If an alarm is detected on the synchronization source interface, the current quality level indicates failure (Independent on SSM usage).
- The priority of the synchronization source candidate. This priority will apply only when there are multiple candidates all having the highest QL among all possible source candidates.
- Hold-Off time and wait-to-restore time.

For each synchronization source candidate the following methods are available:

- Set or Clear lockout. This is used to temporarily exclude a specified synchronization source.
- Clear WTR.

### 4.4.2.3 QL-Monitoring and Switching

The QL-monitoring and selection process will continuously monitor the QL of the candidate synchronization references and select the reference with the best QL. Only error free references are included in the selection process. (Alarms are detected in the signal monitoring functional block). If there is more than one candidate with the highest available QL, the priority parameter will be used for selection.

The following parameters can be read or configured for the selection process:

- Selected synchronization reference and its QL.
- Switch mode. This indicates whether the selection process is running in the automatic, forced, or manual switch mode.
  - Manual switch command. A manual switch can be performed only to a source with the highest available QL. This means that manual switching can only be used to override the synchronization source priorities.
  - Forced switch command. This command overrides the currently selected synchronization source.
  - Clear command. Clears any of the manual or forced switch commands.

### 4.4.2.4 SEC

The ONS 15305 slave clock.

SEC will enter holdover mode for the specified Hold-Off time if an alarm is detected on the selected synchronization reference. After the Hold-Off time the selection process will switch to the error free reference with the highest QL.

When a candidate synchronization reference recovers from an alarm condition, the signal is free for faults for the wait-to-restore period before taken into consideration by the selection process.

The selected T0 reference is also used on all output STM-N signals.

### 4.4.2.5 Synchronizing External Equipment

ONS 15305 also provides an external synchronization output (T4). This is a separate 2 MHz signal that can be used directly as a synchronization reference for other equipment or as a synchronization reference to separate stand alone synchronization equipment (SASE).

The figure shows that only one of the available synchronization references will be used for external timing (T4).

```

graph LR
 STMN[STM-N (T1)] --> SM[Signal Monitoring]
 T0[Internal Timing (T0)] --> SM
 SM --> CSC[Candidate selection and configuration]
 CSC --> QLS[QL-monitoring and switching]
 QLS --> T4[External Timing (T4)]
 SM -.-> SMgt[Synchronization Management]
 CSC -.-> SMgt
 QLS -.-> SMgt
 SMgt -.-> SM
 SMgt -.-> CSC
 SMgt -.-> QLS

```

- When referring to a T1 or T2 synchronization reference, slot and port numbering is used.
- When referring to the T0 or T3 synchronization reference, no further identification is required.
- SSM is always disabled for T2 and T3 references
- A 2 Mbps PDH port should be treated as a T2 source only when it is operating in PRA mode.
- In principle a user can add the same source twice, but you should be advised not to do this.
- More than one reference can have the same priority.
- A warning message appears before an active synchronization source is deleted. No further restrictions apply.
- The automatic selection process will find the best source based on the current QL. If more than one source has the highest QL, the source with the highest QL and priority will be selected. If the priority is also the same, the ONS 15305 will choose the first source in the list with the highest QL and priority.
- A manual switch can be performed only to a source with the highest available QL.
- A forced switch overrides the currently selected synchronization source.
- The new source selected by the manual and forced switching cannot have a current quality level of failure or SEC.
- WTR clear does not exist as a method in the MIB. The WTR must be set to 0 and then back to its original value if the method is implemented in the manager.
- T0 is the default candidate for T4.
- If no candidates are available for the T4 selection process, no synchronization source is selected and the external synchronization output is squelched.

- When QL of the selected T4 reference falls below the QLM level, the T4 output signal is squelched (muted) to allow the slaved oscillator to go into holdover or to select another reference.
- T4 is only used for external synchronization output (not for output STM-N signals).

### 4.4.2.7 Synchronization Alarms

Synchronization alarms are treated the same as other ONS 15305 alarms.

Figure 4-29 identifies the alarms related to SDH synchronization events.

**Table 4-6 Alarms Related to SDH Synchronization Events**

Alarm ID	Description	Comment	Clearable	Default Severity
T0_HOLDOVER	SETG enters holdover	No sync. sources available (applies to T0 sync. only)	Yes	MAJOR
T0_SWITCH	Change of sync. source	Applies to automatic, manual or forced switchover (T0 only).	No	INFO
SYNCSRC_QL	QL_FAILED or QL_DNU for any sync. candidate	Applies to T1/T2/T3 sources member of the T0 sync. table	No	INFO
T4_SQUELCH	T4 output squelched (on permanent basis)	No T4 sync. candidate with QL equal to or above QLmin	Yes	MAJOR
T0_DEFECT	SETG failure	Caused by defective hardware impacting the internal T0 clock	Yes	CRITICAL



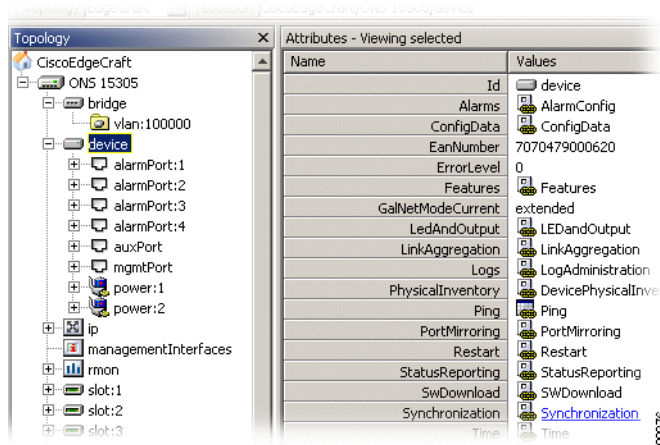
**Note**

A synchronization candidate is a synchronization source contained in either of the T0 or T4 synchronization source tables (5 entries each).

### 4.4.3 View the Synchronization Data (T0 or T4)

T0 and T4 Synchronization are combined in the flow descriptions because of their common behavior. Users are assumed to be experienced SDH users because synchronization management is not directly related to the services offered by ONS 15305.

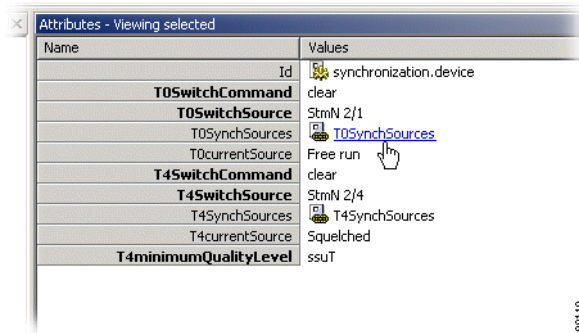
Access the synchronization attributes from the topology browser (Figure 4-30).

**Figure 4-30 Synchronization - Selecting Managed Object**

The system presents a list of all Synchronization Source candidates (Figure 4-31).

**Figure 4-31 Synchronization - T0 SynchSources attribute**

1.



If the source experiences a signal error the SSM attribute shows failure instead of the SSM value.

The system presents the synchronization attributes with the relevant data.

## 4.4.4 Add Synchronization Source Candidate (T0 or T4)

- Step 1** Select T0 SynchSources or T4 SynchSources (Figure 4-31).
- Step 2** Click **Add** in the toolbar (Figure 4-32).

Figure 4-32 Add Synchronization Source

Id	PortDes...	Lockout	Type	OperQuality	Slot	HoldOffTi...	Ssm	AdminQuality	Priority	Port
axxEdeDeviceSyncT4Entry:1		set	stmN	doNotUse	2	300	enabled	sec	1	1
axxEdeDeviceSyncT4Entry:2		clear	stmN	failed	2	300	enabled	sec	1	4
axxEdeDeviceSyncT4Entry:3		clear	stmN	failed	2	300	enabled	sec	1	2

**Step 3** Enter the synchronization parameters in the topology browser for the new candidate. The list of existing synchronization source candidates must be less than five.

- **Type:** STM-n, e1, external
- **Slot/ Port:** number
- **SSM:** enabled/disabled
- **Admin Quality/Assigned Quality Level** (N/A when SSM is enabled): sec, ssuL, ssuT, prc
- **Priority:** 1..5 (where 1 is highest priority)
- **Lockout:** clear/set
- **Hold-Off Time:** 300..1800 ms
- **Wait To Restore Time:** 0..12 min

**Step 4** Click **Save**.

If you attempts to add a new synchronization source candidate when the candidate list is fully populated (five entries), you will be informed that a candidate must be deleted before adding a new candidate.

The system verifies that the candidate is legal before performing the addition. If any errors are found, the candidate is not added and you are given the opportunity to correct the problem.

You can add more than one candidate before committing, and a failure on one candidate has no consequence for the addition of the other candidates.

## 4.4.5 Modify Synchronization Source Candidate (T0 or T4)

**Step 1** Access the synchronization attributes from the topology browser (Figure 4-31).

**Step 2** Modify the synchronization source candidate attributes as needed. SSM Enabled can be True only for T1. QL can only be modified if SSM enabled is False.

**Step 3** Click **Save** to commit the changes.

## 4.4.6 Delete Synchronization Source Candidate (T0 or T4)

There are two methods for deleting a synchronization source candidate:

**Step 1** Access the synchronization attributes from the topology browser.

## 4.4 Synchronization Management

**Step 2** Select the **synchronization source candidate(s)** to delete and click **Delete** in the toolbar menu.

**Step 3** Click **Save**.

**Step 1** Select the Port (synchronization source) in the topology browser

**Step 2** Select **Do not use for T0 Synchronization** from the drop-down menu.

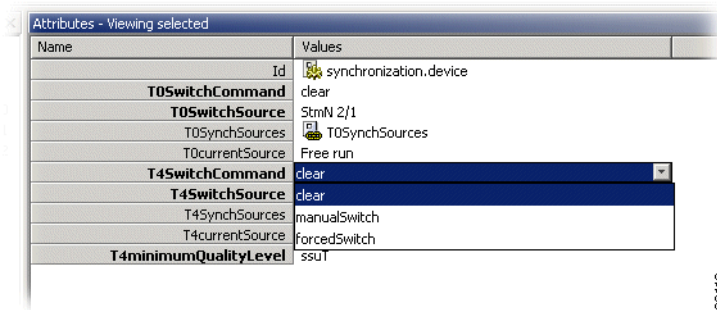
**Step 3** Select **Delete**. If synchronization source candidate is the active synchronization source, a warning message appears.

**Step 4** Click **Save**.

## 4.4.7 Operate Synchronization Switch (T0 or T4)

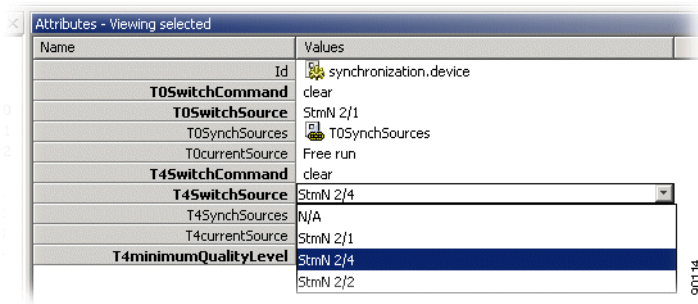
**Step 1** Select **T0** or **T4SwitchCommand** and set to desired value, [Figure 4-33](#).

**Figure 4-33 Operate Synchronization Switch 1**



**Step 2** Click **T0** or **T4SwitchSource** and select **new** synchronization source ([Figure 4-34](#)).

**Figure 4-34 Operate Synchronization Switch 2**



**Step 3** Click **Save**.

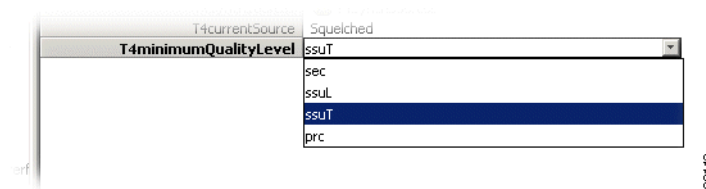


If the switch parameters are valid, the switch is performed. If a manual or forced switch is performed, the selected source will remain selected until a new forced, manual, or clear command is sent.

## 4.4.8 View Synchronization Switch (T0 or T4)

**Step 1** Access the synchronization attributes from the topology browser (Figure 4-35).

**Figure 4-35 View Synchronization Switch**



**Step 2** Edit the synchronization switch attributes as needed:

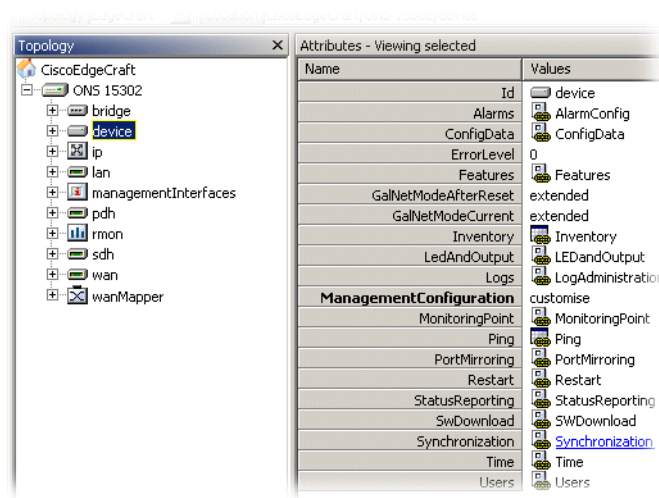
- QLM (T4 Only)
- Manual, Forced, or Automatic selection mode

## 4.4.9 Activate Synchronization on the ONS 15302

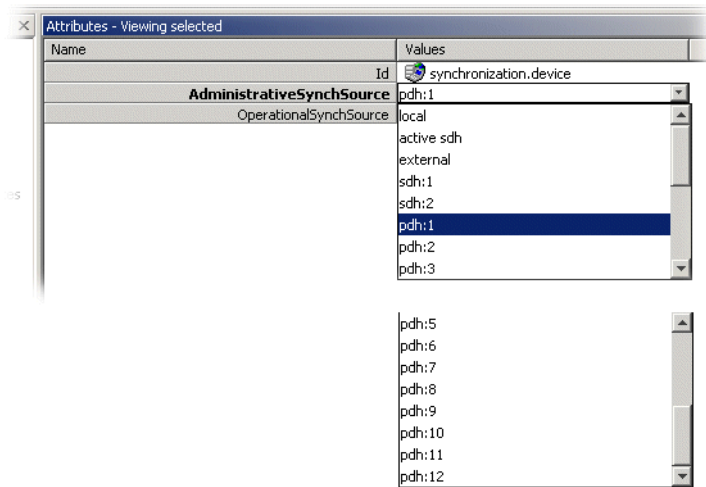
Complete the following steps to activate synchronization for the ONS 15302.

**Step 1** In the topology browser select **device > Synchronization** (Figure 4-36).

**Figure 4-36 Select Synchronization**



**Step 2** Select **AdministrativeSynchSource** from the pulldown menu (Figure 4-37).

**Figure 4-37 Select AdministrativeSynchSource**

**Step 3** Click **Save** to activate the selected synchronization source.

## 4.5 Download Software to a Network Element

The purpose of this section is to describe the download of new software to the network element. The task of the management system is to give the network element the necessary information for it to begin downloading new software. The download process is controlled by the element itself.

The section involves presentation of an ongoing download process, starting a new software download process, restart of device after download, and switching between two banks in the element where the software is located.

### 4.5.1 Network Release

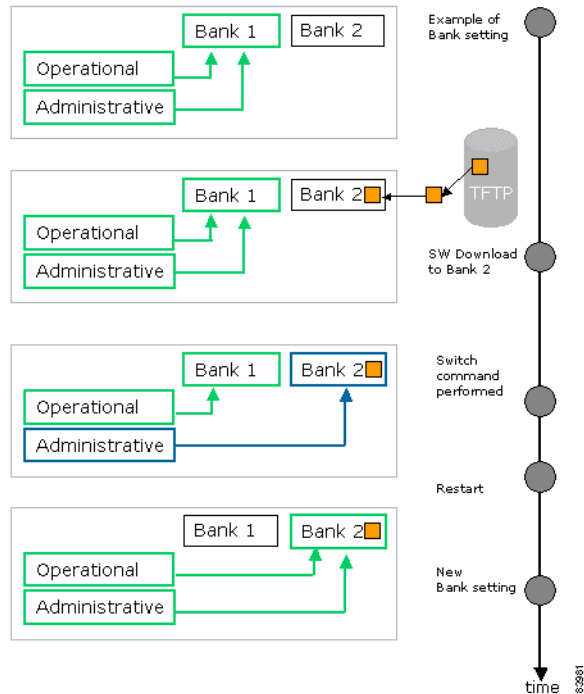
The network element contains device software, firmware, and license and module firmware. Software and firmware updates are delivered in network releases, which supports a given set of traffic modules. If a new module is introduced, the network element needs a new network release.

A network release is delivered as a zip-file together with a network release control file. The file must be unzipped and its contents must be copied to the TFTP server. You must initiate the download of the control file. The remaining part of the upgrade will be controlled by the embedded software on the network element; therefore, verify which files are included in the release and download those files that are missing or are too old in the network element.

## 4.5.2 Operational and Administrative Software Bank

ONS 15305 network elements store software or firmware in banks. There are two banks, one administrative and one operational. Bank 1 initially is both the administrative and the operational (Figure 4-38). After a software download to bank 2, a switch (bank) command is performed and bank 2 becomes the administrative bank. When a restart is done, bank 2 also becomes the operational bank and the new software is active.

**Figure 4-38 Example of Switching Software Banks**



## 4.5.3 Effect of Software Upgrades on Traffic

A software update/upgrade including an FPGA fix will affect all traffic. Traffic affected depends on module configuration, therefore a network release download will affect the modules that are a target for the FPGA fix in the downloaded network release.

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:

- When the STP mode is changed, for example from per device to per VLAN (Ethernet/IP traffic affecting)
- When decreasing/increasing entries in tunable tables, for example maxARP, maxVLANs, maxBridge, etc.
- When a software upgrade without an FPGA fix occurs (Ethernet/IP traffic affecting)

- When a software upgrade with FPGA fix occurs (All traffic affected)

The period of time from the moment you have triggered a restart to when the device is up and running depends on modules and the software configuration of the device. The down period depends on installed modules and configuration.

## 4.5.4 Download an ONS 15305 Network Release

A network release is delivered as a zip-file together with a network release control file (Figure 4-39).

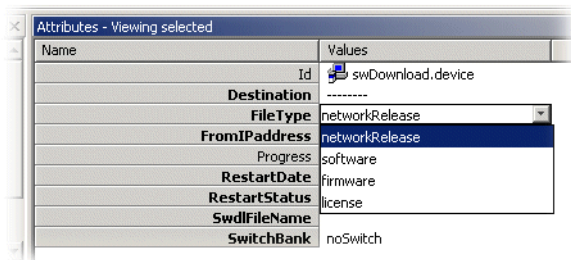


### Note

See the release notes for an example of a TFTP server that has been verified to work in cooperation with CiscoEdgeCraft.

- Step 1** Unzip the Network Release File.
- Step 2** Copy the contents to the TFTP - server.
- Step 3** In the topology browser select **device** > **SWdownload**.
- Step 4** Set **destination** to **device**.
- Step 5** Set **Filetype** to **networkRelease**.

**Figure 4-39 Download of Release Files**



- Step 6** Enter **FromIPAddress** (TFTP server Ip address).
- Step 7** Set **restartstatus** to **immediateRestart**.
- Step 8** Enter **SwdlFileName** attribute values (File path and name).



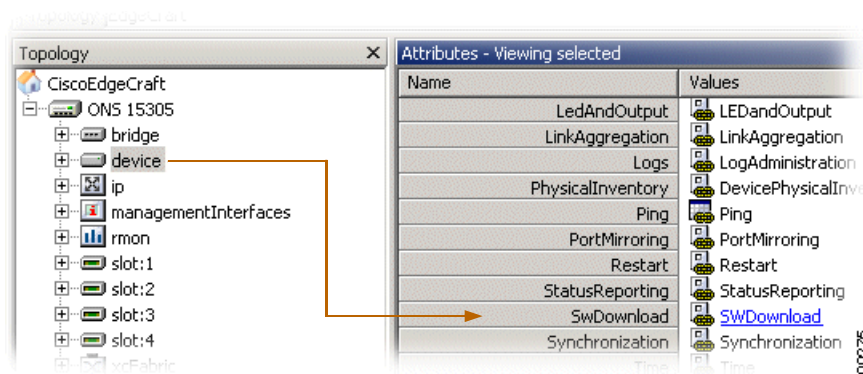
### Note

Click **Save**. The status of the SwitchBank attribute (switch/noSwitch) is overruled when Filetype is set to networkRelease; a switch will be performed.

## 4.5.5 Download Software to the ONS 15305

- Step 1** In the topology browser select **device** and then **SWDownload** (Figure 4-40).

Figure 4-40 Select Device



Modify the following attributes as needed:

- Select a **destination**.
- Set **Filetype** to software.
- Enter the **FromIPAddress** (TFTP server Ip address).
- Set the **RestartDate**.
- Select **RestartStatus**.
- Select **Delayed Restart** if the network element should restart at a specific date/time after the download process.
- Enter the **SwdlFileName** attribute values (File path and name).
- Set the **SwitchBank** attribute:
  - Switch
 

After the restart the operational bank will be switched and the new (downloaded) SW will be active.
  - noSwitch
 

The operational bank will not be switched after the restart, hence a manual switch must be performed in order to activate the new software. For further details see [“4.5.5.1 Switch Banks Manually”](#) section on page 4-35.

**Step 2** Click **Save**.

### 4.5.5.1 Switch Banks Manually

- Step 1** In the topology browser select **device > DevicePhysicalInventory > Software**.
- Step 2** Select **Administrativebank** and switch to **opposite** bank number.
- Step 3** Click **Save**.
- Step 4** Perform a restart.

## 4.5.6 Download Software to the ONS 15302

- 
- Step 1** In the topology browser select **device > SWdownload**.
- Step 2** Enter the **FromIPAddress** (TFTP server Ip address).
- Step 3** Enter the **SwdlFileName** attribute values (File path and name).
- Step 4** Click **Save**.
- Step 5** Perform a restart.
- 

## 4.6 Back Up and Restore Configuration Data

The purpose of this section is to guide you through management of the configuration data in the network element.

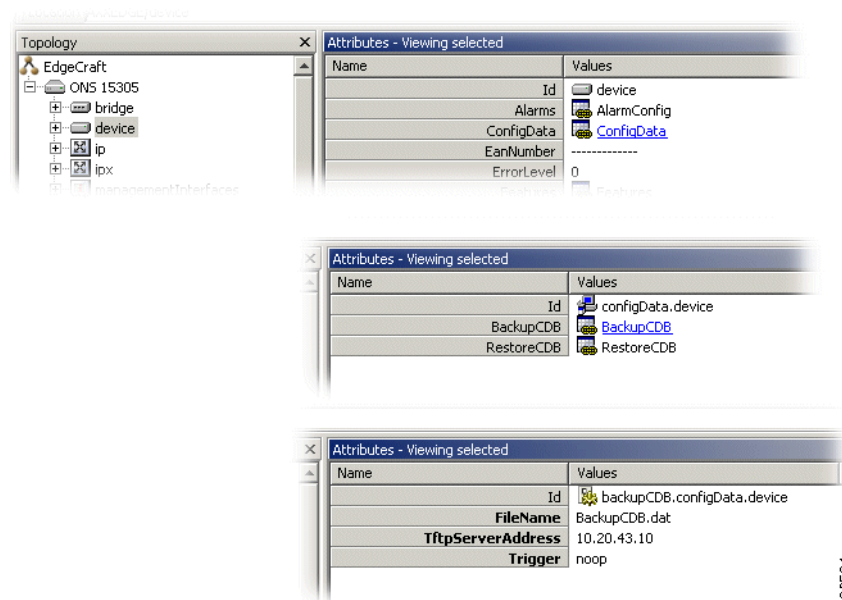
The configuration data is BER coded and cannot be edited on the host.

### 4.6.1 Back Up Configuration Data

Use the following steps to perform a back up of the configuration data and put it on the TFTP-server.

- 
- Step 1** In the topology browser select **device**.
- Step 2** Click **ConfigData**. Select whether to upload or download the configuration from or to the network element ([Figure 4-41](#)).

**Figure 4-41 Select ConfigData**



**Step 3** Select **BackupCDB**.

**Step 4** Edit the following attributes as needed:

- **TftpServerAddress**  
Destination IP address if configuration data should be uploaded on a remote host.
- **FileName**  
File name and path for the configuration data storage.
- **Trigger**  
If set to noop only parameters are saved.  
If set to backup, the backup operation is started when clicking save.

**Step 5** Set **trigger** to **backup**.

**Step 6** Click **Save**.

**Step 7** The TFTP upload process starts on the network element and the configuration data is stored on the selected host in the specified location (path and file name.)



---

**Note** Cisco recommends monitoring the TFTP console during the upload process.

---



---

**Note** Some TFTP servers require that the file exist on the TFTP server before the upload can be performed.

---

## 4.6.2 Restore Configuration Data

If a scheduled restart is set before a new configuration data download process is started, the scheduling parameters will be overwritten.

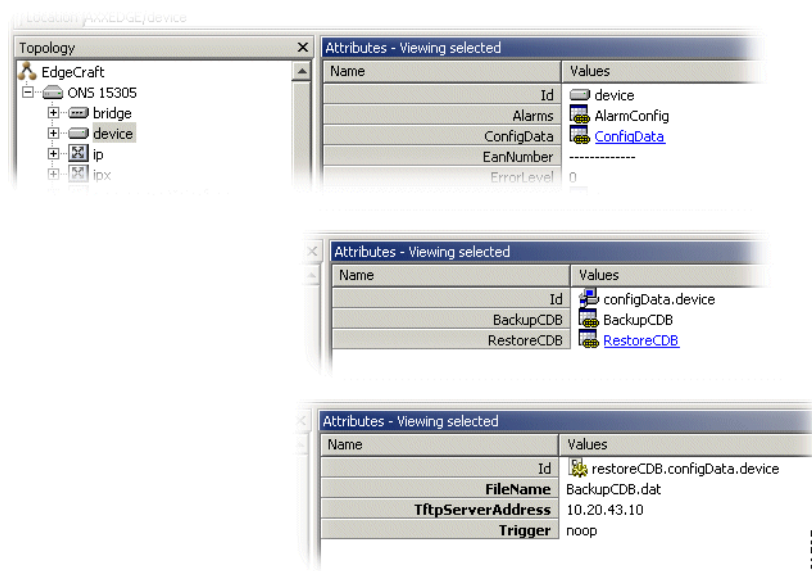
For Cisco Edge Craft to restart the NE after the TFTP download session is terminated, the Cisco Edge Craft needs to be able to capture the endTftpSession trap sent from the NE. To enable trap-sending see the [“1.3.2 Configure Community-Handler”](#) section on page 1-5.

---

**Step 1** In the topology browser select **device**.

**Step 2** Click **ConfigData**. Select whether to upload or download the configuration from or to the network element ([Figure 4-42](#)).

Figure 4-42 Select Device



**Step 3** Select **RestoreCDB**.

**Step 4** Edit the following attributes as needed:

- **TftpServerAddress**  
Source IP address if configuration data to be downloaded.
- **FileName**  
File name and path for the configuration data storage.
- **Trigger**  
If set to noop only parameters are saved.  
If set to backup, the restore operation is started when clicking save.

**Step 5** Set **trigger** to **restore**.

**Step 6** Click **Save**.

The TFTP upload process begins and the configuration data is stored in the network element. Cisco Edge Craft will restart the network element after the restore is complete.



**Note** Cisco recommends the TFTP console during the download process.

## 4.7 Alarm and Event Configuration

This section explains how to configure alarm and event reporting and suppress and configure specific alarms.



The network element has a predefined set of combinations of managed objects and alarm types, that means alarm points. These combinations can not be changed by you but the severity level and a description can be defined.

Suppression of specific alarms is important to avoid alarm floods in the network and to focus on the root cause. The ONS 15305 allows you to suppress many alarm types, for example AIS.

You can suppress alarms that are oscillating between activity and inactivity. A time interval (a persistency filter) indicates the time period an alarm must have been on or off before being reported. The persistency filters are defined for a group of alarms of a specific type.

There are three possible persistency group categories:

- High order level alarms
- Low order level alarms
- Unfiltered alarms

For some managed objects you can enable or disable the alarm reporting.

## 4.7.1 Event Forwarding

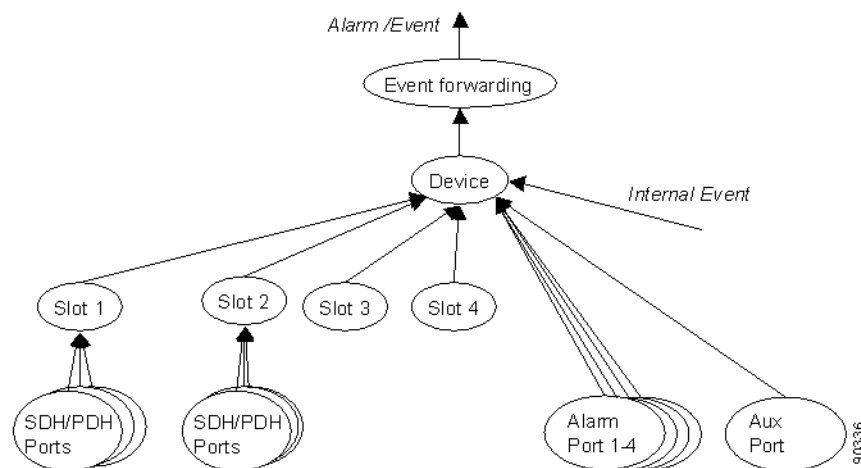
Alarms or events cannot be reported before the identity of the receiver of alarms and events has been configured. It is possible to forward alarms and events to more than one receiver.

Event forwarding is enabled when a new user is added with the TrapsEnable attribute set to TrapsEnable as described in the [“5.3.2 Set a Loop in a ONS 15305 PDH Port”](#) section on page 5-8.

## 4.7.2 Configure General Alarm Reporting

In ONS 15305 there are several levels where alarm reporting can be disabled or enabled. Alarms will be reported to a manager only when alarm reporting is enabled on all levels ([Figure 4-43](#)). In addition the event forwarding must be configured for the IP address of the manager (described in the [“4.7.1 Event Forwarding”](#) section on page 4-39).

**Figure 4-43 General Alarm Reporting Filters.**



Note that all alarms from objects in the following sections must pass through the filter:

- [4.7.2.1 Device Alarm Enabling, page 4-40](#)
- [4.7.2.2 Slot Alarm Enabling, page 4-40](#)
- [4.7.2.3 Traffic Port Alarm Enabling, page 4-40](#)
- [4.7.2.4 Alarm Port Alarm Enabling, page 4-40](#)
- [4.7.2.5 Aux Port Alarm Enabling, page 4-40](#)

In addition to general alarm reporting, it is possible to filter specific alarm types on specific object instances.

### 4.7.2.1 Device Alarm Enabling

It is possible to enable or disable alarm and event reporting from ONS 15305. In the disabled state, alarms or events are not reported (some generic events, like cold start, etc. are still reported).

- 
- |               |                                                                                     |
|---------------|-------------------------------------------------------------------------------------|
| <b>Step 1</b> | In the topology browser select <b>device &gt; AlarmConfig &gt; AlarmReporting</b> . |
| <b>Step 2</b> | Set <b>AlarmReporting</b> to <b>enabled</b> or <b>disabled</b> .                    |
- 

### 4.7.2.2 Slot Alarm Enabling

- 
- |               |                                               |
|---------------|-----------------------------------------------|
| <b>Step 1</b> | Select the slot that should report alarms.    |
| <b>Step 2</b> | Set <b>AlarmReporting</b> to <b>enabled</b> . |
- 

### 4.7.2.3 Traffic Port Alarm Enabling

- 
- |               |                                                       |
|---------------|-------------------------------------------------------|
| <b>Step 1</b> | Select the SDH or PDH port that should report alarms. |
| <b>Step 2</b> | Set <b>AdminStatus</b> to <b>enabled</b>              |
- 

### 4.7.2.4 Alarm Port Alarm Enabling

- 
- |               |                                                               |
|---------------|---------------------------------------------------------------|
| <b>Step 1</b> | Select the Alarm port that should report alarms.              |
| <b>Step 2</b> | Set <b>AdminStatus</b> to <b>enabled</b> or <b>disabled</b> . |
- 

### 4.7.2.5 Aux Port Alarm Enabling

- 
- |               |                                                |
|---------------|------------------------------------------------|
| <b>Step 1</b> | Select the Aux port that should report alarms. |
| <b>Step 2</b> | Set <b>AdminStatus</b> to <b>enabled</b> .     |
-

**Note**

Slot and port alarm reporting is disabled by default when the slot is configured for a new module.

## 4.7.3 Suppress Specific Alarms

In addition to configuration of the general alarm filters described above, it is possible to suppress specific alarm types to avoid alarm floods in the network. Other alarms from the same objects will be reported independently of these settings.

### 4.7.3.1 Suppress RDI, EXC, DEG, SSF Alarms

RDI, EXC, DEG, and SSF alarm reporting can be suppressed from the VC-12, VC-3 or VC-4 layers.

- 
- Step 1** In the topology browser select **device > AlarmConfig > AlarmReportingVc**.
- Step 2** Set **suppress** for the **attributes** corresponding to the **Alarms** that should be suppressed:
- RdiAlarms
  - ExcAlarms
  - DegAlarms
  - SsfAlarms
- 

### 4.7.3.2 Suppress AIS Alarms from SDH Ports

AIS alarm reporting can be suppressed from the TU-12, TU-3, or AU-4 layers.

- 
- Step 1** In the topology browser select **device > AlarmConfig > AlarmReportingVc**.
- Step 2** Set **suppress** for the **AisAlarms** attribute.
- 

### 4.7.3.3 Suppress AIS Alarms from E1 Ports

- 
- Step 1** In the topology browser select **device > AlarmConfig > AlarmReportingE1**.
- Step 2** Set **AisAlarms** to **suppress**.
- 

### 4.7.3.4 Suppress AIS Alarms from AUX Port

- 
- Step 1** In the topology browser select **device > AlarmConfig > AlarmReportingAux**.
-

**Step 2** Set **AisAlarms** to **suppress**.

## 4.7.4 Modify Alarm Severity and Description

It is possible to modify the severity of the reported alarms from ONS 15305.

**Step 1** In the topology browser select **device > AlarmConfig > AlarmPointConfig**.

**Step 2** Set the severity level and description for the combination of alarm type and object type. The next time the alarm is reported from this object type it will come up with the configured severity and description in the alarm list.

## 4.7.5 Set Signal Degrade Threshold

The threshold for a DEG alarm to be reported (and used for MSP switching) can be set for the VC-12, VC-3, VC-4, MS, and RS layers.

**Step 1** In the topology browser select **device > AlarmConfig > SdThreshold**.

**Step 2** Set **SdThreshold** to a value between  $-6$  and  $-9$  ( $\text{BER} = 10 \exp -6$  to  $10 \exp -9$ ).

## 4.7.6 Modify Alarm Persistency

Alarm reporting on and off can be delayed by setting the alarm persistency filters in ONS 15305. The alarms are divided into groups according to their importance for fault management (Table 4-7, Table 4-8, and Table 4-9).

### 4.7.6.1 Persistency Group 1 (HighOrderLevel)

**Table 4-7 Persistency Group 1 (HighOrderLevel)**

Associated Alarm Types	Object Classes Associated with Each Alarm Type
LOS	SdhPort, pdhPort
LOF	rs
AIS	ms
EXC	rs, ms
DEG	rs, ms
TIM	rs
RDI	ms

**Table 4-7** Persistence Group 1 (HighOrderLevel)

Associated Alarm Types	Object Classes Associated with Each Alarm Type
CDF	rs, ms
AUX	auxPort

### 4.7.6.2 Persistence Group 2 (Unfiltered)

**Table 4-8** Persistence Group 2 (Unfiltered)

Associated Alarm Types	Object Classes Associated with Each Alarm Type
LOP	tu4, tu3, tu12
LOM	vc4
LOF-RX, LOF-TX	e1

### 4.7.6.3 Persistence Group 3 (LowOrderLevel)

**Table 4-9** Persistence Group 3 (LowOrderLevel)

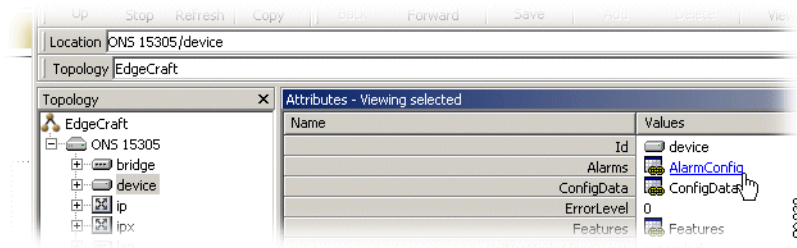
Associated Alarm Types	Object Classes Associated with Each Alarm Type
AIS	tu4, tu3, tu12, e1, e3
EXC	vc4, vc3, vc12
DEG	vc4, vc3, vc12
SSF	vc3, vc12
TIM	vc4, vc3, vc12
RDI	vc4, vc3, vc12
UNEQ	vc4, vc3, vc12
PLM	vc4, vc3, vc12

**Step 1** In the topology browser select **device > AlarmConfig > AlarmPersistence**.

**Step 2** Set **onFilter** or **offFilter** to a value between 0 and 30 seconds.

## 4.7.7 Modify ONS 15302 Alarm Configuration Attributes

**Step 1** To locate alarm configuration attributes, select **device > AlarmConfig** (Figure 4-43).

**Figure 4-44 Select Device**

- Step 2** To modify the alarm severity and description, select device > **AlarmConfig** > **AlarmConfig** (Figure 4-45).

**Figure 4-45 Select Alarm Config**

Name	Values
Id	alarms.device
AlarmConfig	AlarmConfig
<b>AlarmReporting</b>	enabled
AlarmReportingAisRdi	AlarmReportingAisRdi
AlarmReportingAll	AlarmReportingAll
Persistency	Persistency
SdThreshold	SdThreshold

- Step 3** Set the **Severity level** and **Description** for the combination of alarm type and object type of your choice.
- Step 4** Click **Save**. The next time the alarm is reported from this object type it will come up with the configured severity and description in the alarm list.

### 4.7.7.1 View all Alarm Reporting Instances

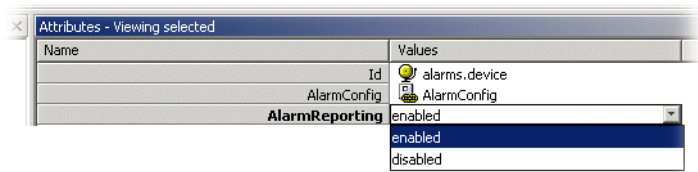
To view all alarm reporting instances, select **AlarmReportingAll** (Figure 4-46).

**Figure 4-46 Select AlarmReportingAll**

Name	Values
Id	alarms.device
AlarmConfig	AlarmConfig
<b>AlarmReporting</b>	enabled
AlarmReportingAisRdi	AlarmReportingAisRdi
AlarmReportingAll	AlarmReportingAll
Persistency	Persistency
SdThreshold	SdThreshold

### 4.7.7.2 Enable Alarm Reporting

- Step 1** To enable alarm reporting, set **AlarmReporting** to **enable** using the drop-down menu (Figure 4-47).

**Figure 4-47 Select AlarmReporting**

**Step 2** Click Save.

### 4.7.7.3 Modify Ais Rdi Alarm Reporting

**Step 1** Select AlarmreportingAisRdi (Figure 4-48).

**Figure 4-48 Select AlarmreportingAisRdi**

Name	Values
Id	alarms.device
AlarmConfig	AlarmConfig
<b>AlarmReporting</b>	enabled
AlarmReportingAisRdi	AlarmReportingAisRdi
AlarmReportingAll	AlarmReportingAll
Persistency	Persistency
SdThreshold	SdThreshold

**Step 2** Select the instance.

**Step 3** Select **allow** or **suppress** for the Ais alarm (Figure 4-49).

**Figure 4-49 Select AIS Attributes**

Id	Instance	RdiAlarms	AisAlarms
axx15SE5dhMsAisAlarmReporting:1	ms:1	allow	allow
axx15SE5dhMsAisAlarmReporting:2	ms:2	allow	allow
axx15SE5dhAu4AisAlarmReporting:1	au4:1	NA	allow
axx15SE5dhVc4RdiAlarmReporting:1	vc4:1	allow	NA
axx15SE5dhVc12sRdiAlarmReporting	vc12	supress	NA
axx15SE5dhTu12sAisAlarmReporting	tu12	NA	supress

**Step 4** Repeat for the Rdi alarm.

**Step 5** Click Save.

### 4.7.7.4 Modify Alarm Persistency

Modifying the alarm prsistency filters in the ONS 15302 can prevent alarms that vascillate between activity and inactivity.

**Step 1** In the topology browser select **device** > **AlarmConfig** > **AlarmPersistency** (Figure 4-50).

**Figure 4-50 Set Alarm Persistency Attributes**

Name	Values
Id	alarms.device
AlarmConfig	AlarmConfig
<b>AlarmReporting</b>	enabled
AlarmReportingAisRdi	AlarmReportingAisRdi
AlarmReportingAll	AlarmReportingAll
Persistency	Persistency
SdThreshold	SdThreshold

**Step 2** Set **onFilter** or **offFilter** to a value between 0 and 255 seconds.

**Step 3** Click **Save**.

### 4.7.7.5 Modify Signal Degraded (Sd) Threshold

**Step 1** Select **SdThreshold** (Figure 4-51).

**Figure 4-51 Select SDThreshold**

Name	Values
Id	alarms.device
AlarmConfig	AlarmConfig
<b>AlarmReporting</b>	enabled
AlarmReportingAisRdi	AlarmReportingAisRdi
AlarmReportingAll	AlarmReportingAll
Persistency	Persistency
SdThreshold	<b>SdThreshold</b>

**Step 2** Select desired **MO** class

**Step 3** Set **SdThreshold** to a value between 6 and 9 (Figure 4-52).

**Figure 4-52 Set SDThreshold**

Id	MoClass	SdThreshold
axxx155ESdhMsSignalDegradedThreshold:1	Ms	9
axxx155ESdhMsSignalDegradedThreshold:2	Ms	7
axxx155ESdhRsSignalDegradedThreshold:1	Rs	7
axxx155ESdhRsSignalDegradedThreshold:2	Rs	6
axxx155ESdhVc4SignalDegradedThreshold:1	Vc4	8
axxx155ESdhVc12SignalDegradedThreshold	Vc12	7

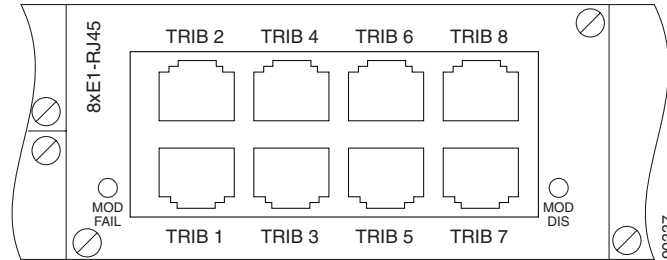
**Step 4** Click **Save**.

## 4.8 Manage ONS 15305 Slots

A slot represents a physical position on the network element where different hardware modules can be installed (Figure 4-53). This section explains how to install and remove modules.



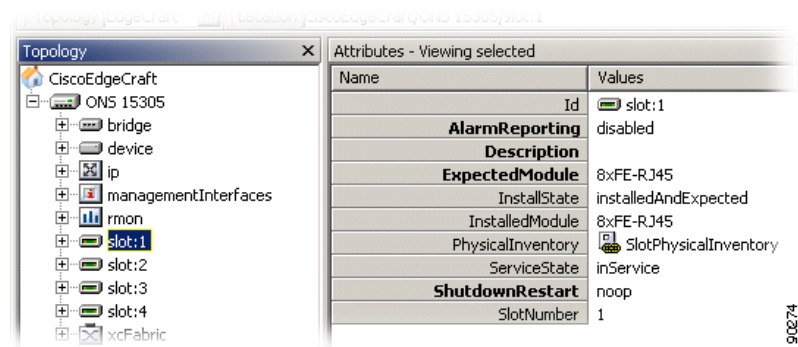
Figure 4-53 ONS 15305 Slots



## 4.8.1 View a Slot

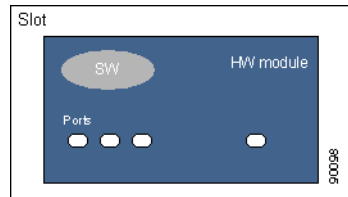
The browser presents four slots numbered from 1 to 4. The slot attributes as defined in the information model are available in the attribute window. Each slot can be equipped with one HW module. By default the slot is unequipped (Figure 4-54).

Figure 4-54 Select Slot



A slot can be empty or have a hardware module with a given number of ports and software version installed (Figure 4-55).

Figure 4-55 Slot Module - Port Concept



The physical inventory data for an installed module also appears in the attribute window.

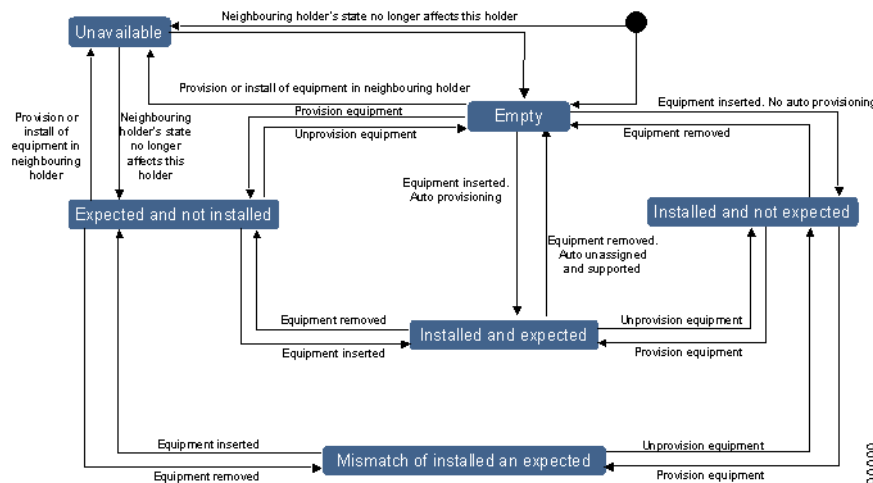
You can preconfigure a slot with an expected module before physically installing a module. The system populates the topology browser according to the specified expected module. The slot has an attribute that reflects the relation between the expected module and the installed module. Slot states include:

- Empty

- Installed and expected
- Expected and not installed
- Installed and not expected
- Mismatch of installed and expected
- Unavailable
- Unknown

A state diagram for the possible transitions of a slot is shown in [Figure 4-56](#). This is the suggested state machine from *TMF 814 supporting documentation, equipmentStates.pdf*.

**Figure 4-56 Relation Between Installed and Expected Module in a Slot.**



A state machine for the values of the attribute describing the relation between an installed and expected module is shown in [Figure 4-56](#).

If a mismatch between the two modules occurs, an alarm will be generated. The alarm is cleared if the module is replaced or the expected module is changed, which means a match between expected and installed is present.

Before replacing a module and selecting a new expected module type, the expected module of the slot must be set to unequipped.

For management of different ports, see [Chapter 5, “Traffic Port Management.”](#)

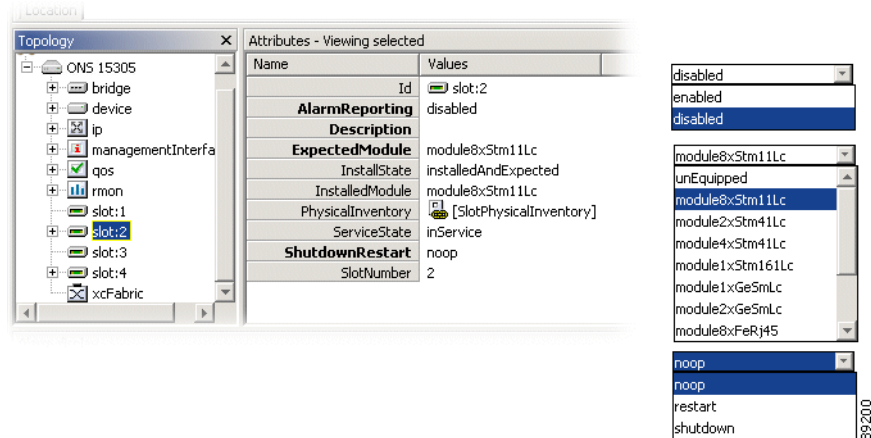
## 4.8.2 Modify a Slot

To modify the expected module attribute, the ports of the previous expected module must be unused and unstructured.

---

**Step 1** Select a target slot ([Figure 4-57](#)).

Figure 4-57 Select Target Slot



**Step 2** Edit the following attributes as needed:

- AlarmReporting  
enable or disable
- ExpectedModule  
select module of current interest
- ShutdownRestart  
noop, restart or shutdown. (noop; No operation is applied)



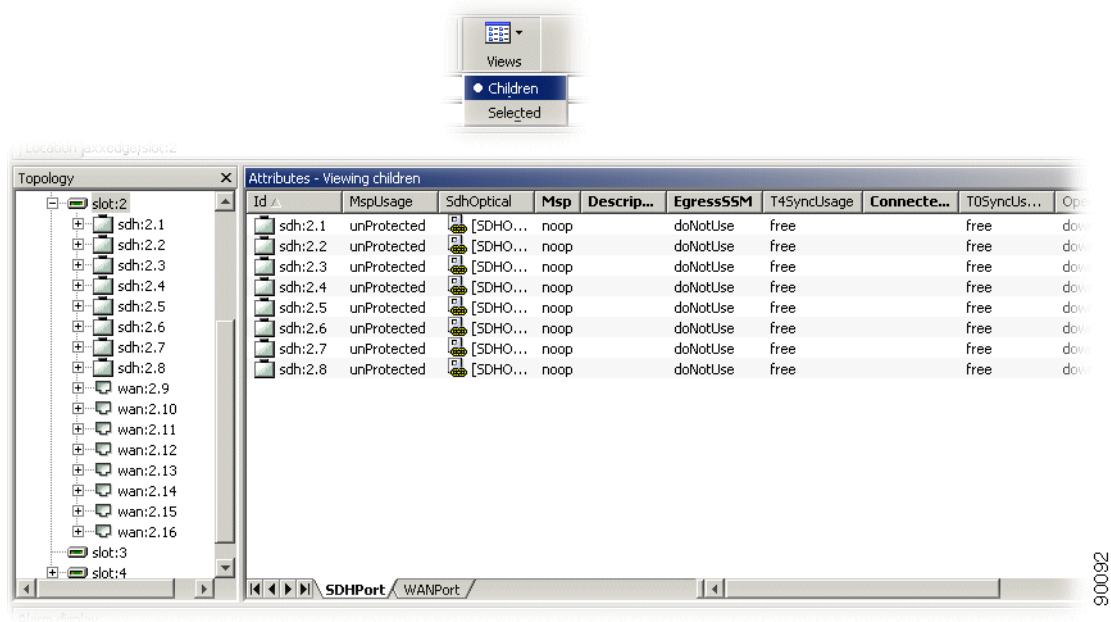
**Note** The attribute Module Interface shows the physical interface on the selected module. This attribute value indicates LongHaul (for example, L-4.2-LC) or ShortHaul (for example, S-4.1-LC) for STM modules. The connector is also indicated.

**Step 3** Click **Save**.

Some changes require a restart of the module. If this is the case you will be prompted to restart.

When a slot has been configured to contain a specific module, the ports of the module are automatically created in the network element. The type of ports created depends on the module type configured for the slot (Figure 4-58).

Figure 4-58 Set View Mode to Children



The ports of an installed module were not created if the slot was configured to contain another module type or being empty.



# Traffic Port Management

---

The ONS 15305 can be equipped with a number of different port types. Some ports are part of the base unit and always present (management port, AUX ports, alarm input, and output ports). The alarm ports and auxiliary port cannot be created or deleted.

For more information see the [“4.1.1 Management Port Configuration” section on page 4-2](#), the [“4.3.10.5 Alarm Ports” section on page 4-20](#), and the [“4.3.10.6 AUX Port - ONS 15305” section on page 4-20](#).

Traffic ports are available on replacable traffic modules. When a slot is configured to support a specific traffic module, the ports of the traffic module are automatically created as described in the [“4.8 Manage ONS 15305 Slots” section on page 4-46](#).

This chapter explains how to configure SDH, PDH, LAN, and WAN traffic ports.

## 5.1 Select a Traffic Port

Traffic ports are always located on a traffic module in Slots 1 to 4. This section describes how to select a traffic port independent of the traffic it carries.

- 
- Step 1** Click on the ONS 15305 managed object, then in the topology browser click the slot managed object where the port is located.
- Step 2** When the slot is expanded, click the port managed object with the desired port number.
- The port is selected and the attributes related to the physical and electrical characteristics of the port appear in the attributes view.
- The physical port usually carries a set of protocols (for example SDH) and the protocols are available from the topology browser.
- 

## 5.2 SDH Ports



### Note

Some procedures in this chapter apply to the ONS15302 and ONS 15305. The procedure heading indicates if a procedure applies only to the ONS15305.

---

## 5.2.1 Configure ONS 15305 SDH Port Structure (Channelization)

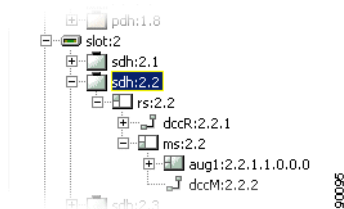
By default the SDH ports are unstructured (or not channeled) when created. Only the sdh Port, rs, ms and aug1 managed objects are available. In this state the paths inside the STM-N frame cannot be terminated or cross connected, but the port can be used as a protection port in an MSP protection scheme and a synchronization source candidate. It can also carry DCN traffic in the DCC channels.

The motivation for structuring an SDH port is to identify the paths in the STM-N frame and make them available for cross-connection. As you structure the port it will fan out in the topology browser, showing termination points that are now available for cross-connection.

### 5.2.1.1 AU4 Termination Points for Cross-connection

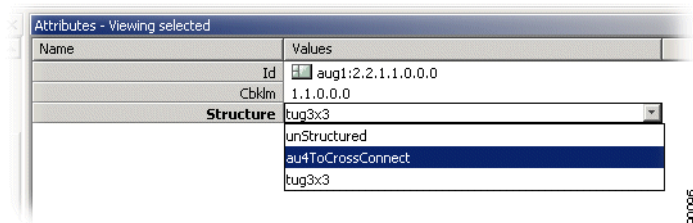
- Step 1** Select an sdh port ([Figure 5-1](#)).
- Step 2** Select the **rs** and then the **ms** managed objects as the port expands.
- Step 3** Select the **aug1** managed object that should be structured. (STM-N ports have N aug1 objects).

**Figure 5-1 Select the Aug1 Managed Object**



- Step 4** Set the **Structure** attribute to **au4ToCrossconnec** ([Figure 5-2](#)).

**Figure 5-2 Set the Structure Attribute**



- Step 5** Click **Save** on toolbar.
- Step 6** Repeat for the other aug1 objects on the port if you want to structure them as au4ToCrossconnect.

### 5.2.1.2 Tu3 Termination Points for XC

- Step 1** Perform [Step 1](#) to [Step 3](#) in the “5.2.1.1 AU4 Termination Points for Cross-connection” section on [page 5-2](#).

- Step 2** Set the **Structure** attribute to **3xtug3**.
  - Step 3** Select the **au4**, **vc4**, and the **tug3** managed objects that should be structured.
  - Step 4** Set the **structure** attribute to **tu3ToCrossConnect**.
  - Step 5** Click **Save** on toolbar.
  - Step 6** Repeat for the other tug3 objects on the port if you want to structure them as tu3ToCrossconnect.
- 

### 5.2.1.3 Tu12 Managed Objects for XC

- Step 1** Perform [Step 1 to Step 3](#) in the “[5.2.1.1 AU4 Termination Points for Cross-connection](#)” section on [page 5-2](#).
  - Step 2** Set the **Structure** attribute of the **tug3** managed object to **21xtu12ToCrossConnect**.
  - Step 3** Click **Save** on toolbar.
  - Step 4** Repeat for the other tug3 objects on the port if you want to structure them as 21xtu12ToCrossconnect.
- 

## 5.2.2 Modify or Remove ONS 15305 SDH Port Structure

It is also possible to modify or remove the structure of an SDH port when the involved termination points are not cross connected.

### 5.2.2.1 Modify Between Tu12 and Tu3 Objects

- Step 1** Remove all cross-connections that are terminated in the tu12 or tu3 termination points belonging to the tug3 object that you want to modify.
  - Step 2** Follow the guidelines in the “[5.2.1 Configure ONS 15305 SDH Port Structure \(Channelization\)](#)” section on [page 5-2](#), to make tu3 or tu12 termination points of an SDH port available for cross-connection.
- 

### 5.2.2.2 Modify Between Au4 and Tu3 or Tu12 Objects

- Step 1** Remove all cross-connections that are terminated in the au4, tu12, or tu3 termination points belonging to the aug1 object that you want to modify.
- Step 2** Set the tug3 Structure to **none** for all tug3 objects contained by the aug1 object that should be modified; see the “[5.2.2.1 Modify Between Tu12 and Tu3 Objects](#)” section on [page 5-3](#).
- Step 3** Follow the guidelines in the “[5.2.1 Configure ONS 15305 SDH Port Structure \(Channelization\)](#)” section on [page 5-2](#), to make au4, tu3, or tu12 termination points of an SDH port available for cross-connection.

**Note**

Modifying the structure means deleting existing termination points and creating new termination points (if the new structure is not “none”). To avoid unintentional traffic loss, the ONS 15305 will not allow modification of the structure before all cross-connections belonging to a structure object have been deleted.

**Note**

The structure of all contained tug3 objects must have been set to “none” before the aug1 can be modified.

## 5.2.3 Set and Read Path Trace Identifiers

Path Trace is available at two levels in an SDH port:

- RS path trace, terminated in the STM-N port on the opposite side of the link.
- VC-4 Path Trace, terminated in the SDH node terminating the VC-4 path.

### 5.2.3.1 Set or Read RS Path Trace Identifiers

- 
- Step 1** Select an sdh port.
- Step 2** When the sdh port managed object is expanded, click **rs**.
- Step 3** Click **PathTraceRS**.
- Step 4** The following attributes can be set:
- PathTrace  
Set to enable if TIM alarms should be reported when there is a mismatch between PathTraceReceived and PathTraceExpected.
  - PathTraceExpected  
Enter a value for the path trace identifier that you expect to receive from the other side of the path.
  - PathTraceTransmitted  
Enter a value for the path trace identifier that you want to transmit to the other side of the path.
- Step 5** The following attributes can be read:
- PathTraceReceived  
The actual received path trace identifier from the other side of the link.
- Step 6** Click **Save** on the toolbar.
-



### 5.2.3.2 Set or Read VC-4 Path Trace Identifiers


**Note**

VC4 path trace is available only when the SDH port is structured with a VC-4 object, which means the **aug1** Structure is **tug3x3**; see the [“5.2.1 Configure ONS 15305 SDH Port Structure \(Channelization\)” section on page 5-2](#).

- 
- Step 1** Select an **sdh** port.
- Step 2** Select the **rs** and then the **ms** managed objects as the port expands.
- Step 3** Select the **aug1** managed object that contains the **vc4** to measure.
- Step 4** Select the **au4** and then the **vc4** managed objects as the port expands.
- Step 5** Click **PathTraceVC4**.
- The attributes are the same as the RS path trace.
- Step 6** Click **Save** on the toolbar after setting the path trace parameters.


**Note**

When path trace is set to enabled, AIS is inserted downstream instead of the original signal when there is a mismatch between expected and received path trace.

## 5.2.4 Monitor SDH Port Performance

Performance monitoring is available at three levels in the SDH port:

- RS PM, monitoring near end of the regenerator section.
- MS PM, monitoring near and far end of the multiplexer section.
- VC-4 PM, monitoring near and far end of the VC-4 path.

### 5.2.4.1 Read RS PM Counters

- 
- Step 1** Select an **sdh** port.
- Step 2** When the **sdh** port managed object is expanded, select the **rs** managed object.
- Step 3** Click on the **vc12** (for e1 ports) **or** **vc3** (for e3 ports) managed object.
- Step 4** Click **PmG826NearEnd** to read near end PM data **or** **PmG826FarEnd** to read far end PM data.
- The following attributes are available:
- Current15Min ES,SES, BBE and UAS
  - Current24Hour ES, SES, BBE and UAS
- Step 5** To see the performance history of the previous 16x15 minute counters, click **Interval15Min** or click **Interval24Hour** to see the previous 24 hour counter.
- The following attributes are available:
- Interval15Min ES,SES, BBE and UAS

- Interval24Hour ES, SES, BBE and UAS

### 5.2.4.2 Read MS PM Counters

- 
- Step 1** Select an sdh port.
- Step 2** Select the **rs** and then the **ms** managed objects as the port expands.
- Step 3** Click **PmG826NearEnd** to read near end PM data or **PmG826FarEnd** to read far end PM data.  
The attributes are the same as for RS PM.
- 

### 5.2.4.3 Read VC-4 PM Counters

- 
- Step 1** Select an sdh port.
- Step 2** Select the **rs** and then the **ms** managed objects as the port expands.
- Step 3** Select the **aug1** managed object that contains the **vc4** to measure.
- Step 4** Select the **au4** and then the **vc4** managed objects as the port expands.
- Step 5** Click **PmG826NearEnd** to read near-end PM data or **PmG826FarEnd** to read far-end PM data.  
The attributes are the same as RS PM in the [“5.2.4.1 Read RS PM Counters”](#) section on page 5-5.
- 

## 5.2.5 Enable the SDH Port to Carry Traffic and Report Alarms

By default the Administrative Status of the SDH port is set to disabled when the port is created. No alarms are reported before it is enabled.

- 
- Step 1** Select an sdh port.
- Step 2** Set **AdminStatus** to **enabled**.
- Step 3** Click **Save** on the toolbar.



**Note**

If the administrative status is disabled, the following applies :

- No alarms are reported towards the port.
- PM counters for the port will only count 0.
- If the port is part of MSP , the port will not be selected for traffic (unless this is a working port and the protecting port also is disabled or has SPI/RS/MS alarm).

---

**Note**

Even if the SDH port is enabled it will only report alarms if the AlarmReporting attribute of the slot is set to enabled.

## 5.2.6 Set ONS 15305 SDH Port Synchronization Quality Output Signaling

STM-N signals are often used to carry synchronization information. A dedicated protocol is used to indicate the quality of the signal from one SDH node to the next SDH node.

- 
- Step 1** Select an sdh port.
- Step 2** Set **EgressSSM** to **t0** or **doNotUse**. T0 will always indicate the quality status of the internal clock.
- Step 3** Click **Save** on the toolbar.

**Note**

When an SDH port is used as a synchronization source candidate, the S1 byte will be set to do-not-use-automatically.

## 5.2.7 SDH Port as a Synchronization Source Input

See the [“4.4.4 Add Synchronization Source Candidate \(T0 or T4\)”](#) section on page 4-28.

## 5.2.8 DCC Channels on the SDH Port Carrying Management Traffic

See the [“4.1.2 DCC Configuration”](#) section on page 4-4.

## 5.3 PDH Ports

The ONS 15305 can be equipped with two different PDH port types:

- E1 Ports (2 Mbps) supporting transparent data and NT functionality of ISDN PRA. E1 Ports are available when the slot is configured for the 8xE1 module or the 6xE1 module.
- E3 Ports (34/45 Mbps) supporting transparent data. E3 Ports are available when the slot is configured for the 6xE3 module.

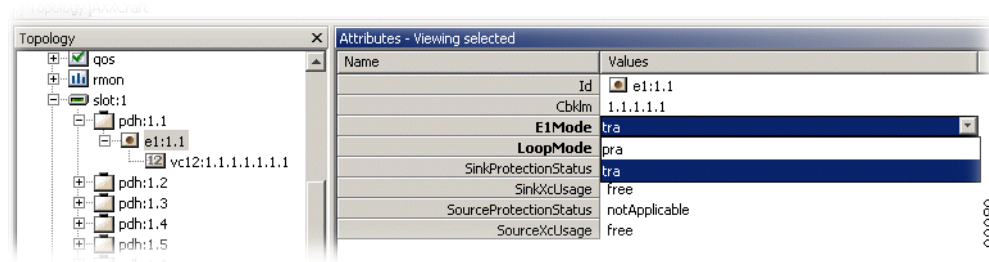
The ONS 15302 is equipped with E1 ports.

### 5.3.1 Set the Port Mode for ONS 15305

- 
- Step 1** Select a pdh port ([Figure 5-3](#)).

- Step 2** When the pdh port managed object is expanded, select the **e1** or **e3** managed object.
- Step 3** For e1 ports, set the E1Mode attribute to **tra** (2 Mbps transparent G.703) or **pra** (ISDN PRA).

**Figure 5-3 Set the E1 Mode Attribute**

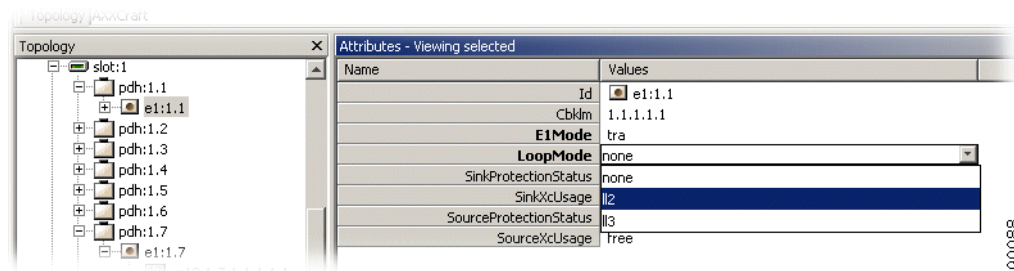


- Step 4** For e3 ports set the E3Mode attribute to **e3** (34 Mbps transparent G.703) or **t3** (45 Mbps) transparent G.703).
- Step 5** Click **Save** on the toolbar.

## 5.3.2 Set a Loop in a ONS 15305 PDH Port

- Step 1** Select a pdh port (Figure 5-4).
- Step 2** When the pdh port managed object is expanded, select the **e1** or **e3** managed object.
- Step 3** Set the loopMode attribute to **ll2** (loop back to network) or **ll3** (loop back to customer).

**Figure 5-4 Set Loop Mode Attributes**



- Step 4** Click **Save** on the toolbar.



**Note**

There are a number of restrictions for setting the loops of PDH ports. Cisco Edge Craft cannot set and release loops when the E1Mode is set to pra (in this mode loops can only be managed from an NT1 or similar). A loop cannot be set when the pdh port AdminStatus is set to disabled.

### 5.3.3 Set a Loop in a ONS 15302 PDH Port

- 
- Step 1** Select a pdh port.
  - Step 2** When the pdh port managed object is expanded, select the **e1** managed object.
  - Step 3** Set the loopMode attribute to **l12** (loop back to network) or **l13** (loop back to customer).
  - Step 4** Click **Save** on the toolbar.
- 

### 5.3.4 Release a Loop in a PDH Port

- 
- Step 1** Select a pdh port.
  - Step 2** When the pdh port managed object is expanded, select the **e1** or **e3** managed object.
  - Step 3** Set the loopMode attribute to **none**.
  - Step 4** Click **Save** on the toolbar.



---

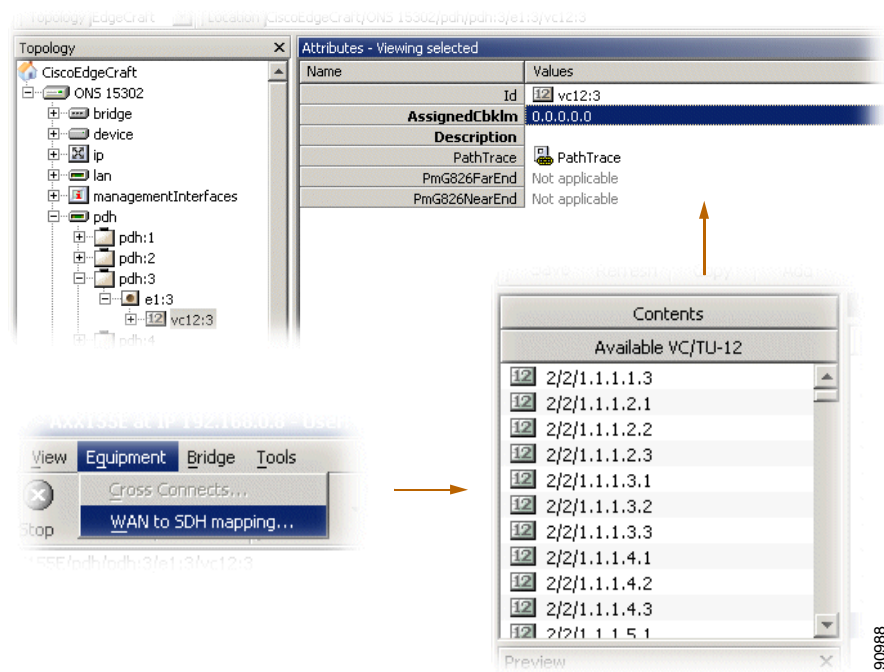
**Note** Any loop will be released if the pdh port AdminStatus is changed from enabled to disabled.

---

### 5.3.5 Assign VC12s in the ONS 15302

- 
- Step 1** Expand desired PDH port in the topology browser. To view VC12 managed object attributes, see [Figure 5-5](#).
  - Step 2** Change **AssignedCbklm** ([Figure 5-5](#)).  
You may use the WAN to SDH mapping window to view available VC12s with cbklm values.
  - Step 3** Click **Save**.

Figure 5-5 Assign VC 12 Port



### 5.3.6 Set and Read Path Trace Identifiers

- Step 1** Select a pdh port.
- Step 2** When the pdh port managed object is expanded, click on the **e1** or **e3** managed object.
- Step 3** Click on the **vc12** (E1) or **vc3** (E3) managed object.
- Step 4** Click on **PathTraceVC12**.  
The following attributes can be set:
  - **PathTrace**  
Set to enable if TIM alarms should be reported when there is a mismatch between PathTraceReceived and PathTraceExpected.
  - **PathTraceExpected**  
Enter a value for the path trace identifier that you expect to receive from the other side of the path.
  - **PathTraceTransmitted**  
Enter a value for the path trace identifier that you want to transmit to the other side of the path.
- Step 5** The Path Trace Received attribute can be read. It is the actual received path trace identifier from the other side of the link.
- Step 6** Click **Save** on the toolbar.

**Note**

When path trace is set to enabled, AIS is inserted downstream instead of the original signal when there is a mismatch between expected and received path trace.

## 5.3.7 Monitor PDH Port Performance

- Step 1** Select a pdh port.
- Step 2** When the pdh port managed object is expanded, select the **e1** or **e3** managed object.
- Step 3** Click on the **vc12** (for e1 ports) or **vc3** (for e3 ports) managed object.
- Step 4** Click on **PmG826NearEnd** to read near end PM data or **PmG826FarEnd** to read far end PM data.

The following attributes are available:

- Current15Min ES, SES, BBE and UAS
- Current24Hour ES, SES, BBE and UAS

- Step 5** To see the Performance history of the previous 16x15 minute counters click **Interval15Min**, or click **Interval24Hour** to see the previous 24 hour counter (Figure 5-6 and Figure 5-7).

The following attributes are available

- Interval15Min ES, SES, BBE and UAS
- Interval24Hour ES, SES, BBE and UAS

**Figure 5-6 Select Interval24Hour**

Name	Values
Id	pmG826NearEnd.vc12:1.3.1.1.1.1
Current15MinBBE	0
Current15MinES	0
Current15MinSES	0
Current15MinStartTime	2002/12/02 08:15:00
Current15MinTimeElapsed	00:20
Current15MinUAS	0
Current24HourBBE	0
Current24HourES	0
Current24HourSES	0
Current24HourStartTime	2002/12/02 00:00:00
Current24HourTimeElapsed	08:15:19
Current24HourUAS	0
Interval15Min	<a href="#">Interval15Min</a>
Interval24Hour	<a href="#">Interval24HourNearEndVC12</a>

**Figure 5-7 Set Interval24Hour Attributes**

Name	Values
Id	interval24Hour.pmG826NearEnd.vc12:1.3.1.1.1.1.1
BBE	0
ES	0
EndTime	2002/12/02 00:00:00
SES	0
Status	valid
UAS	0

### 5.3.8 Enable the PDH Port to Carry Traffic and Report Alarms

By default the administrative status of the PDH port is set to disabled when the port is created. No traffic will pass through the port and no alarms are reported before it is enabled.

- 
- Step 1** Select a pdh port.
- Step 2** Set AdminStatus to **enabled**.
- Step 3** Click **Save** on the toolbar.



**Note** When disabled the PDH port generates AIS upstream and downstream.

---

### 5.3.9 Cross-Connect the ONS 15305 PDH Port to Another Port

See [“5.7 ONS 15305 SDH Layer Network and Cross-Connections”](#) section on page 5-33.

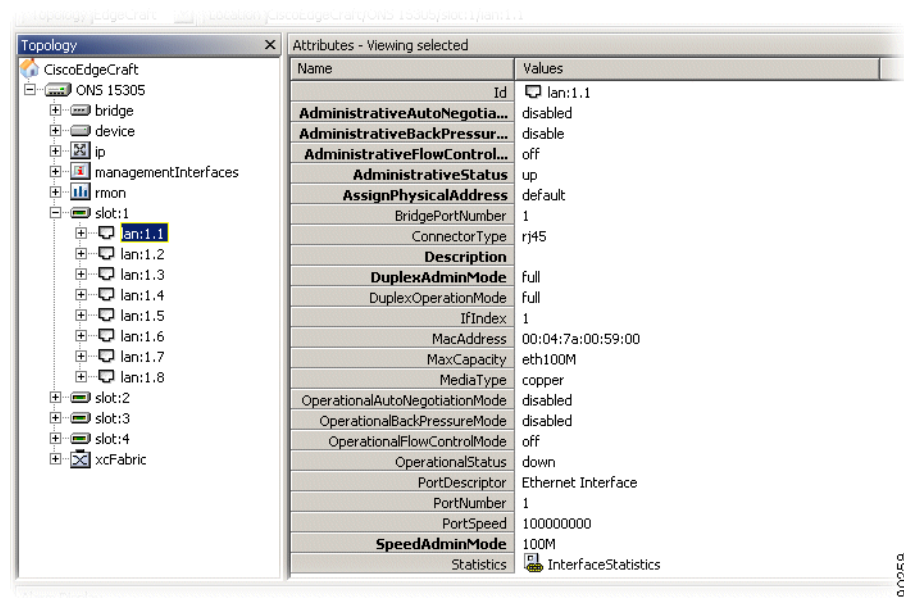
## 5.4 LAN Ports

### 5.4.1 ONS 15305 - LAN Port Attributes

An ONS 15305 slot can be configured to carry an 8xFeRj45 module. See the [“4.8 Manage ONS 15305 Slots”](#) section on page 4-46 for details.

- 
- Step 1** When the module is installed, click a LAN port to view modifiable attributes ([Figure 5-8](#)). Attributes marked as bold are modifiable.



**Figure 5-8 LAN Port Attributes**

**Step 2** Modify the following attributes as needed:

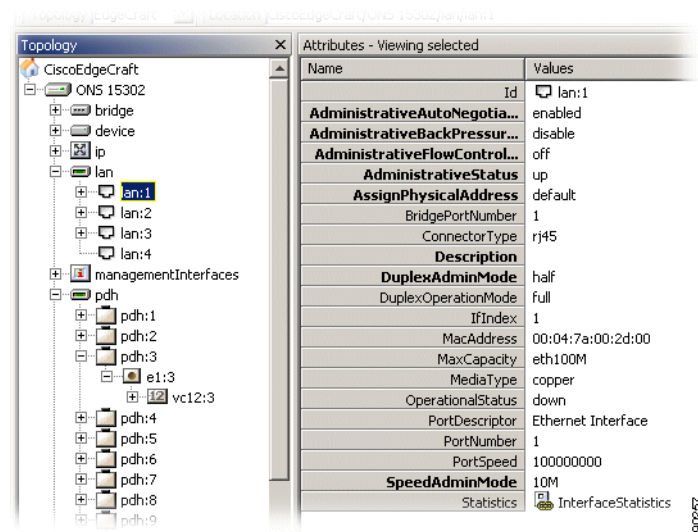
- AdministrativeAutoNegotiationMode  
disabled or enabled
- AdministrativeBackPressureMode  
disabled or enabled
- AdministrativeFlowControlMode  
on, off or auto negotiation
- AdministrativeStatus  
up, down or testing
- AssignPhysicalAddress  
reserve or default
- Description  
string
- DuplexAdminMode  
none, half or full
- SpeedAdmin mode  
not set, 10M, 100M or 1000M

**Step 3** Click **Save**.

## 5.4.2 ONS 15302 LAN Port Attributes

The ONS 15302 is equipped with 4 LAN ports (Figure 5-9). For configuration of LAN ports see the “5.4.1 ONS 15305 - LAN Port Attributes” section on page 5-12.

**Figure 5-9 LAN Port Attributes - ONS 15302**



## 5.5 WAN Ports - ONS 15305

The ONS 15305 can concentrate IP traffic over the SDH network. The purpose of this section is to describe the tasks involved in assigning capacity from the SDH server layer to WAN ports. The total assigned WAN capacity is made up of SDH channels.

Each SDH channel is equivalent to a VC-12 (2 Mbps). This is available in the first release of the network element. Future releases will also include mapping to VC-3 and VC-4. This section only describes the VC-12/TU-12 layer rate.

The SDH channels can be from different SDH ports.

The WAN channels can be sub-network connection (SNC) protected. In the first release of the ONS 15305, only protection scheme SNC/I (inherent monitoring) is supported.

### 5.5.1 WAN Ports and Mapping

The eight WAN ports are located on the 8xSTM-1 module. They are connected to a Galileo switch (Figure 5-10). A WAN port has a maximum capacity of 100 Mbps.

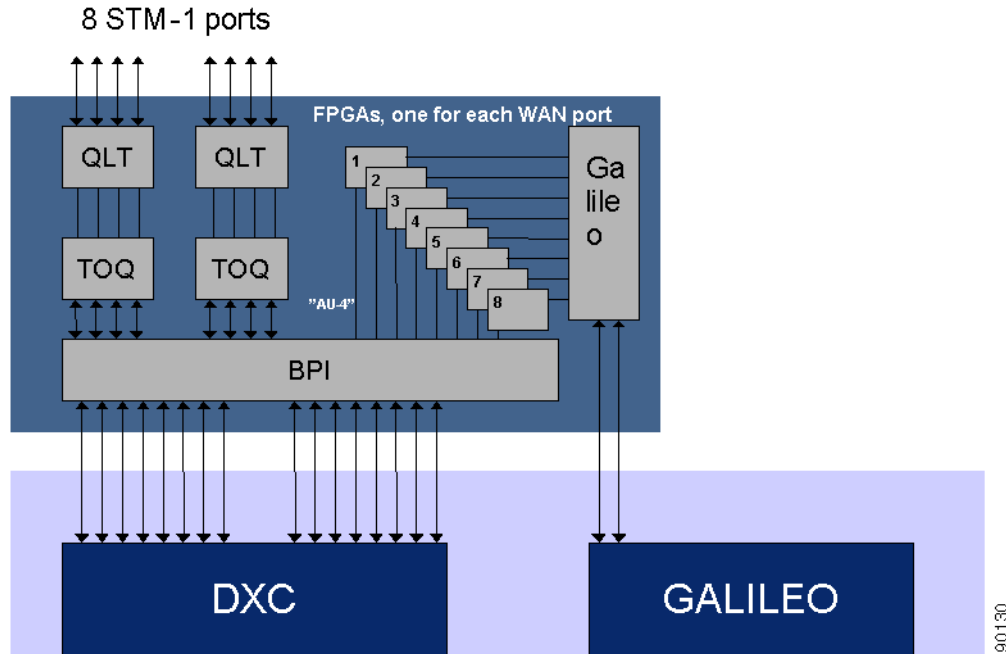
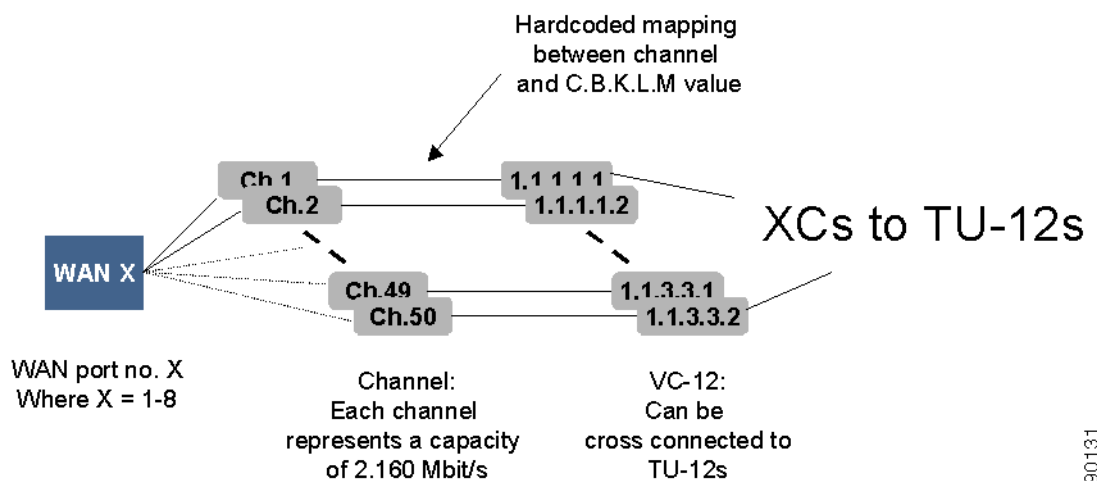
**Figure 5-10 The 8 x STM-1 Module with WAN Ports**

Figure 5-11 shows that the potential capacity of 100 Mbps is realized through 50 channels, each of which can carry 2.160 Mbps. The capacity of the WAN port is therefore decided by how many channels are used for traffic.

A WAN port can be mapped to one STM-1 port, which means there are potentially 63 available VC-12s. Only the first 50 of these are used. These 50 channels have hard-coded mapping to 50 VC-12 containers. The C.B.K.L.M numbering is described in the “5.7.1.1 C.B.K.L.M Value Usage” section on page 5-35.

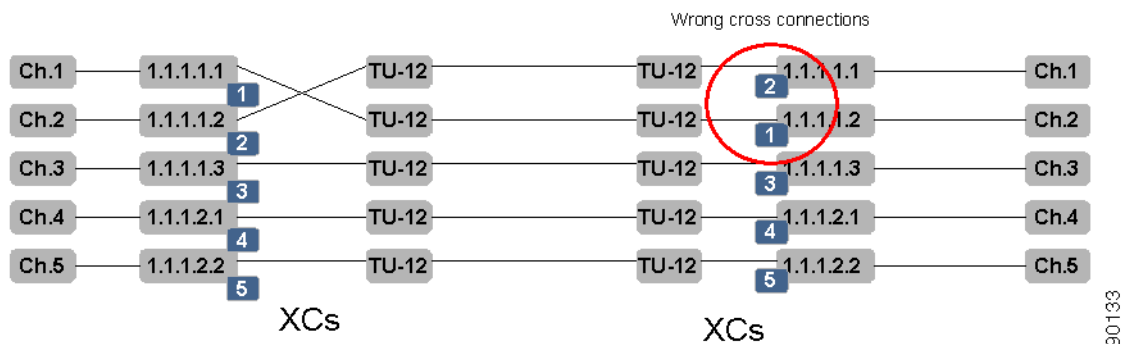
**Figure 5-11 View of one WAN Port and its Logical View**

The WAN VC-12s are cross connected to the available TU-12s on the SDH ports. All 50 WAN VC-12s are available for cross connection. A WAN VC-12 represents the termination point A in a cross connection and the connection is always bidirectional. The cross connection can be protected.

If there exists a VC-12 (or channel) inside the WAN capacity that is not cross connected, the network element issues an unequipped alarm on the WAN VC-12.

The order of the channels is essential and must be the same on both sides of a WAN connection, for example, containers sent from channel 1 must be received on channel 1. A sequence number is used to indicate the correct order of the VC-12 on the receiving side of a WAN connection between two ONS 15305 network elements. If the connection is not between two ONS 15305 NEs, the sequence number will be zero. Figure 5-12 shows a scenario where the cross connection between two TU-12s and two VC-12s in one ONS 15305 are incorrect.

**Figure 5-12 Sequence Numbers for Correct Order of TU-12 to VC-12 Cross Connects.**



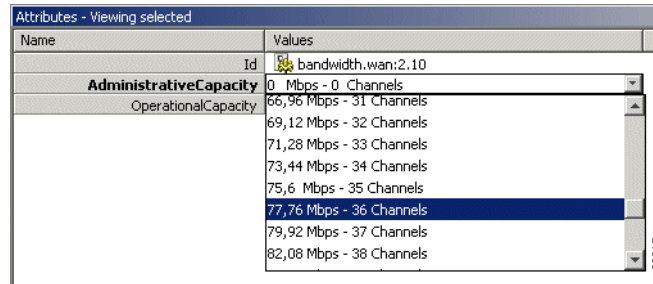
Alarm and performance monitoring data is collected and reported for those VC-12s that are within the WAN capacity.

## 5.5.2 Add Initial WAN Port Capacity

The addition of WAN port capacity is performed in a two step process.

The first step is to set the administrative capacity of the WAN port. This will tell ONS 15305 how many of the 50 possible WAN channels to use for mapping into the SDH server layer.

- 
- Step 1** Select a WAN port.
  - Step 2** When the WAN port managed object is expanded, select **Bandwidth**.

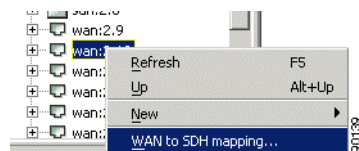
**Figure 5-13 Set Bandwidth**

**Step 3** Set the Bandwidth to a value between 0 and 100 Mbps (Figure 5-13).

**Step 4** Click **Save** on the toolbar.

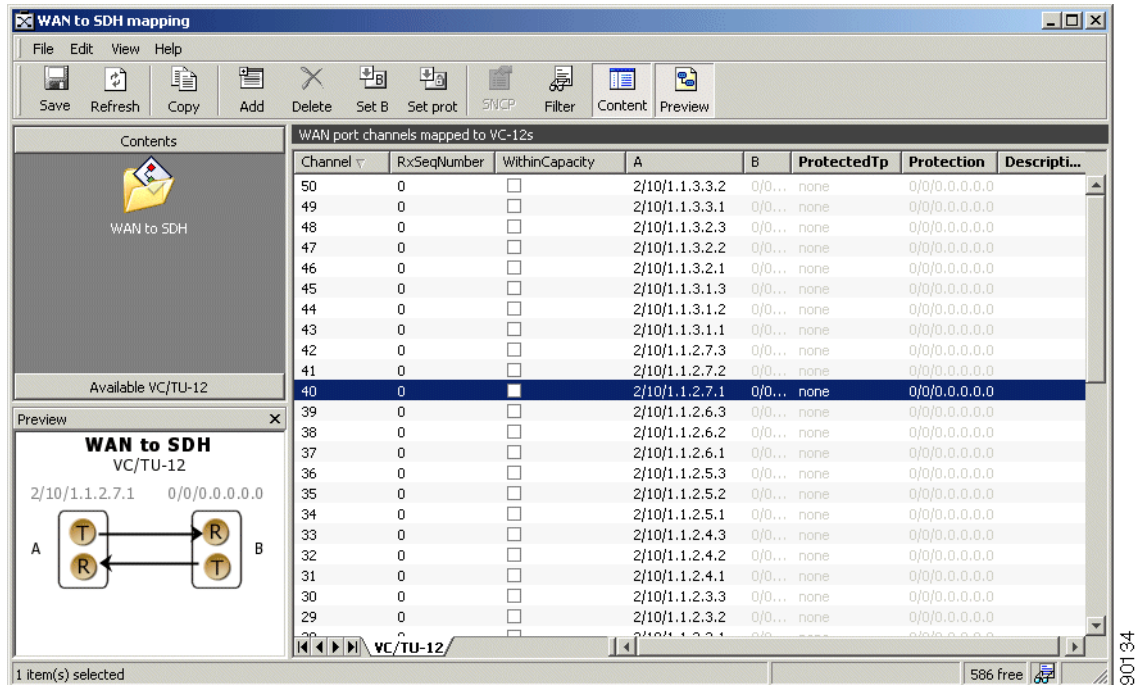
The next step is to cross-connect the WAN channels that are in use after setting the administrative capacity.

**Step 5** Right click the WAN port and select **WAN to SDH mapping** (Figure 5-14).

**Figure 5-14 Select WAN Port Attributes**

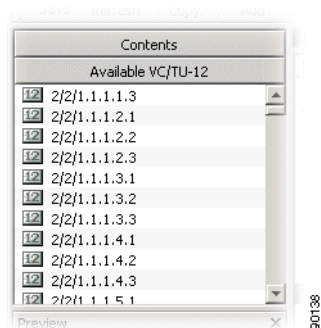
A list of all the WAN channels of the WAN port is shown. The list shows the static relation between each channel number and a VC12 object in the WAN port. The WithinCapacity attribute indicates if the channel is in use by the WAN channel (that means if it was included when setting administrative capacity above).

Figure 5-15 Set WAN Port Attributes



- Step 6** Make sure the Content panel is available in the left part of the window (Figure 5-15).  
If it is not available select the **Content** button in the toolbar.
- Step 7** Select the Available VC/TU12 List in the content panel. SHIFT and CTRL buttons can be used for multiple selection. The list contains the free TU12 termination points in ONS 15305 (Figure 5-16).

Figure 5-16 Select Available VC/TU12

**Note**

If the Available VC or TU12 List in the content panel does not show the TU12 termination points that you want to map your WAN port to, you have to make sure they are made available for cross-connection; see the [“5.2.1 Configure ONS 15305 SDH Port Structure \(Channelization\)”](#) section on page 5-2.

- Step 8** Double-click the TU12 termination point that you want to use to map to WAN channel number 1. The selected TU12 is inserted as the B termination Point for channel 1.

- Step 9** Double-click the termination point that you want to use to map to WAN channel number 2.
- Step 10** Repeat until all channels that are within capacity have a B termination point.
- Step 11** Click **Save** on the toolbar.



**Note** Remember to perform the same operation on the WAN port on the other side of the SDH network and adding cross-connections in intermediate nodes. The WAN channel will only work if it is connected to the WAN channel with the same channel number on the opposite end of the SDH network.



**Note** The WAN port will not report alarms on channels that are not part of the administrative capacity.

## 5.5.3 Modify WAN Port Capacity

You can modify the WAN port capacity in the same way you added the initial WAN capacity; see the [“5.5.2 Add Initial WAN Port Capacity” section on page 5-16](#).

- Step 1** Select a WAN port.
- Step 2** When the WAN port managed object is expanded, select **Bandwidth**.
- Step 3** Set the Bandwidth to a new value between 0 and 100 Mbps.
- Step 4** Click **Save** on the toolbar.
- Step 5** Select the WAN port again, right click and select **WAN to SDH mapping**.
- A list of all the WAN channels of the WAN port appears. The list shows the static relation between each channel number and a VC12 object in the WAN port. The WithinCapacity attribute indicates if the channel is in use by the WAN channel (that means if it was included when setting administrative capacity above).
- Step 6** If you increased the administrative capacity using the [“5.5.2 Add Initial WAN Port Capacity” section on page 5-16](#), more channels have the WithinCapacity attribute set and they need a B termination point to be mapped to the SDH server layer.
- Step 7** If you decreased the administrative capacity using the [“5.5.2 Add Initial WAN Port Capacity” section on page 5-16](#), fewer channels have the WithinCapacity attribute set and the B termination points can be released for other purposes.

### 5.5.3.1 Increase Capacity in the SDH Server Layer

Make sure the content panel is available in the left part of the window. If it is not available select the content button in the toolbar.

- Step 1** Select the Available VC or TU12 List in the content panel. The list contains the free TU12 termination points in the ONS 15305.

**Note**

If the available VC or TU12 list in the content panel does not show the TU12 termination points that you want to map your WAN port to, you have to make sure they are made available for cross-connection using the [“5.2.1 Configure ONS 15305 SDH Port Structure \(Channelization\)” section on page 5-2](#).

- Step 2** Double-click the TU12 termination point that you want to use to map to your first new WAN channel. The selected TU12 is inserted as the B termination Point for this channel.
- Step 3** Double-click the termination point that you want to use to map to your next new WAN channel.
- Step 4** Continue until all new channels that are within capacity have a B termination point.
- Step 5** Click **Save** on the toolbar.
- Step 6** Remember to perform the same operation on the WAN port on the other side of the SDH network and add cross-connections in intermediate SDH nodes.

### 5.5.3.2 Decrease Capacity in the SDH Server Layer

- Step 1** Select the WAN channels that are no longer used by the WAN port mapping (channels with B termination points, but not WithinCapacity). Multiple selection is possible with Shift or Ctrl buttons ([Figure 5-17](#)).
- Step 2** Click **Delete** on the toolbar. The selected channels becomes red.

**Figure 5-17 Select WAN Channels**

WAN port channels mapped to VC-12s

Channel ▾	RxSeqNumber	WithinCapacity	A	B	ProtectedTp	Protection	Desc
50	0	<input type="checkbox"/>	2/10/1.1.3.3.2	2/2...	none	0/0/0.0.0.0.0	
49	0	<input type="checkbox"/>	2/10/1.1.3.3.1	0/0...	none	0/0/0.0.0.0.0	
48	0	<input type="checkbox"/>	2/10/1.1.3.2.3	2/2...	none	0/0/0.0.0.0.0	
47	0	<input type="checkbox"/>	2/10/1.1.3.2.2	0/0...	none	0/0/0.0.0.0.0	
46	0	<input type="checkbox"/>	2/10/1.1.3.2.1	0/0...	none	0/0/0.0.0.0.0	

- Step 3** Click **Save** on toolbar. The SDH TU12 termination points are released from WAN port mapping.
- Step 4** Remember to perform the same operation on the WAN port on the other side of the SDH network and deleting cross-connections in intermediate SDH nodes.

**Note**

It is not possible to modify the B termination point after it has been saved. If you want to modify the B termination point the channel must first be deleted, and then a new termination point can be added.

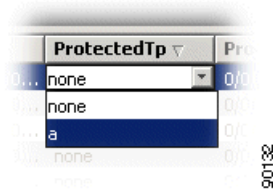
## 5.5.4 Protect a WAN Port

WAN ports can be protected by the SNC protection scheme in the VC12 or TU12 SDH layer, meaning that the WAN channels (not necessarily all WAN channels of a WAN port) can have two different routes through the SDH server network and that the receiving WAN channel selects the route with the best signal.



- Step 1** Add initial WAN port capacity as described in the [“5.5.2 Add Initial WAN Port Capacity”](#) section on page 5-16.
- Step 2** Set the ProtectedTP attribute to **a** for the WAN channels you want to protect (Figure 5-18).

**Figure 5-18 Select Protected Mode**



- Step 3** Select the first WAN channel you want to protect.
- Step 4** Make sure the content panel is available in the left part of the window. If it is not available select the content button in the toolbar.
- Step 5** Select the available VC or TU12 list in the content panel. The list contains the free TU12 termination points in ONS 15305.



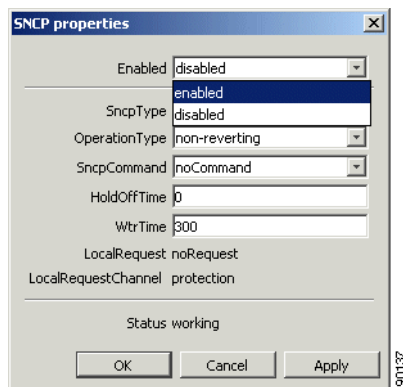
**Note** If the available VC or TU12 list in the content panel does not show the TU12 termination points that you want to protect your WAN channel with, you have to make sure they are made available for cross-connection, [“5.2.1 Configure ONS 15305 SDH Port Structure \(Channelization\)”](#) section on page 5-2.

- Step 6** Select the TU12 termination point that will protect your WAN channel.
- Step 7** Click the **Set Prot** button in the toolbar. The protection TP is filled in for the selected WAN channels.
- Step 8** Select the next WAN channel to protect and insert the protection TU12. Continue until all WAN channels are protected (channels that have the Protected TP attribute set to a).
- Step 9** Click **Save** on toolbar. Remember to perform the same operation on the WAN port on the other side of the SDH network and add cross-connections in intermediate nodes.



**Note** By default the protection is disabled and will not work before it is enabled.

- Step 10** Select the WAN channels where you want to enable protection (Shift and Ctrl buttons can be used for multiple selection).
- Step 11** Click the **SNCP** button in the toolbar (Figure 5-19).
- Step 12** Set the Enabled attribute to **enabled** and click **OK**.

**Figure 5-19 Set SNCP Properties Enabled**

- Step 13** Click **Save** on toolbar. Remember to perform the same operation on the WAN port on the other side of the SDH network. (However SNC protection is not bidirectional and does not have to be enabled in both ends simultaneously for the SNC protection scheme to work on the side that is enabled).

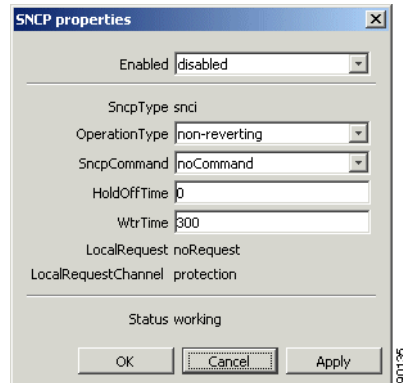
**Note**

It is not possible to modify the protection termination point after it has been saved. If you want to modify the protection termination point the ProtectedTP must first be saved as none. Then the protection TP can be modified. Remember to set the ProtectedTP back to a.

## 5.5.5 Modify Protection Parameters on the WAN Port

WAN ports are protected as described in the “[5.5.4 Protect a WAN Port](#)” section on page 5-20. The SNC is then set up with default parameters. The parameters can easily be modified ([Figure 5-20](#)).

- Step 1** Select a WAN port.
- Step 2** Right-click and select **WAN to SDH mapping**.
- Step 3** Select the WAN channels where you want to modify protection parameters (The Shift and Ctrl buttons can be used for multiple selection).
- Step 4** Click the **SNCP** button in the toolbar.
- Step 5** Modify the SNC protection parameters and click **OK**.

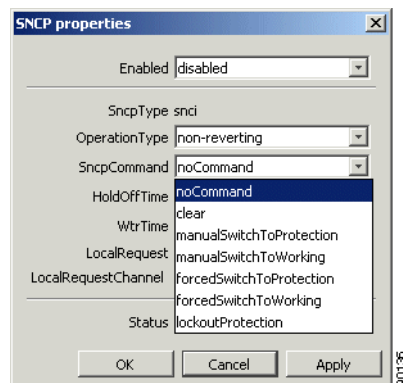
**Figure 5-20 Set SNCP Properties Protection**

**Step 6** Click **Save** on toolbar.

## 5.5.6 Command a WAN Port Protection Switch

The Cisco Edge Craft user can control the SNC protection switch by sending a command (Figure 5-21).

- Step 1** Select a WAN port.
- Step 2** Right-click and select **WAN to SDH mapping**.
- Step 3** Select the WAN channels where you want to modify protection parameters (The Shift and Ctrl buttons can be used for multiple selection).
- Step 4** Click the **SNCP** button in the toolbar.
- Step 5** Select the **SncpCommand** and click **OK**.

**Figure 5-21 Set SNCP Properties Command**

- Step 6** Click **Save** on toolbar. Depending on the priority of the command and current status of each channel, a switch may now take place for some or all selected WAN channels.

## 5.5.7 Set Path Trace Identifiers for a WAN Port

Path Trace parameters can be set for each channel (VC12) in the WAN port.

- 
- Step 1** Select a WAN port.
- Step 2** Click on the **PathTraceWAN** parameter group.
- Step 3** The following attributes can be set collective for all channels of the WAN port:
- **PathTrace**  
Set to enable if TIM alarms should be reported for the WAN port when there is a mismatch between PathTraceReceived and PathTraceExpected.
  - **PathTraceExpected**  
Enter a value for the path trace identifier that you expect to receive from the other side of the WAN channels.
  - **PathTraceTransmitted**  
Enter a value for the path trace identifier that you want to transmit to the other side of the WAN channels.
- Step 4** Click **Save** on toolbar.



**Note** When path trace is set to enabled, AIS is inserted downstream instead of the original signal when there is a mismatch between expected and received path trace.

---

## 5.5.8 Read Path Trace Identifiers for a WAN Port

Path trace parameters can be read for each channel (VC12) in the WAN port.

- 
- Step 1** Select a WAN port.
- Step 2** When the WAN port managed object is expanded, click on the **channel (vc12)** where you want to see the Received Path Trace.
- Step 3** Click on **PathTraceVC12**
- The following attributes can be read:
- **PathTrace**  
Set to enable if TIM alarms should be reported when there is a mismatch between PathTraceReceived and PathTraceExpected.
  - **PathTraceExpected**  
Enter a value for the path trace identifier that you expect to receive from the other side of the path.
  - **PathTraceTransmitted**  
Enter a value for the path trace identifier that you want to transmit to the other side of the path.
  - **PathTraceReceived**  
The actual received path trace identifier from the other side of the link.

**Note**

When path trace is set to enabled, AIS is inserted downstream instead of the original signal when there is a mismatch between expected and received PathTrace.

## 5.5.9 Monitor WAN Port Performance

- 
- Step 1** Select a WAN port.
- Step 2** When the WAN port managed object is expanded, click the **channel (vc12)** where you want to see the Performance data.
- Step 3** Click **PmG826NearEndVc12** to read near-end PM data or **PmG826FarEndVC12** to read far-end PM data.
- The following attributes are available:
- Current15Min ES,SES, BBE and UAS
  - Current24Hour ES, SES, BBE and UAS
- Step 4** To see the Performance history of the previous 16x15 minute counters click on **Interval15Min**, or click on **Interval24Hour** to see the previous 24 hour counter.
- The following attributes are available:
- Interval15Min ES, SES, BBE and UAS
  - Interval24Hour ES, SES, BBE and UAS
- 

## 5.5.10 Advanced WAN Port Operations

For frequent users of Cisco Edge Craft, it is possible to make use of the enhanced editing facilities to speed up the configuration work.

### 5.5.10.1 Select and Insert Multiple Termination Points

- 
- Step 1** Select the channels where you want to add termination points as B-end or Protection. Use Shift or Ctrl buttons to select more than one channel, or simply drag the mouse down the list while pressing the left mouse button.
- Step 2** Select the TU-12 termination points that you want to add to the B-ends of the channels in the same way.
- Step 3** Click the **Set B** button in the toolbar.
- Step 4** Select the TU-12 termination points that you want to add to the Protection TPs of the channels.
- Step 5** Click the **Set Prot** button in the toolbar.
- Step 6** Click **Save** on the toolbar.

**Note**

You are only allowed to set the B or protection termination points of channels where B or P are not in use.

If you want to modify the B termination point the relation with the existing B termination point must first be deleted. Then a new termination point can be added.

If you want to modify the protection termination point the ProtectedTP must first be saved as none. Then the protection TP can be modified. Remember to set the ProtectedTP back to a.

**Note**

If you do not select the same number of instances of WAN channels and termination points, the channels will be filled in with as many TPs as available, starting from the top of the selected channel list. If more TPs are selected than channels, the last TPs will not be used.

### 5.5.10.2 Manually Enter Termination Points

- Step 1** Select an unconfigured WAN channel.
- Step 2** Click the **B termination point**. A list of slots appears.
- Step 3** Select a slot. A list of ports appears.
- Step 4** Select a port.
- Step 5** Continue selecting each of the CBKLM values.
- Step 6** Enter the Protection termination point the same way if used (and set **ProtectedTP** to a).
- Step 7** Click **Save** on the toolbar.

**Note**

The information can also be entered directly without selecting the numbers from the drop-down menu. Remember to use the following format: <slot/port/C.B.K.L.M>

## 5.6 WAN Ports - ONS 15302

The ONS 15302 can concentrate IP traffic over the SDH network. This section describes the tasks involved in assigning capacity from the SDH server layer to WAN ports.

Each SDH channel is equivalent to a VC-12 (2.160 Mbps). The ONS 15302 has one or four WAN ports depending on the hardware configuration.

### 5.6.1 WAN ports and the Mapping

The network element has one or four WAN ports. A WAN port has a maximum capacity of 100 Mbps.

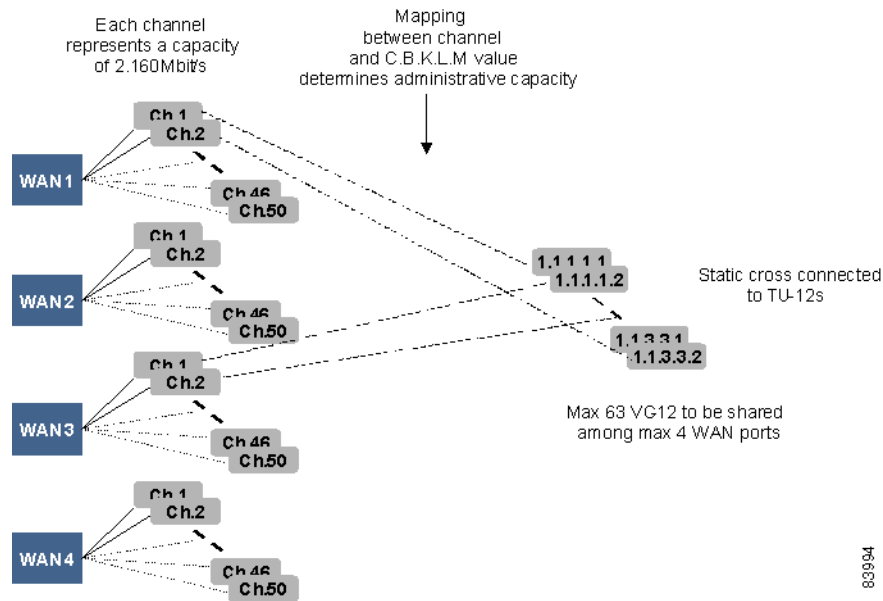
The WAN ports are logical ports and not physical ports. The potential capacity of 100 Mbps is realized and guaranteed through 47-50 VC12s, each of which can carry 2.160 Mbps. The overhead (extra bits) are used to handle escaped characters. The capacity of the WAN port is therefore decided by how many VC12s that are assigned to the port.

The ONS 15302 has one STM-1 port and potentially 63 VC12s are available for a WAN port. Each WAN port has 50 channels that are dynamically mapped to VC12s.

The VC-12s have static cross connections to the available TU-12s on the SDH ports.

The order of the 0-50 channels are essential and must be the same on both sides of a WAN connection, for example containers sent from channel 1 must be received on channel 1 (Figure 5-22).

**Figure 5-22 View of the WAN Ports and their Logical View**



Alarm and performance monitoring data is collected and reported for the VC-12s.

## 5.6.2 Differences Between the ONS 15305 and ONS 15302

In ONS 15305 each WAN port has always a potential capacity of 100 Mbps realized through 50 channels. The available capacity is not dependent on the capacity used by the other WAN ports. When you set the capacity, the system selects the first X channels corresponding to this capacity. The channels have a static mapping to VC-12s. You must cross connect the VC-12s to TU-12s to activate the capacity.

In the ONS 15302 each WAN port also has a potential capacity of 100 Mbps, but the available capacity is dependent on the capacity used by the other WAN ports. You set and activate the capacity indirectly by selecting a set of channels and map them to VC-12s. The VC-12s are statically cross connected to TU-12s.

## 5.6.3 Add Initial WAN Port Capacity

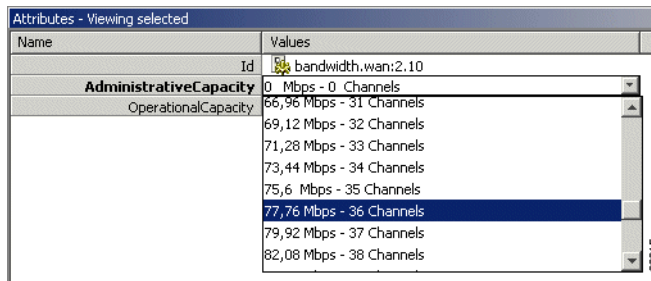
The addition of WAN port capacity is performed in a two-step process.

### 5.6.3.1 Set the Administrative Capacity (Optional)

The first step is to set the administrative capacity of the WAN port. This will tell the ONS 15302 how many of the 50 possible WAN channels to use for mapping into the SDH server layer ([Figure 5-23](#)).

- Step 1** Select a WAN port.
- Step 2** When the WAN port managed object is expanded, select **Bandwidth**.

**Figure 5-23 Set Bandwidth**



- Step 3** Set the Bandwidth to a value between 0 and 100 Mbps.



**Note**

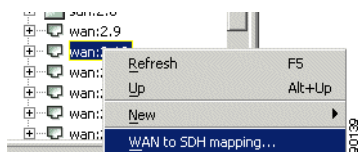
If you choose to set the administrative capacity to a desired number of channels and during the WAN to SDH mapping increases the number of channels, the administrative capacity reflects the preset value and not the actual number of channels mapped. When Cisco Edge Craft is restarted, administrative capacity will display actual channel number currently mapped.

- Step 4** Click **Save** on the toolbar.

### 5.6.3.2 Cross-Connect the WAN Channels

- Step 1** Select the WAN port again, right click and select **WAN to SDH mapping** ([Figure 5-24](#)).
- Step 2** A list of all the WAN channels of the WAN port is shown. The list shows the static relation between each channel number and a VC12 object in the WAN port.

**Figure 5-24 Select a WAN port**

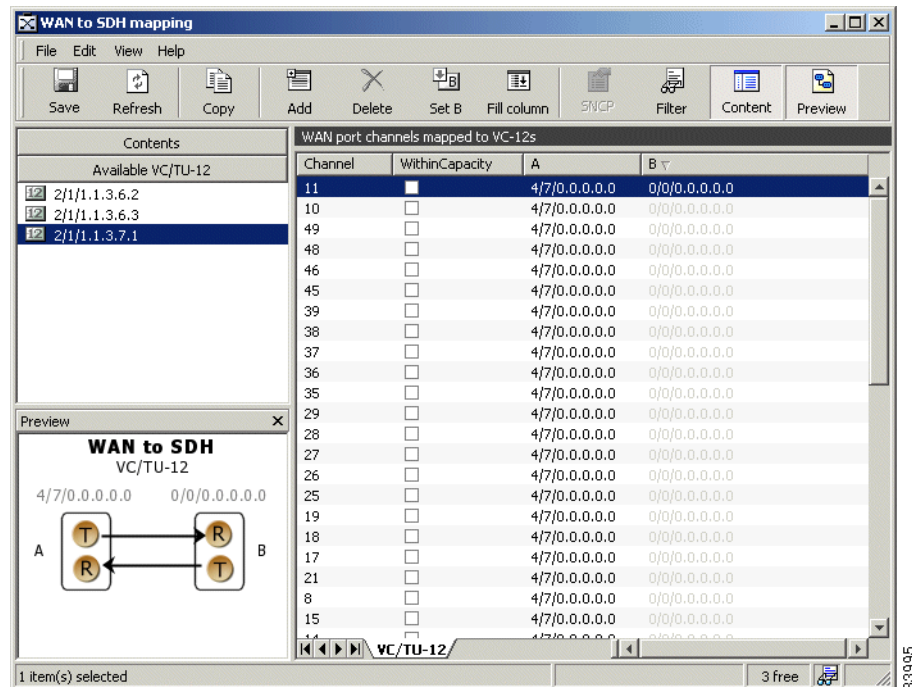


If the Administrative Capacity is set, the WithinCapacity attribute indicates if the channel is in within the desired capacity ([Figure 5-25](#)).

If the Administrative Capacity is not set, the WithinCapacity attribute indicates the channels mapped.



Figure 5-25 Set WAN Attributes

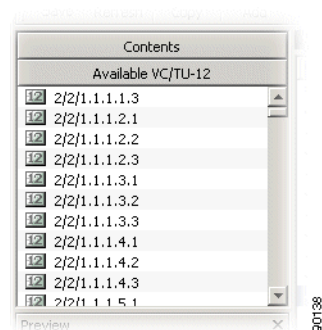


**Step 3** Make sure the Content panel is available in the left part of the window.

If it is not available select the Content button in the toolbar.

**Step 4** Select the available VC or TU12 List in the content panel. The list contains the free TU12 termination points in ONS 15305 (Figure 5-26).

Figure 5-26 Select Available VC/TU12 Container



**Step 5** Double-click the TU12 termination point that you want to use to map to your WAN channel number 1. The selected TU12 is inserted as the B termination Point for channel 1.

**Step 6** Double-click the termination point that you want to use to map to your WAN channel number 2.

**Step 7** If AdministrativeCapacity is set, repeat until all channels that are within capacity has a B termination point.

**Step 8** Click **Save** on the toolbar.

**Note**

Remember to perform the same operation on the WAN port on the other side of the SDH network and adding cross-connections in intermediate nodes. The WAN channel will only work if it is connected to the WAN channel with the same channel number on the opposite end of the SDH network.

**Note**

The WAN port will not report alarms on channels that are not part of the administrative capacity.

## 5.6.4 Increase Capacity in the SDH Server Layer

Make sure the content panel is available in the left part of the window. If it is not available select the content button in the toolbar.

- Step 1** Select the available VC or TU12 List in the content panel. The list contains the free TU12 termination points in the ONS 15302.
- Step 2** Double-click the TU12 termination point that you want to use to map to your first available WAN channel. The selected TU12 is inserted as the B termination point for this channel.

**Note**

For the ONS 15302, mapping must be performed in a continuous range.

- Step 3** Double-click the termination point that you want to use to map.
- Step 4** If AdministrativeCapacity is set, continue until all channels that are within capacity have a B termination point.
- Step 5** Click **Save** on the toolbar.
- Step 6** Remember to perform the same operation on the WAN port on the other side of the SDH network and add cross-connections in intermediate SDH nodes.

## 5.6.5 Decrease Capacity in the SDH Server Layer

- Step 1** Select the WAN channels that are no longer used by the WAN port mapping (channels with B termination points but not WithinCapacity). Multiple selection is possible with Shift or Ctrl buttons.

**Note**

For the ONS 15302, mapping must be deleted in a continuous range.

- Step 2** Click **Delete** on the toolbar. The selected channels becomes red ([Figure 5-27](#)).

**Figure 5-27 Delete WAN Port**

WAN port channels mapped to VC12s

Channel	RxSeqNumber	WithinCapacity	A	B	ProtectedTp	Protection	Description
50	0	<input type="checkbox"/>	2/10/1.1.3.3.2	2/2...	none	0/0/0.0.0.0	
49	0	<input type="checkbox"/>	2/10/1.1.3.3.1	0/0...	none	0/0/0.0.0.0	
48	0	<input type="checkbox"/>	2/10/1.1.3.2.3	2/2...	none	0/0/0.0.0.0	
47	0	<input type="checkbox"/>	2/10/1.1.3.2.2	0/0...	none	0/0/0.0.0.0	
46	0	<input type="checkbox"/>	2/10/1.1.3.2.1	0/0...	none	0/0/0.0.0.0	

- Step 3** Click **Save** on the toolbar. The SDH TU12 termination points are released from WAN port mapping.
- Step 4** Remember to perform the same operation on the WAN port on the other side of the SDH network and delete cross-connections in intermediate SDH nodes.

**Note**

It is not possible to modify the B termination point after it has been saved. If you want to modify the B termination point the mapping must first be deleted, and then a new termination point can be added.

## 5.6.6 Set Path Trace Identifiers for a WAN Port

Path trace parameters can be read for each channel (VC12) in the WAN port.

- Step 1** Select a WAN port.
- Step 2** Click the **PathTraceWAN** parameter group
- Step 3** As needed, edit the following attributes for any channel on the WAN port:
- PathTrace  
Set to enable if TIM alarms should be reported for the WAN port when there is a mismatch between PathTraceReceived and PathTraceExpected.
  - PathTraceExpected  
Enter a value for the path trace identifier that you expect to receive from the other side of the WAN channels.
  - PathTraceTransmitted  
Enter a value for the path trace identifier that you want to transmit to the other side of the WAN channels.
- Step 4** Click **Save** on the toolbar.

**Note**

When the path trace is set to enabled, an AIS is inserted downstream instead of the original signal when a mismatch occurs between expected and received path trace.

## 5.6.7 Read Path Trace Identifiers for a WAN Port

Path trace parameters can be read for each channel (VC12) in the WAN port.

- 
- Step 1** Select a WAN port.
- Step 2** When a WAN port managed object is expanded, click on the channel (vc12) where you want to see the Received Path Trace.
- Step 3** Click **PathTraceVC12**.

The following attributes can be read:

- **PathTrace**  
Set to enable if TIM alarms should be reported when there is a mismatch between PathTraceReceived and PathTraceExpected.
- **PathTraceExpected**  
Enter a value for the path trace identifier that you expect to receive from the other side of the path.
- **PathTraceTransmitted**  
Enter a value for the path trace identifier that you want to transmit to the other side of the path.
- **PathTraceReceived**  
The actual received path trace identifier from the other side of the link.




---

**Note** When path trace is set to enabled, the AIS is inserted downstream instead of the original signal when a mismatch occurs between expected and received PathTrace.

---

## 5.6.8 Monitor WAN Port Performance

- 
- Step 1** Select a WAN port.
- Step 2** When the WAN port managed object is expanded, click the channel (vc12) where you want to see the performance data.
- Step 3** Click **PmG826NearEndVc12** to read near-end PM data or **PmG826FarEndVC12** to read far-end PM data.

The following attribute is available:

- **Current15Min ES,SES, BBE and UAS**

- Step 4** To see the Performance history of the previous 16x15 minute counters click **Interval15Min**.

The following attribute is available:

- **Interval15Min ES,SES, BBE and UAS**
-

## 5.6.9 Advanced WAN Port Operations

For frequent users of Cisco Edge Craft, it is possible to make use of the enhanced editing facilities to speed up the configuration work. Complete the following steps to select and insert multiple termination points.

- Step 1** Select the channels where you want to add termination points as B-end. Use Shift or Ctrl buttons to select more than one channel, or simply drag the mouse down the list while pressing the left mouse button.
- Step 2** Select the TU-12 termination points that you want to add to the B-ends of the channels in the same way.
- Step 3** Click the **Set B** button in the toolbar.
- Step 4** Click **Save** on the toolbar.



**Note** You are only allowed to set the B termination points of channels where B is not in use. If you want to modify the B termination point, the relation with the existing B termination point must first be deleted. Then a new termination point can be added.



**Note** If you do not select the same number of instances of WAN channels and termination points, the channels will be filled in with as many TPs as available, starting from the top of the selected channel list. If more TPs are selected than channels, the last TPs will not be used.

## 5.7 ONS 15305 SDH Layer Network and Cross-Connections

This section describes how to manage cross connections between termination points on the network element and includes management of the complete life cycle of a cross connection, including creation, presentation, modification, deletion, and manual operation of the sub-network connection protection (SNCP) switch.

A cross-connection is defined by its termination points. Only termination points with the same characteristic information can be cross connected. The characteristic information of a termination point defines the format of the signal that can be transferred by this termination point. Format defines the capacity of the signal, for example TU-12 and VC-12 have the same characteristic information since they both have a 2 Mbps traffic capacity.

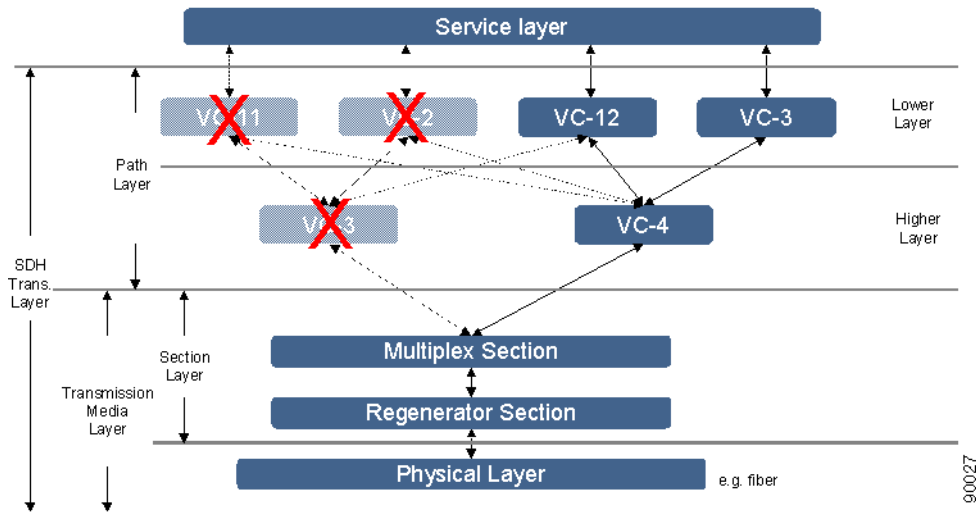
Unidirectional and bidirectional point-to-point cross connections with or without protection are supported.

The protection scheme supported by the first release of the ONS 15305 is SNC/I (inherent monitoring). Non-intrusive monitoring SNC/N will be supported in later releases.

The [“5.7.1 SDH Port Structuring” section on page 5-34](#) gives an introduction to SDH layers and cross connections. For further reading on SDH and cross connections, see ITU-T Recommendations G-Series.

An SDH network has layered structure as shown in [Figure 5-28](#). The layers operate in a client/server based scenario. The service layer generates the bit streams that are to be carried across the SDH network. This layer is not part of SDH. The path layer is a virtual layer and can only be observed through a management system. It is in this layer that the cross-connection management and structuring of the SDH ports is performed. The path layer works on containers.

Figure 5-28 SDH Layer Network

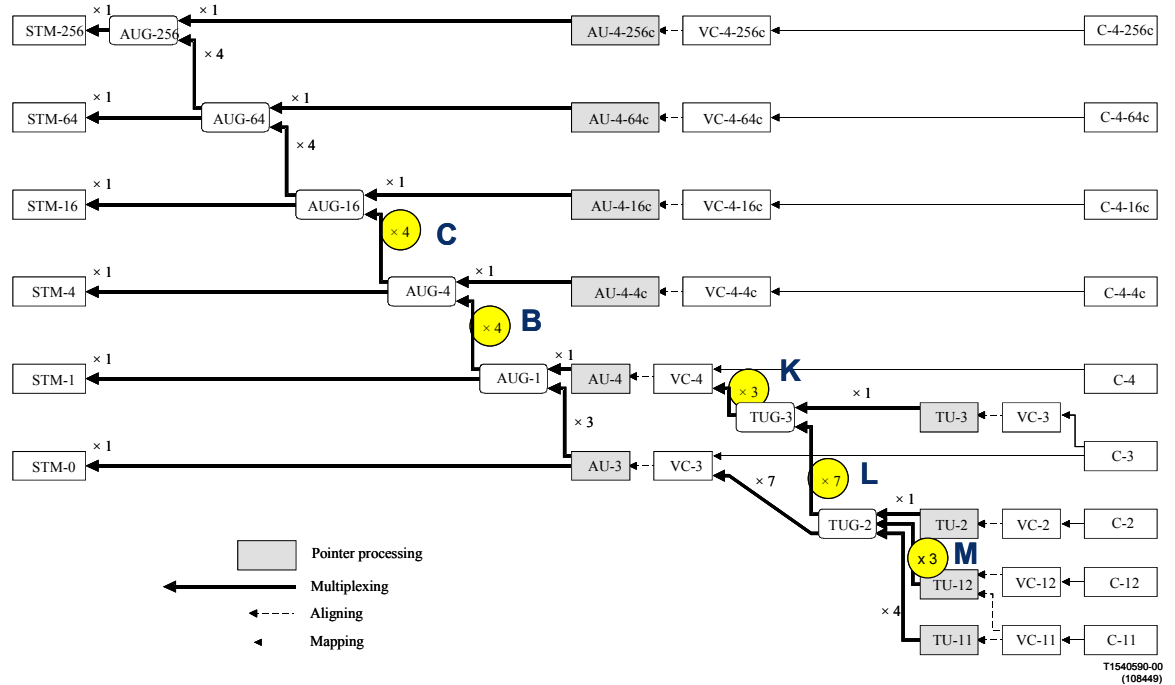


The ONS 15305 network element has support for VC-4 in the higher order layer and in the lower order layer VC-12 and VC-3.

### 5.7.1 SDH Port Structuring

The multiplexing structure of the SDH ports determines which layers and their termination points are available to be cross-connected. The multiplexing structure for SDH in all layers is shown in [Figure 5-29](#) (taken from ITU-T Recommendation G.707). The CBKLM value determines the path through the structure. The usage of the CBKLM value follows the rules defined in [Table 5-1](#).

Only traffic on non-terminated containers called connection termination points can be cross connected (AU-4, TU-3, and TU-12). The other containers, VC-4, VC-3, and VC-12, represent trail termination points where the traffic can be read.

**Figure 5-29 SDH Multiplexing Structure**

The original illustration used in [Figure 5-29](#) is found in ITU-T G.707/Y1322 (10/2000).

### 5.7.1.1 C.B.K.L.M Value Usage

**Table 5-1 CBKLM Value Usage**

Rules	Examples
When referring to SDH objects the complete CBKLM value is used even if some fields are in-significant.	
Not significant fields in CBKLM are set to 0.	AU-4 in STM-16: C.B.0.0.0 TU-3 in STM-16: C.B.K.0.0

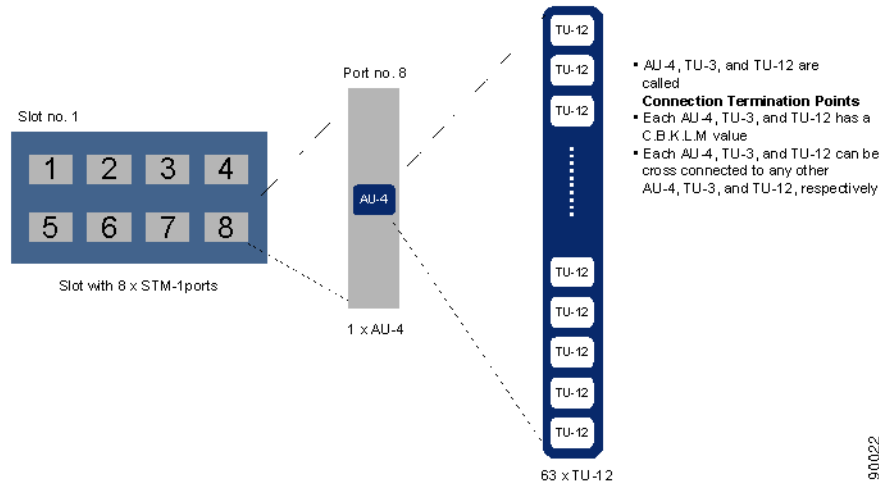
**Table 5-1 CBKLM Value Usage (continued)**

Rules	Examples
C identifies which AUG4. If no AUG4 exists, its is set to 1, like a phantom AUG4. B identifies which AUG1. If no AUG1 exists, its is set to 1, like a phantom AUG1.	<p>STM-1: C = 1, B = 1 There is <b>one</b> AUG1 in STM-1 and a phantom AUG4</p> <p>STM-4: C = 1, B = 1 - 4 There is one AUG4 in STM-4</p> <p>STM-16: C = 1 - 4, B = 1 - 4</p> <p>Example: AU-4 in STM-1: 1.1.0.0.0 TU-3 in STM-4: 1.3.3.0.0 TU-12 in STM-16: 2.4.2.7.2</p>
The CBKLM value is used for VC objects associated with E1, E3, and E4 modules but the C and B values are always 0.	<p>VC-12 on E1 module: 1.1.1.1.1 Protecting: 1.1.1.1.2 VC-3 on E3 module: 1.1.1.0.0 Protecting: 1.1.2.0.0 VC-4 on E4 module: 1.1.0.0.0 (not release1) Protecting: 1.2.0.0.0</p>
For VC objects for WAN	<p>VC-12 on E1 module: 1.1.x.y.z VC-3 on E3 module: x.y.z.0.0 (not release 1) VC-4 on E4 module: x.y.0.0.0 (not release 1)</p>
Combination 0.0.0.0.0 is not a legal value and can be used as an error code.	

### 5.7.1.2 Cross-Connection Management

Cross-connection management is the management of connectivity within the network element itself. Cross-connections (XC) are set up between connection termination points with the same characteristic information, for example cross connections between AU-4s, TU-3s, VC-12 and TU-12, or two VC-12s.



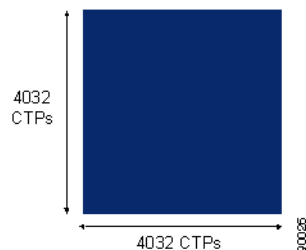
**Figure 5-30 Slot - Port - CTP Relations**

The ONS 15305 has four slots that can hold an SDH module. The module can be of different types, that means, STM-1, STM-4, or STM-16. In this document the STM-1 module with 8 ports is used as an example.

In addition the ONS 15305 can have PDH modules with a number of E1 or E3 ports. The E1 and E3 ports have a corresponding VC-12 or VC-3, respectively. These VCs can be cross connected to termination points on the SDH modules or with each other.

### 5.7.1.3 8-Port STM-1 Module Example

A slot with an 8 x STM-1 module has eight ports. Available CTPs on port no.8 in slot no. 1 are shown in [Figure 5-30](#). There is one AU-4 on the port and depending on the structuring of the AU-4 container, there are 63 TU-12s, 3 TU-3s, or a combination of TU-12s and TU-3s since the TUG-3s can be structured independently, which can be cross connected. This means that in this single slot there are  $8 \times 63 = 504$  CTPs (maximum) in the lower layer and  $8 \times 1 = 8$  CTPs in the higher layer. And what are the possible CTPs to be cross connected to? If we assume that all four slots in this ONS15305 are equipped with 8 x STM-1 modules there are  $3 \times 504 = 1512$  possible choices for the connecting CTP in the lower layer and  $8 \times 3 = 24$  in the higher layer. If an ONS15305 is equipped with four STM-16 modules, each of these modules has  $4 \times 4 \times 63 = 1008$  TU-12 CTPs. This means that the cross connect matrix in the fabric has the dimension 4032 x 4032 ([Figure 5-31](#)).

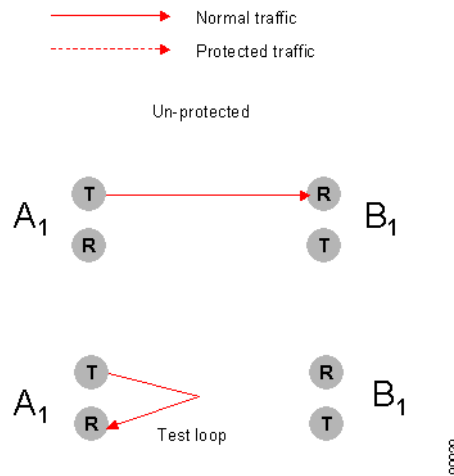
**Figure 5-31 Largest Possible Cross Connect Matrix**

There are several different types of cross connections:

- Point-to-point
- WAN XCs (a special type of point-to-point; see the “5.5.1 WAN Ports and Mapping” section on page 5-14).
- Drop and continue (not in R1).
- Broadcast (not in R1)

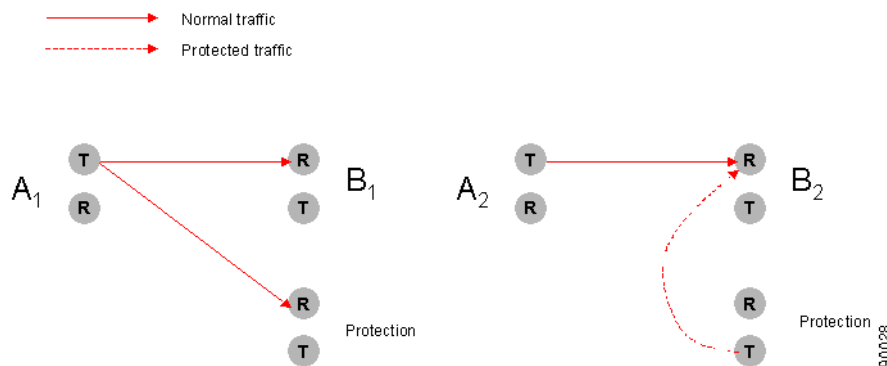
All of these types can be with or without protection and unidirectional or bidirectional. Un-protected, uni-directional cross connects can be used for test loops, as illustrated in Figure 5-32.

**Figure 5-32 Unidirectional XC, Unprotected**

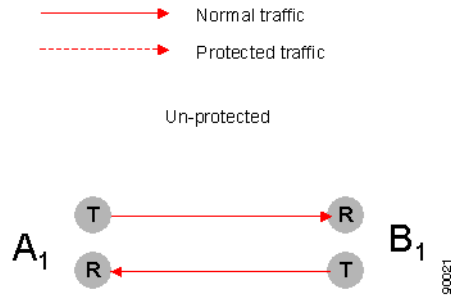


In Figure 5-33 protection has been set up for the termination point A1 and B2. The protected termination point A1 has no switching possibility since the cross connection is uni-directional, but termination point B2 has switching.

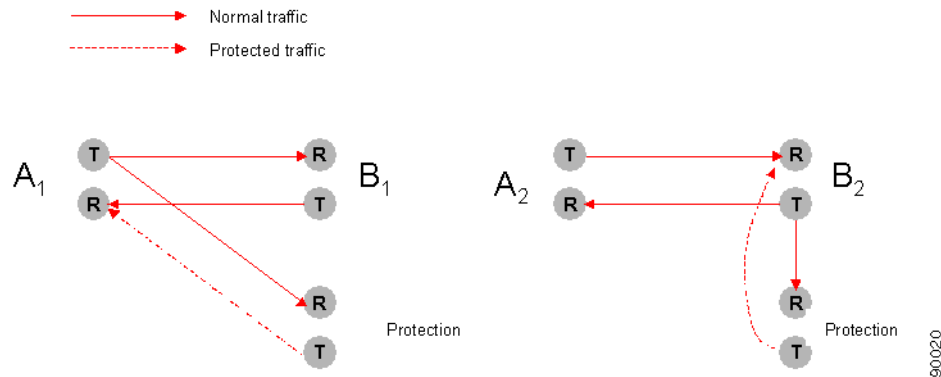
**Figure 5-33 Unidirectional XC, Protected**



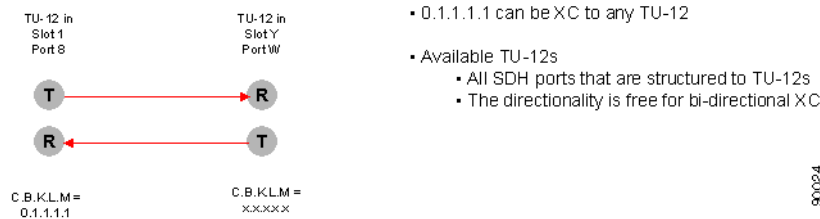
The bidirectional, unprotected cross connection is depicted in Figure 5-34. For bidirectional cross-connections all termination points have switching possibilities when protected.

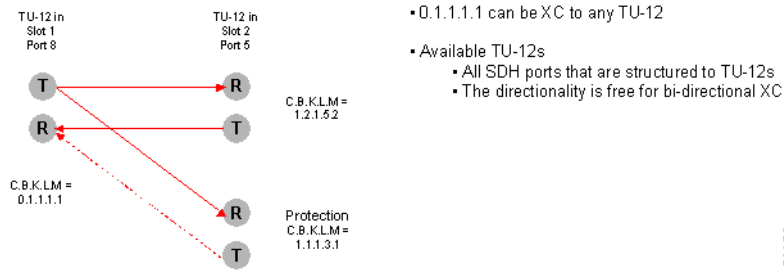
**Figure 5-34 Bidirectional XC, Unprotected**

In [Figure 5-35](#) the termination points A1 and B2 are protected, that means A1 can choose to receive from either B1 or the protection and B2 can switch between A2 or the protection.

**Figure 5-35 Bidirectional, Protected**

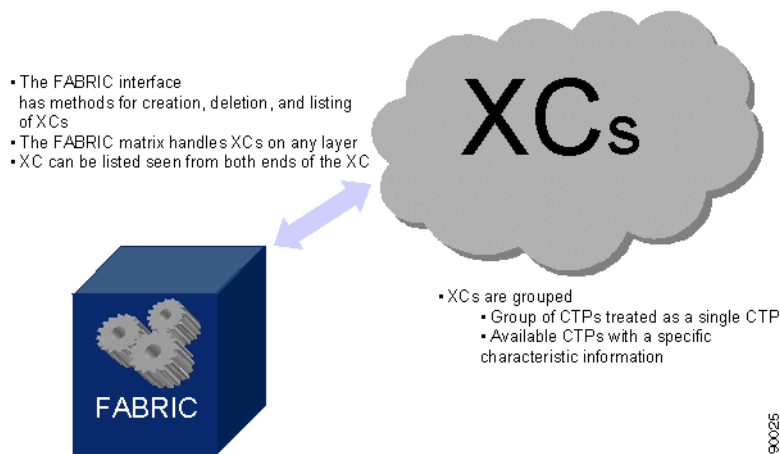
Examples of an unprotected, bidirectional, point-to-point cross connect and a protected, bidirectional, point-to-point cross connect are given in [Figure 5-36](#) and [Figure 5-37](#).

**Figure 5-36 Example of Bidirectional, Unprotected, Point-to-Point XC**

**Figure 5-37 Example of Bidirectional, Protected, Point-to-Point XC**

### 5.7.1.4 XC Fabric

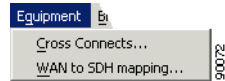
The connection management is taken care of by FABRIC as depicted in [Figure 5-38](#). The FABRIC has an interface that offers a set of methods that helps you in the cross-connection management tasks on any layer. The FABRIC can create, delete, and modify cross-connections. It has several options for listing XCs, for example, all XCs with the same characteristic information or all available CTPs on one port of a specific characteristic information. A third possible listing of CTPs can be a pre-defined grouping of points. A user might be indifferent to which specific CTP is used in an XC as long as it is a member of a specific group of CTPs. The system will choose an arbitrary CTP in the group. This will simplify the selection of CTP for you.

**Figure 5-38 XC Fabric**

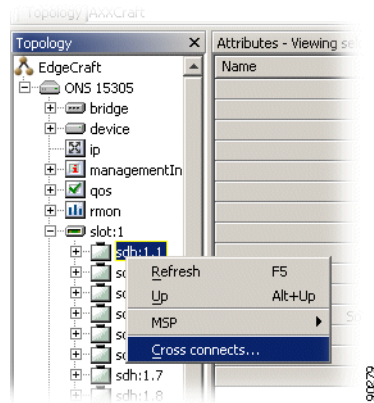
## 5.7.2 Open the Cross-Connection GUI

You have three possible choices for opening the Cross-Connection GUI.

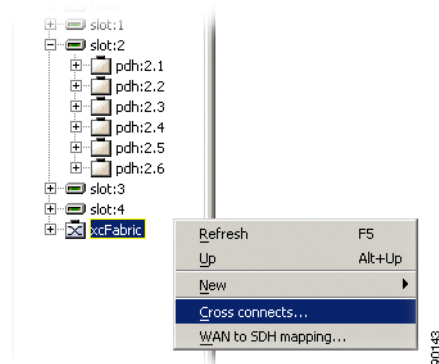
- Step 1** You can start the cross-connection GUI from the desktop menu. The system presents an empty cross-connection GUI ([Figure 5-39](#)).

**Figure 5-39 Select Cross Connect**

**Step 2** You can also start the cross-connection menu by clicking an **sdh port** (Figure 5-40)

**Figure 5-40 Select SDH Port Cross Connect**

**Step 3** Right-click the **xcFabric** managed object in the topology browser (Figure 5-41).

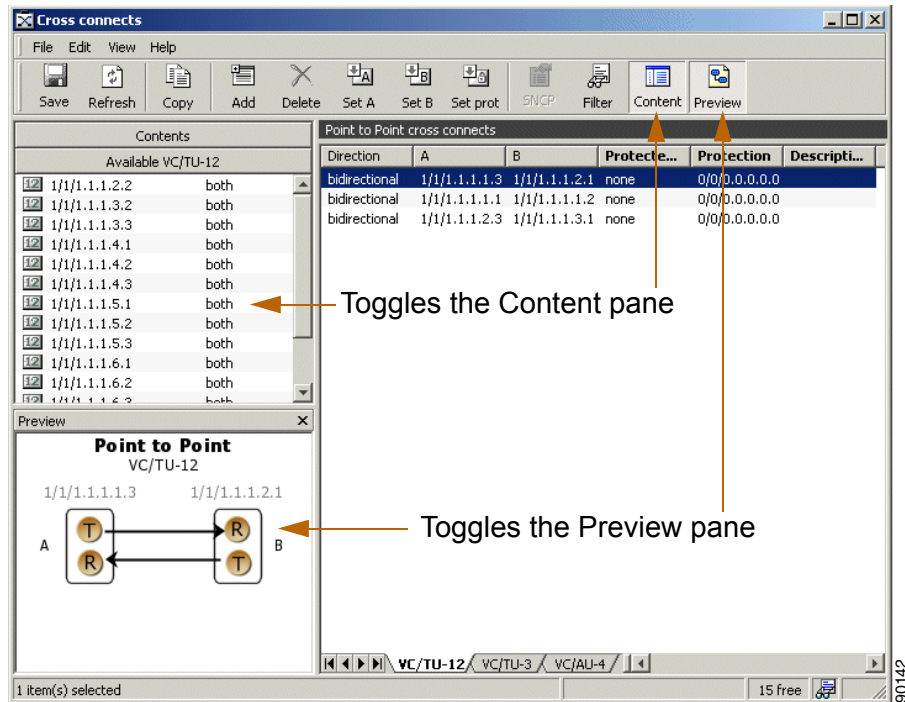
**Figure 5-41 Select XCFabric Cross Connect**

The system presents the cross-connection GUI with the relevant data from the selected managed object in the topology browser.

The cross-connection GUI allows you to filter the selection based on a predefined set of queries.

Figure 5-41 shows the cross-connection screen.

Figure 5-42 Cross-Connection GUI - Overview



## 5.7.3 Browse Existing Cross-Connections

This section explains how to browse and filter cross-connections.

### 5.7.3.1 Browse all Cross-Connections

Open the cross-connects window from the equipment menu. A list of all cross-connections appears.

For bidirectional cross-connections the termination points are located in the A column and the B column, according to how the cross-connection was created. One termination point can be in both the A and B-end column if the cross-connections are unidirectional. By default the cross-connections are sorted based on the A-end. Click the B column header to sort based on the B-end.

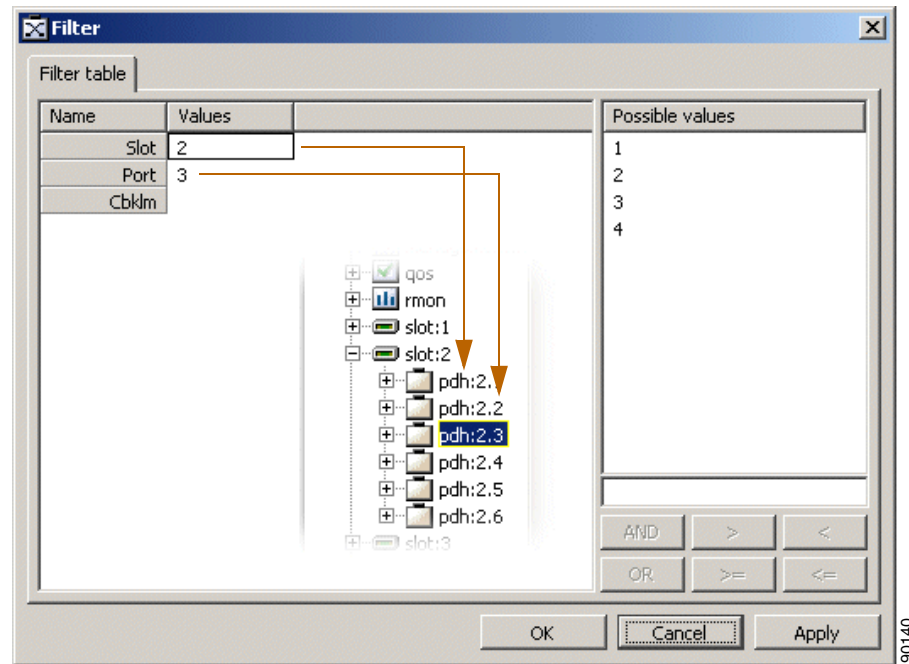
### 5.7.3.2 Browse Cross-Connections of a Port

- 
- Step 1** Select a port.
- Step 2** Right-click the port and select cross-connects.
- A list of all cross-connections to and from the port is shown.
-

### 5.7.3.3 Filter the Content of the Cross-Connection List

- Step 1** Open the Cross-connects window from the equipment menu or from a port as described above.
- Step 2** Click the **Filter** button in the toolbar (Figure 5-43).
- Step 3** Select the filtering criteria you want for slot, port, CBKLM, or a combination of the three.

**Figure 5-43 Example of Filtering Criteria - Cross-Connections**

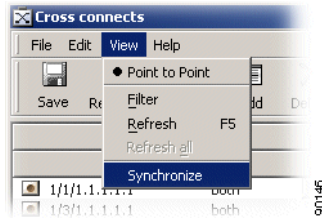


- Step 4** Click **Apply**.
- The cross-connects window shows only cross-connections where at least one of the termination points is included in the filtering criteria.
- A filter icon appears in the status bar of the window to indicate that the filter is active.

### 5.7.3.4 Synchronize or Refresh the Cross-Connect Window

Synchronization of the cross-connect GUI will synchronize the available TP list and cross-connections list with the MIB in ONS 15305 (Figure 5-44).

- Step 1** Select **Synchronize** from the View menu.

**Figure 5-44 Select Synchronize****Note**

This operation may take some time depending on the number of cross-connections that are created in the ONS 15305 and the management network. It ensures data integrity with the ONS 15305 MIB.

**Step 2** Click **Refresh** button on toolbar.

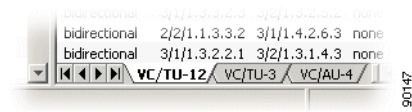
Refreshing the window will refresh the available TP list and cross-connection list based on the last operations performed by the local user of Cisco Edge Craft.

## 5.7.4 Set Up Cross-Connections from a 2 Mbps E1 Port to a Timeslot in an SDH Port

Creating a cross-connection from a 2 Mbps E1 port to a timeslot in an SDH port (TU-12 termination point).

**Step 1** Open the Cross-connects window from the equipment menu.

**Step 2** Select the **VC/TU12** tab in the bottom of the window, [Figure 5-45](#).

**Figure 5-45 Select the VC/TU12 Tab**

**Step 3** Make sure the Content panel is available in the left part of the window. If it is not available select the Content button in the toolbar.

**Step 4** Select the Available TP List in the Content panel. The list contains the free E1 ports and TU-12 termination points in ONS 15305.

**Note**

If the available TP List in the content panel does not show the E1 termination points that you want to cross-connect from, you have to make sure the slot is configured for E1 ports; see the [“5.3.1 Set the Port Mode for ONS 15305”](#) section on page 5-7.



**Note**

If the available TP list in the content panel does not show the TU-12 termination points that you want to cross-connect to, you have to make sure they are made available for cross-connection; see the [“5.2.1 Configure ONS 15305 SDH Port Structure \(Channelization\)”](#) section on page 5-2.

**Note**

You can create bidirectional or unidirectional cross-connections. In the available TP list you will see whether the termination point is available in both directions or as A-end or B-end.

- Step 5** Double-click the **E1 port** in the available TP list. A new cross-connection is created with the E1 port as the A-end.
- Step 6** Double-click the **TU-12** (timeslot) that you want to connect to. The TU-12 is moved to the B-end of the cross-connection.
- Step 7** Select **Direction** (unidirectional or bidirectional).
- Step 8** Click **Save** on the toolbar.

**Note**

Remember that both the E1 port and the SDH port must be enabled before traffic can flow between the ports; see the [“5.2.5 Enable the SDH Port to Carry Traffic and Report Alarms”](#) section on page 5-6 and the [“5.2.6 Set ONS 15305 SDH Port Synchronization Quality Output Signaling”](#) section on page 5-7.

## 5.7.5 Set Up Cross-Connections from a 45 Mbps E3 (T3) Port to a Timeslot in an SDH Port

Use the following steps to create a cross-connection from a 45 Mbps E3 (T3) port to a timeslot in an SDH port (TU-3 termination point).

- Step 1** Open the cross-connects window from the equipment menu.
- Step 2** Select the **VC/TU3** tab in the bottom of the window ([Figure 5-46](#)).

**Figure 5-46** Select the VC/TU12 Tab



## 5.7.6 Create a Pass-through Cross-Connection

Use the following steps to create a pass-through cross-connection from one SDH port to another SDH port.

- 
- Step 1** Open the Cross-connects window from the equipment menu.
- Step 2** Select the **TU-12** or **TU-3** or **AU-4 tab** termination points for both A and B ends in the bottom of the window.
- 

## 5.7.7 Modify Cross Connections

A cross-connection is a relationship between termination points; the relationship cannot be modified after it has been created.

It is not possible to modify the direction (bidirectional or unidirectional) of a cross-connection in the supported release of ONS 15305. The only parameter that can be modified is the description of the cross-connection.

Cross-connections can be protected after they have been created.

## 5.7.8 Protect Cross Connections

The A-end or B-end of a cross-connection can be protected by the SNC protection scheme either before or after a cross-connection has been created.



**Note**

When the cross-connection is uni-directional and protectedTP is **a**, a static bridge will be created from the A-end to the B and protection termination points. (SNCP parameters are not used).



**Note**

When the cross-connection is uni-directional and protected TP is **b**, an SNC protection switch is created where the signal from A is a working connection and the signal from protection is a protection connection. In this case the SNCP parameters are available after the cross-connection has been saved.

- 
- Step 1** Open the Cross-connects window from the equipment menu.
- Step 2** Set the protectedTP attribute to **a** or **b** for one or more cross-connections. This is the termination point you want to protect.
- Step 3** Select the cross-connection you want to protect.
- Step 4** Make sure that the content panel is available in the left part of the window. If it is not available select the Content button in the toolbar.
- Step 5** Select the available TP list in the content panel. The list contains the free TU12/VC12, TU3/VC3, or AU4 termination points in ONS 15305.



**Note**

If the available TP list in the content panel does not show the termination points that you want to protect your WAN channel with, you have to make sure they are made available for cross-connection; see the [“5.2.1 Configure ONS 15305 SDH Port Structure \(Channelization\)” section on page 5-2](#).

---

**Note**

You can protect bidirectional or unidirectional cross-connections. In the available TP list you will see whether the termination point is available in both directions or as A-end or B-end.

- Step 6** Select the termination point that you want to use to protect your a-end or b-end.
- Step 7** Click the **Set Prot** button in the toolbar. The protection TP is filled in for the selected cross-connection.
- Step 8** Select the next cross-connection to protect and insert the protection TP. Repeat until all cross-connections are protected (cross-connections that have the protected TP attribute set to a or b).
- Step 9** Click **Save** on the toolbar.

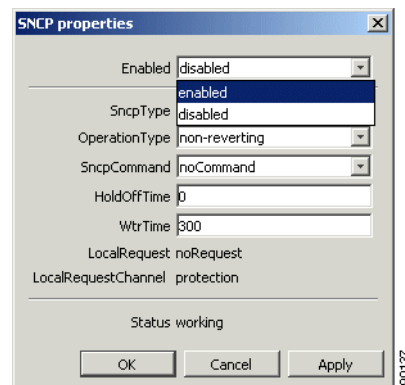
**Note**

By default the protection is disabled and will not work before it is enabled. Follow instructions below to enable SNC protection.

### 5.7.8.1 Enable SNC Protection

- Step 1** Select the cross-connections where you want to enable protection. (SHIFT and CTRL buttons can be used for multiple selection).
- Step 2** Click the **SNCP** button in the toolbar ([Figure 5-47](#)).
- Step 3** Set the Enabled attribute to **enabled** and click **OK**.

**Figure 5-47 Select Enabled Attributes**



- Step 4** Click **Save** on the toolbar.

**Note**

It is not possible to modify the protection termination point after it has been saved. If you want to modify the protection termination point, the ProtectedTP must first be saved as **none**. Then the protection TP can be modified. Remember to set the ProtectedTP back to **a** or **b**.

### 5.7.8.2 Modify Protection Parameters of a Cross-Connection

A-end or B-end of cross-connections are protected as described in “[5.7.8 Protect Cross Connections](#)” section on page 5-46. The SNC is then set up with a number of default parameters. The parameters can easily be modified.

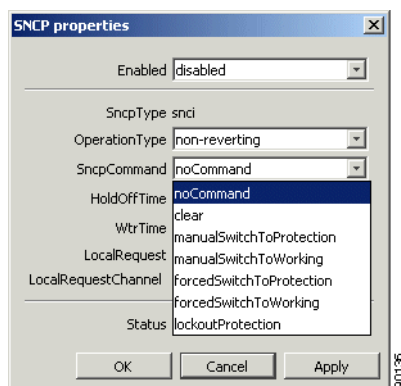
- 
- Step 1** Open the Cross-connects window from the Equipment menu.
  - Step 2** Select a cross-connection in the Cross-connect Window.
  - Step 3** Select the cross-connections where you want to modify protection parameters (Shift and Ctrl buttons can be used for multiple selection).
  - Step 4** Click the **SNCP** button in the toolbar.
  - Step 5** Modify the SNC protection parameters and click **OK**.
  - Step 6** Click **Save** on the toolbar.
- 

### 5.7.8.3 Command a Cross-Connection Protection Switch

With Cisco Edge Craft you can control the SNC protection switch by sending a command.

- 
- Step 1** Open the cross-connects window from the equipment menu.
  - Step 2** Select the cross-connections where you want to modify protection parameters (Shift and Ctrl buttons can be used for multiple selection).
  - Step 3** Click the **SNCP** button in the toolbar ([Figure 5-48](#)).
  - Step 4** Select the SncpCommand and click **OK**.

**Figure 5-48 Select SNCP Command**



- Step 5** Click **Save** on the toolbar.

Depending on the priority of the command and current status of each channel, a switch may now take place for some or all selected cross-connections.

---

## 5.7.9 Delete Cross-Connections

- 
- |               |                                                                                                              |
|---------------|--------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Open the cross-connection GUI by selecting cross-connects from the equipment menu.                           |
| <b>Step 2</b> | Select the panel for the type of cross-connections you want to delete (VC or TU12, VC or TU3, or VC or AU4). |
| <b>Step 3</b> | Select the cross-connections that you want to delete.                                                        |
| <b>Step 4</b> | Click <b>Delete</b> on the toolbar.                                                                          |
| <b>Step 5</b> | Click <b>Save</b> on the toolbar.                                                                            |
- 

## 5.7.10 Advanced Cross-Connection Operations

For frequent users of Cisco Edge Craft, it is possible to make use of the enhanced editing facilities to speed up the configuration work.

### 5.7.10.1 Set Up Multiple Cross-Connections by Multiple Selection

- 
- |               |                                                                                                                                    |
|---------------|------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Select the Termination points that you want to use as A-ends. Use Shift or Ctrl buttons to select more than one termination point. |
| <b>Step 2</b> | Click <b>Add</b> on the toolbar. The same number of cross-connections as the selected TPs are created with the A-end filled in.    |
| <b>Step 3</b> | Select the TU-12 termination points that you want to add to the B-ends of the cross-connections in the same way.                   |
| <b>Step 4</b> | Click the <b>Set B</b> button on the toolbar.                                                                                      |
| <b>Step 5</b> | If you want to protect the connections, select the TU-12 termination points that you want to add to the cross-connections.         |
| <b>Step 6</b> | Click the <b>Set Prot</b> button on the toolbar. Remember to set ProtectedTP to <b>a</b> or <b>b</b> .                             |
| <b>Step 7</b> | Click <b>Save</b> on the toolbar.                                                                                                  |



---

**Note** You are only allowed to set the B or protection termination points of cross-connections where B or P are not in use.  
If you want to modify the A or B termination point the cross-connection must be deleted and created again.  
If you want to modify the protection termination point the ProtectedTP must first be saved as none. Then the protection TP can be modified. Remember to set the ProtectedTP back to a.

---

**Note**

If you do not select the same number of instances of cross-connections and termination points, the A or B end will be filled in with as many TPs as available, starting from the top of the selected cross-connection list. If more TPs are selected than cross-connections, the last TPs will not be used.

### 5.7.10.2 Set Up Multiple Cross-Connections by Repeated Operations

- Step 1** Double-click the termination point you want to use as the A-end. A new cross-connection is created.
- Step 2** Double-click the termination point you want to use as the B-end. .
- Step 3** Repeat [Step 1](#) and [Step 2](#) for each cross-connection.
- Step 4** Click **Save** on the toolbar.

### 5.7.10.3 Enter Termination Points Manually

- Step 1** Add a new cross-connection.
- Step 2** Click n the A, B, or Protection termination points. A list of slots appears.
- Step 3** Select a slot. A list of ports appears.
- Step 4** Select a port.
- Step 5** Continue selecting each of the CBKLM values.
- Step 6** Enter the information the same way (or select from list of free TPs) for the other termination points.
- Step 7** Click **Save** on the toolbar.

**Note**

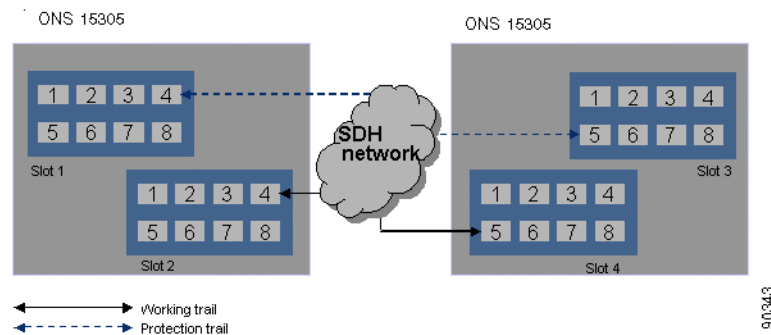
The information can also be entered directly without selecting the numbers from the drop-down list. Remember to use the following format: <slot/port/C.B.K.L.M>

## 5.8 ONS 15305 SDH Protection Management

This section explains how to manage the 1+1 linear multiplex section protection (MSP) between two SDH ports. It includes managing the complete life cycle of an MSP, including creating, presenting, modifying, deleting, and manually operating the MSP switch.

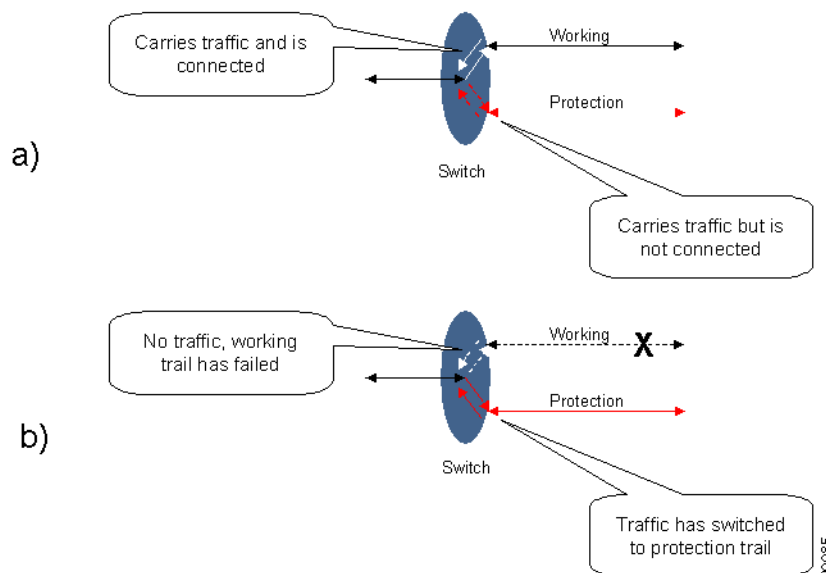
### 5.8.1 Multiplex Section Protection

The 1+1 MSP provides protection of the SDH ports by replacing the supporting trail when it fails, as illustrated in [Figure 5-49](#). This is a 100% redundant protection scheme.

**Figure 5-49 1+1 MSP Between two ONS 15305**

Both working and protection trails are enabled and the signal is bridged to both.

- a. The received signal from the working trail is forwarded to the receiving client while the protection is not. If the working trail fails and a switch is performed, the traffic on the protection trail is received by the client (Figure 5-50).

**Figure 5-50 Protection Switching Scenarios**

- b. Traffic from the working trail is ignored. The network element uses a bidirectional switching protocol, meaning both ends of the trails switch simultaneously. To synchronize simultaneous switching, the network elements signal to each other in the K1 and K2 bytes in the MS overhead of the SDH traffic. A bidirectional switching protocol gives better control of the traffic in the network but uses slightly more time to perform the switching than a uni-directional switching protocol.

The switching has two different modes:

- Revertive traffic returns to the working trail when recovered.
- Non-revertive traffic stays on the protection trail indefinitely or until told otherwise.

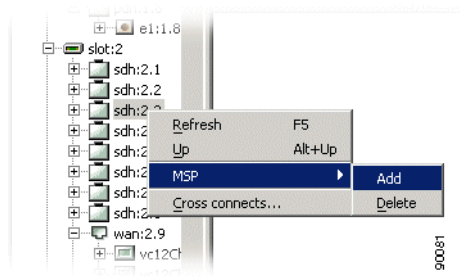
The time to wait before restoring the trail can be defined.

When switching either from or to protection, an event notification is generated.

## 5.8.2 Protect Section by MSP

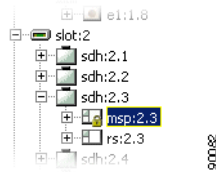
- Step 1** In the topology browser, right-click the sdh port that should be the working port
- Step 2** Click **Add** in the pop-up menu. An msp object is created below the port (Figure 5-51).

**Figure 5-51 Select SDH Port**



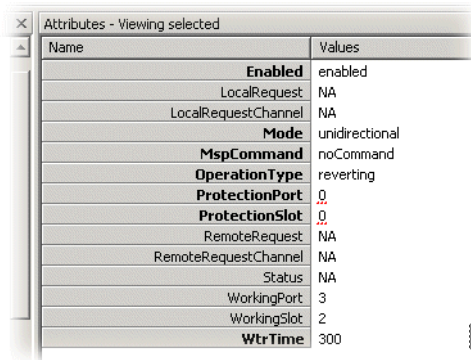
- Step 3** Select the msp object in the topology browser (Figure 5-52).

**Figure 5-52 Select MSP Object**



- Step 4** Fill in the ProtectionSlot and ProtectionPort attributes (Figure 5-53).

**Figure 5-53 Select Protection Port Attributes**



- Step 5** Use default or fill in new values for the other attributes.
- Step 6** Click **Save** on the toolbar.



The MSP scheme is created in ONS 15305 and starts working immediately. You will also see that the same msp object is now available under the protection port. You will also see that if the msp has the same Object identifier (for example 1.2.) as the parent sdh port, the port is a working port. If it has a number that is different from the parent sdh port (for example sdh port is 1.4 and msp is 1.2) it is a protection port for the sdh port with the same object identifier as the msp object.

**Note**

The working and protection ports must be selected from slot 1 and 2 or 3 and 4. For example it is not possible to set up MSP protection with the working port from slot 1 and protection port from slot 3. Working and protection ports can be selected from the same slot.

**Note**

A protection port must be unstructured; see the [“5.2.2 Modify or Remove ONS 15305 SDH Port Structure” section on page 5-3](#).

**Note**

Working and protection port must have the same STM-N rate, for example both STM-1.

## 5.8.3 Modify MSP

- Step 1** In the topology browser right-click the sdh port that is the working port.
- Step 2** Select **msp object** below the sdh port.
- Step 3** Modify the attributes of the MSP scheme.
- Step 4** Click **Save** on the toolbar.

**Note**

If the link is operating on the protection section in bidirectional mode, you can effect traffic if you set Mspenabled to disabled or OperatingMode to unidirectional in one of the nodes. This is due to the behavior of the APS protocol.

**Note**

To avoid problems always make sure the link is operating on the working section and lock out protection before making the modifications.

## 5.8.4 Delete MSP

- Step 1** In the topology browser right-click the sdh port that is the working port.
- Step 2** Select **MSP** and **Delete** in the pop-up menu. The msp object disappears both from the working port and the protection port in the topology browser.
- Step 3** Click **Save** on the toolbar.

**Note**

It is possible to delete an MSP when traffic is on protection section. This will cause a short break during switchover time. (If working section is available).

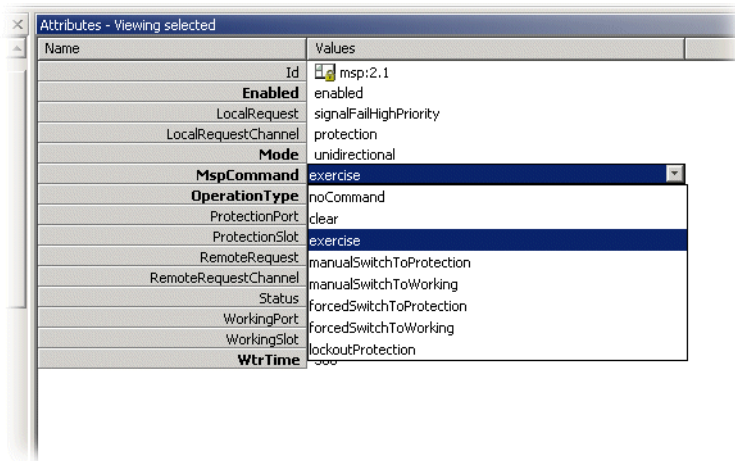
**Note**

To avoid problems always make sure the link is operating on the Working section and to command it to lockout of protection before deleting the MSP.

## 5.8.5 Command an MSP Switch

- Step 1** In the topology browser right-click the sdh port that is the working port.
- Step 2** Select **msp object** below the sdh port.
- Step 3** Select one of the commands under MspCommand (Figure 5-54).

**Figure 5-54 Select MspCommands Attribute**



- Step 4** Click **Save** on the toolbar.

**Note**

Commands will only take place if there are no higher priority requests in the system.

**Note**

A new command will clear the current command before executing the new command. In this case the new command may not be executed when the new command has lower priority than the old command because the MSP will search for the request with highest priority present. For example, sending a manual switch to a protection command instead of a forced switch to a protection command will not work if there is a signal degrade request on the protection section.

**Note**

All commands can be cleared by the clear command.

## 5.8.6 Legal Combinations of SNCP and MSP

It is possible to use both SNCP and MSP in an ONS 15305 simultaneously, as long as the following is satisfied:

The protected SNCP entity can be part of an MSP protected port, but the working or protection entity cannot, for example, consider an STM-4 ring where some TU-12s are dropped off the ring and sent to an ONS 15302 via an STM-1 link. In this case, SNCP can be used in the ring, protecting the TU-12s to be dropped from the ring toward the ONS 15302. MSP can then be used for the STM-1 link to protect the traffic between the ONS 15305 and the ONS 15302. This is because the TU-12s that are dropped from the ring are the protected TU-12s, while the TU-12s in the ring are the working and protection TU-12s. Consequently, it is not possible to use MSP on the east or west links of the ring, since the TU-12s that are carried here are the working or protection part of the SNCP protected path's.

## 5.8.7 SubNetwork Connection Protection

SNCP is strongly related to the cross-connection that is protected in the network element. In Cisco Edge Craft SNCP related issues are handled from the cross-connections GUI.

**Note**

The maximum number of SNCP instances that can be used with guaranteed switching time below 50 ms is 252. This corresponds to one full STM-4 (or four STM-1s) structured into TU-12s. These 252 SNCP instances can be a mixture of AU-4, TU-3 and TU-12 in any combination, and taken from any C.B.K.L.M address within an STM-1/4/16. A larger number of instances than 252 may be used, but in this case we cannot guarantee switching times below 50 ms.

The resolution of the Hold-off timer is  $N \times 100\text{ms} \pm 60\text{ ms}$ . That means for a 500 ms Hold-off timer, the real timer value may be any value between 440 ms and 560 ms. The Working, protection and protected parts of an SNCP protected path can be carried over different link rates. For example for an SNCP protected TU-12, the working TU-12 could be carried over an STM-16 link, while the protection TU-12 could be carried over an STM-4 link.

### 5.8.7.1 Protect Connection by SNCP

See the [“5.7.8.1 Enable SNC Protection”](#) section on page 5-47.

### 5.8.7.2 Modify SNCP

See the [“5.7.8.2 Modify Protection Parameters of a Cross-Connection”](#) section on page 5-48.

### 5.8.7.3 Command an SNCP Switch

See the [“5.7.8.3 Command a Cross-Connection Protection Switch”](#) section on page 5-48.

## 5.9 ONS 15302 SDH Protection Management

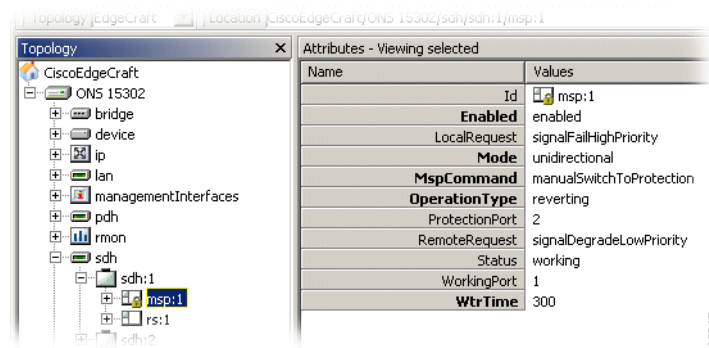
The ONS 15302 offers 1+1 linear multiplex section protection (MSP). The protocol used for K1 and K2 (b1 to b5) is defined in ITU-T G.841, clause 7.1.4.5.1. The protocol used is 1+1 bidirectional switching compatible with 1:N bidirectional switching.

Use the following steps to configure the operation of the protection switch.

### 5.9.1 Modify MSP Parameters

- Step 1** Select **sdh1** port (working) and click the **msp** object (Figure 5-55 and Figure 5-56).

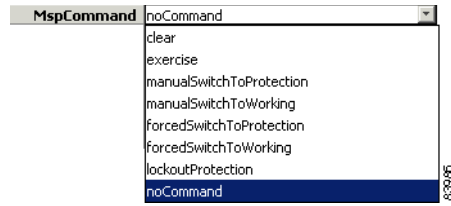
**Figure 5-55 Select SDH1/MSP1 Attributes**



- Step 2** Edit the following parameters as needed:

- **Enabled**  
Set to enabled or disabled.
- **Mode**  
Set to unidirectional or bidirectional.
- **MspCommand**  
Set one of the following.
- **OperatingType**  
Set to reverting or non-reverting.
- **WtrTime**

Wait to restore time; number of seconds to wait before switching back to the preferred link after it has been restored (0,1, .....,12 minutes, default 5 min (300 seconds)).

**Figure 5-56 Set MSP Command**

**Step 3** Click **Save**.

---





## Link Aggregation

---

This chapter describes how to manage the link aggregation functionality of the network element. Link aggregation is also called trunking.

Link aggregation is used to optimize port (link) usage by grouping ports together to form a single aggregate. Link aggregation multiplies the bandwidth between the devices, increases port flexibility and provides link redundancy.

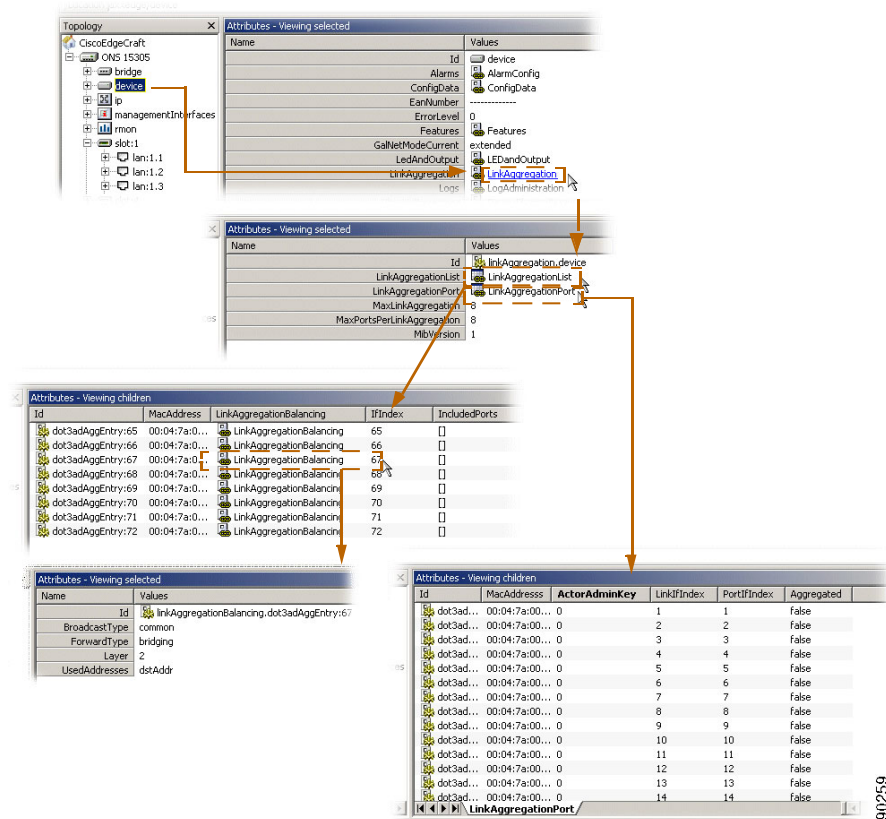
The network element defines the number of link aggregations and a maximum number of ports in each link aggregation.

### 6.1 View Link Aggregation - ONS15305

---

- Step 1** Select the **device > Link Aggregation** object in the topology pane to view the specific object properties in the attributes pane ([Figure 6-1](#)).

Figure 6-1 Attributes Related to Link Aggregation



## 6.2 Modify Link Aggregation - ONS 15305

You can modify the modifiable Link Aggregation parameters, including:

- Modify attributes for an aggregation.
- MAC address type for an aggregation.
- Balance attributes for an aggregation.
- Add of new port(s) to an aggregation.
- Delete of port(s) in an existing aggregation.

The link aggregation feature, also known as trunking, allows you to link a group of ports together to form a single trunk (aggregated group). Link aggregation can be used to increase bandwidth between devices and/or to provide link redundancy.

The link aggregation feature has a number of limitations:

- Only LAN and WAN ports can be part of a trunk.
- Maximum 8 trunks can be defined on the network element.
- Maximum 8 ports can be grouped within a single trunk.



**Note**

8 possible trunks are already created, but they include no port. The trunks are listed under the attribute Device > LinkAggregation > LinkAggregationList. Each trunk is identified by its ifIndex (from 65 to 72).

In order to assign a port to a trunk, the port must comply with the following requirements:

- A layer 3 interface is not configured on the port.
- A VLAN is not configured on the port.
- The port is not assigned to a different trunk.
- An available MAC address exists which can be assigned to the port.
- Auto-negotiation mode is not configured on the port.
- The port is in full-duplex mode.
- All ports in a trunk must operate at the same rate.
- All ports in a trunk must have the same ingress filtering and tagged modes.
- All ports in a trunk must have the same back pressure and flow control modes.
- All ports in a trunk must have the same priority.
- All ports in a trunk must have the same transceiver type.
- All ports in a trunk must belong to the same module, that means they must be located on the same slot.

## 6.2.1 Assign a Port to a Trunk

Use the following steps to assign a port to a trunk.

- Step 1** Make sure that the port to be added to a trunk complies with the requirements listed above.
- Step 2** Click on the ONS 15305 managed object, and then on the device managed object in the topology browser.
- Step 3** Click on the **linkAggregation** attribute in the attribute window.
- Step 4** Click on the **linkAggregationPort** attribute in the attribute window.
- Step 5** Identify the port to add via its ifIndex listed under the portIfIndex attribute.
- Step 6** Verify that the port can be part of a trunk by checking the aggregated attribute. If aggregated displays true, the port can be included in a trunk, please go to the next step. If aggregated displays false, the port can only operate as an individual link, and cannot be part of a trunk. Select another port (go back to [Step 5](#)).
- Step 7** Edit the actorAdminKey attribute. This attribute must be set to the ifIndex of the trunk to which the port shall be assigned. Legal values are [65:72].

**Note**

To find out the ifIndex used by the trunk, check the Device > LinkAggregation > LinkAggregationList attribute

**Step 8** Click **Save**.

## 6.2.2 Trunk Elements used by Management are Named ifindex

Regular ports, LAN and WAN, have ifIndexes from 1 to 64, depending on the slot and port number.

16 ifIndexes are reserved for each slot, although none of today's modules use more than 8. For example, an fast Ethernet (FE) module with 8 ports located in slot 3, have ifindex range from 33 for port 3/1 to 40 for port 3/8.

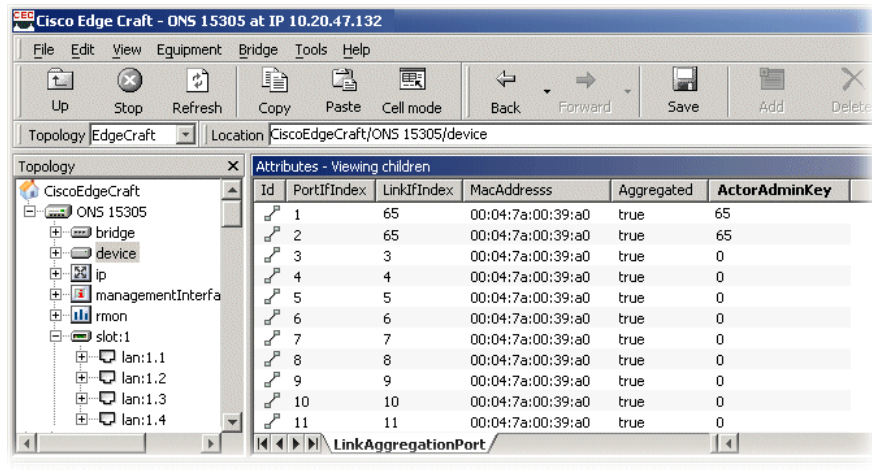
STM-1 modules are special since they are a combination of 8 SDH ports and 8 WAN ports. WAN ports in an 8XSTM1 module are numbered x/9 to x/16 (x is the slot), while the ifIndexes corresponds to x/1 to x/8. For an 8xSTM-1 module located in slot 2, the ifindex range is 17 to 24 (17 for port 2/9, 24 for port 2/16). Giga bit Ethernet (GE) ports use the first ifIndexes for the particular slot. For example, a 2XGE in slot 4 have ifindex numbers 49 for port 4/1 and 50 for port 4/2.

Maximum number of trunks in the system is 8, and the trunk ifindex range is 65 to 72. The trunk ifindex is used as port number when a trunk is assigned to a VLAN.

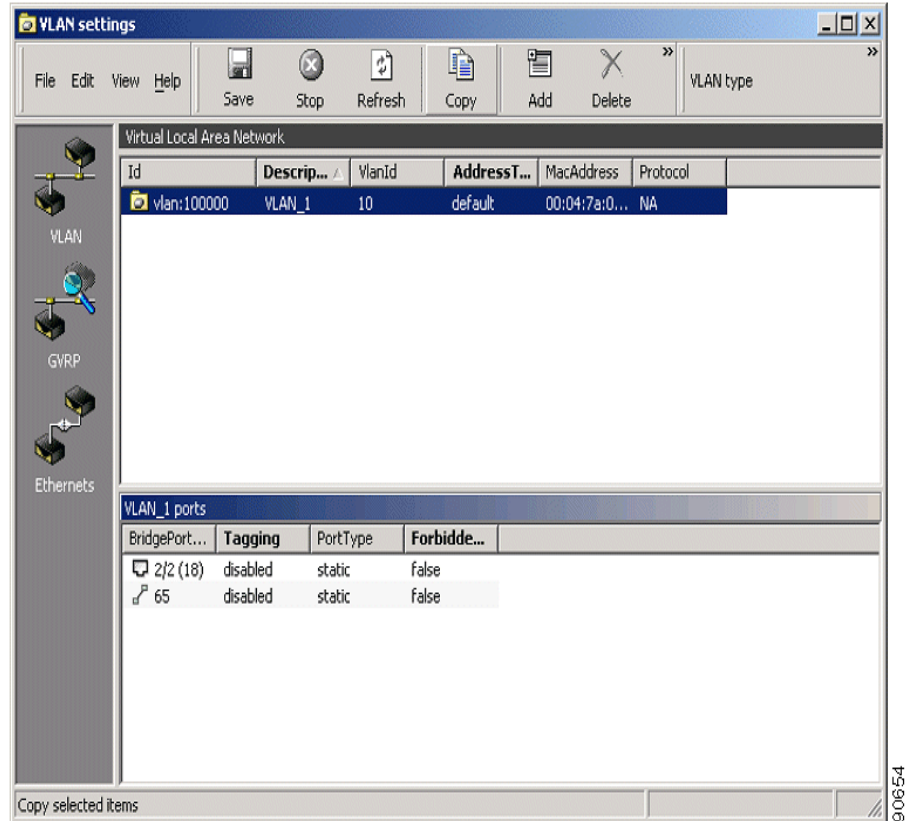
An example to illustrate the creation of a trunk and adding the trunk to a VLAN (Figure 6-2).

The first two WAN ports of slot 1 are used to create a trunk with ifindex 65.

**Figure 6-2** Creating and Editing a Trunk to a VLAN



The trunk and the second GE port in slot 2 are put together in a VLAN (Figure 6-3).

**Figure 6-3** VLAN settings for a Trunk with GE





## Layer 2 Configuration

---

This chapter explains how to manage the bridging service (L2 forwarding) on the network element and includes:

- Presentation and modification of the bridge.
- Presentation and modification of MAC Multicast and IGMP Snooping.
- Presentation and modification of spanning tree protocol (STP) and Rapid STP (RSTP).
- Presentation and modification of traffic control.
- Presentation and modification of virtual local area network (VLAN).



### Note

The following examples focus on ONS15305, but the the features described also apply to the ONS 15302.

---

## 7.1 Bridge

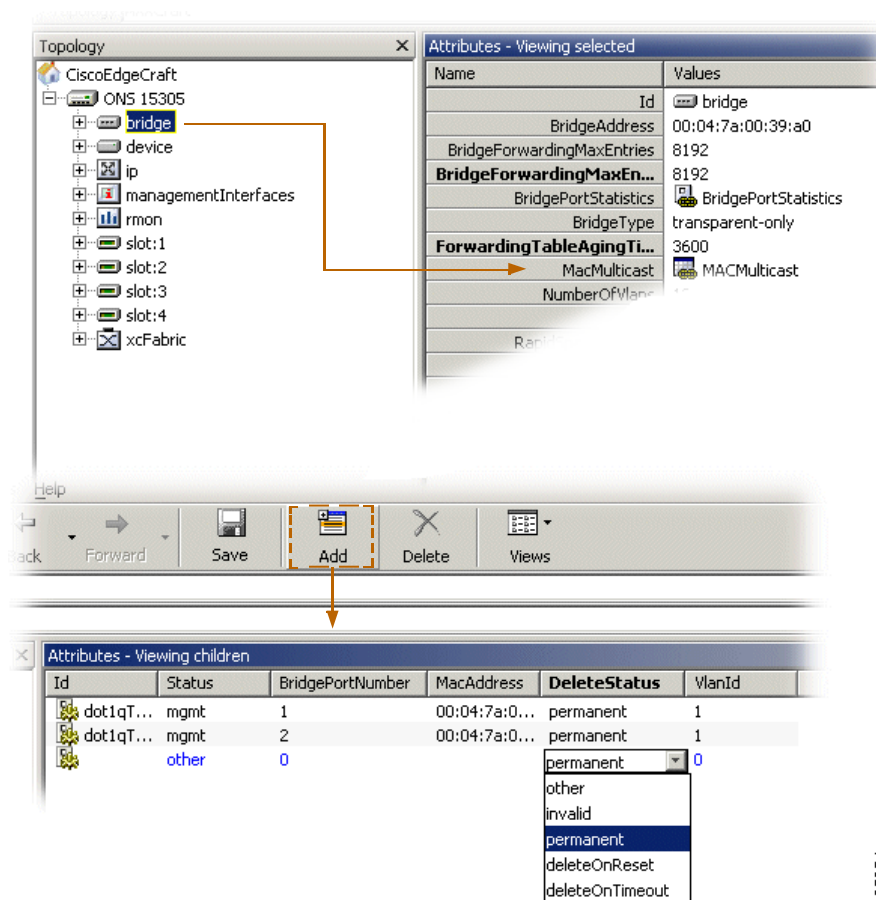
This chapter describes the configuration operations supported by the Bridge managed object.

For troubleshooting information, see [Appendix A, “Troubleshooting and FAQ.”](#) It also contains tips and answers to several frequently asked questions.

### 7.1.1 Configuration of Static Unicast Forwarding Information Example

Use the following steps to configure an entry in the MAC unicast forwarding table ([Figure 7-1](#)).

- 
- Step 1** Click on the ONS 15305 managed object, then click the **Bridge** managed object in the topology browser.
- Step 2** Double-click **unicastForwarding** in the attributes window.

**Figure 7-1 Configuration of Static Unicast Forwarding Information**

**Step 3** Click **Add** on the toolbar.

**Step 4** The following attributes have no default values and must be defined:

- **bridgePortNumber**  
Set the bridge port number of the port through which the MAC address can be reached.
- **macAddress**  
Set the MAC address. The MAC address must be a unicast address.
- **vlanId**  
Set the VLAN ID for which this entry applies.
- **deleteStatus**  
Set permanent if the entry should not be removed dynamically from the table (such an entry will stay over a reset of the bridge). Set deleteOnReset if the entry should be removed dynamically from the table after the next reset of the bridge. Set deleteOnTimeout if the entry should be dynamically aged out by the bridge.

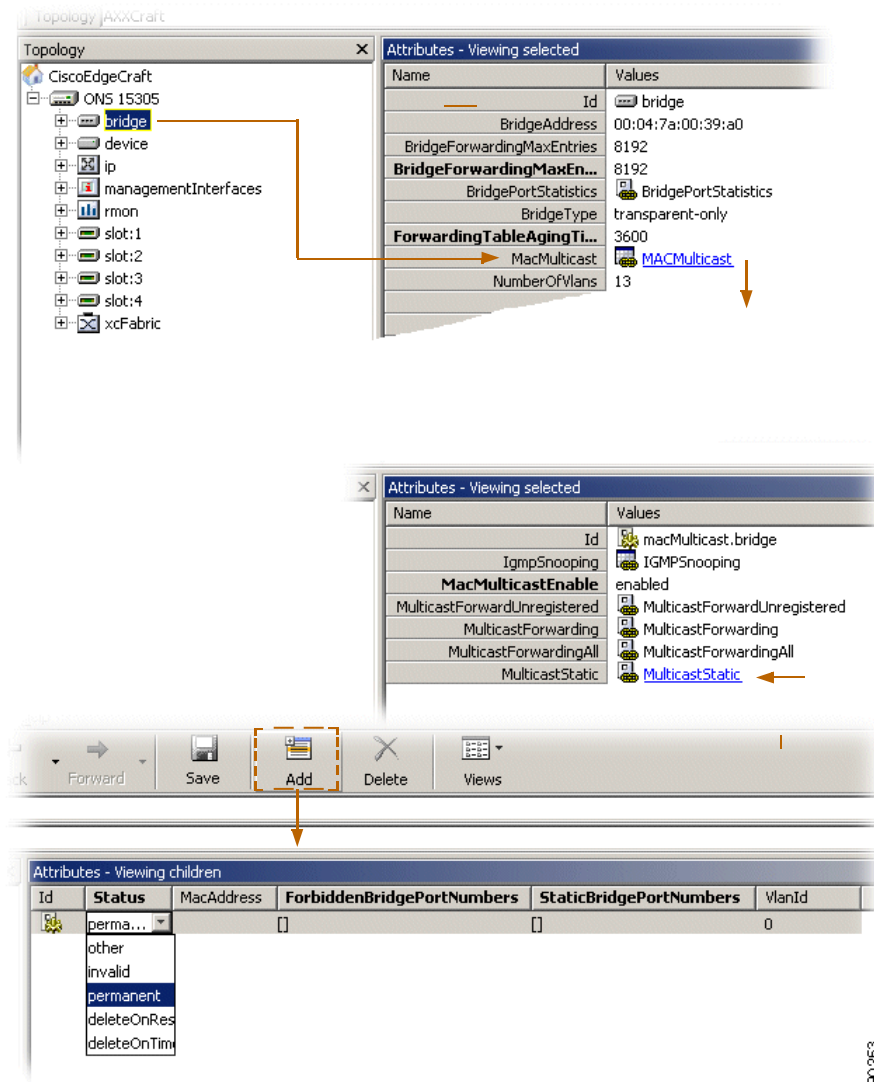
**Step 5** Click **Save** on the toolbar.

## 7.1.2 Configure Static Multicast Forwarding Information

See the “[Question 5](#)” section on page A-2 before you begin configuring an entry in the MAC multicast forwarding table (Figure 7-2).

- Step 1** Click on the ONS 15305 managed object, and then click the **Bridge** managed object in the topology browser.
- Step 2** Double-click **MACMulticast**, then double-click **MulticastStatic** in the attributes window.

**Figure 7-2 Configuration of Static Multicast Forwarding Information**



- Step 3** Click **Add** on the toolbar.
- Step 4** The following attributes have no default values, and must therefore be defined:
- vlanId
- Set the VLAN ID for which this entry applies.

- **MacAddress**  
Set the MAC address. The MAC address must be a multicast address.
- **staticBridgePortNumbers**  
Set the set of ports through which the multicast/broadcast frame must be forwarded regardless of any dynamic information. The set of ports is entered as an octet string where each bit represents one port, for further information see also [Appendix A, “Troubleshooting and FAQ.”](#)
- **forbiddenBridgePortNumbers**  
Set the set of ports through which the frames must not be forwarded regardless of any dynamic information. The set of ports is entered as an octet string where each bit represents one port, for further information see also [Appendix A, “Troubleshooting and FAQ.”](#)
- **status**  
Set permanent if the entry should not be removed dynamically from the table (such an entry will stay over a reset of the bridge). Set `deleteOnReset` if the entry should be removed dynamically from the table after the next reset of the bridge. Set `deleteOnTimeout` if the entry should be dynamically aged out by the bridge.

**Step 5** Click **Save** on the toolbar.



**Note**

When a multicast forwarding information is added to the table, the same entry is automatically added to the Bridge > macMulticast > multicastForwarding attribute. The multicastForwarding attribute contains both static, that means user-defined, and learned entries related to group (multicast) addresses.

## 7.1.3 Enable IGMP Snooping

When a host wants to receive multicast traffic, it must inform the routers on its LAN. The IGMP is the protocol used to communicate group membership information between hosts and routers on a LAN. Based on the information received through IGMP, a router forwards multicast traffic only via interfaces known to lead to interested receivers (hosts).

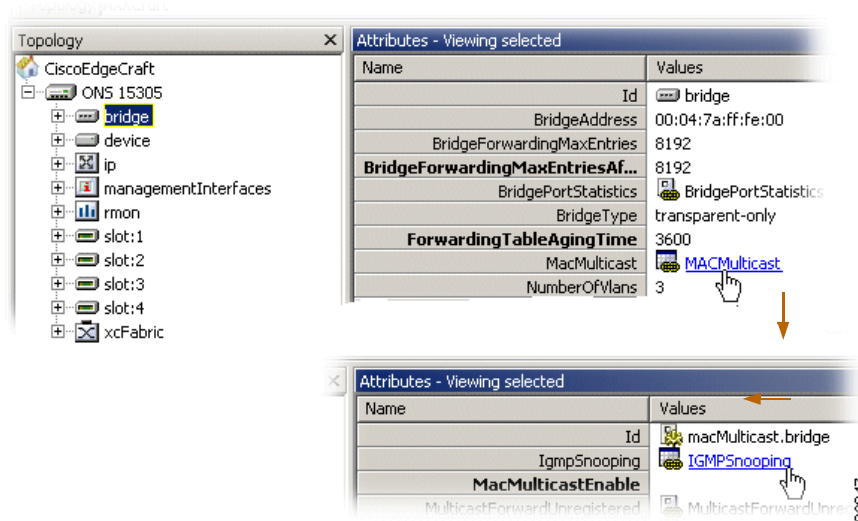
On the contrary, bridges flood multicast traffic out all ports per default, and therefore waste valuable network resources. IGMP snooping on a bridge can eliminate this inefficiency. IGMP snooping looks at IGMP messages to determine which hosts are actually interested in receiving multicast traffic. Based on this information, the bridge will forward multicast traffic only to ports where multicast receivers are attached.

Complete the following steps to enable IGMP snooping on the network element ([Figure 7-3](#)).

- Step 1** Click on the ONS 15305 managed object, and then on the **Bridge** managed object in the topology browser.
- Step 2** Click on the **macMulticast** attribute in the attribute window.
- Step 3** Set the **macMulticastEnable** attribute to **enabled**.
- Step 4** Click on the **igmpSnooping** attribute in the attribute window.
- Step 5** Set the **igmpSnoopingEnable** attribute to **true**.
- Step 6** Click **Save**.



Figure 7-3 Enabling IGMP Snooping



## 7.2 Spanning Tree Protocol (STP) Configuration

The STP allows layer 2 devices to discover a subset of the topology that is loop-free but still has a path between every pair of LANs.

The network element can run either one single STP algorithm for the whole device (perDevice type), or one STP algorithm per VLAN (perVLAN type). The type of STP algorithm can be selected by setting the ONS 15305 > Bridge > SpanningTree > stpTypeAfterReset attribute. The network element must be restarted for the new STP type to become effective.

### 7.2.1 Configure the STP Algorithm per Device

Use the following steps to configure the STP algorithm per device.

- Step 1** Make sure that the STP type is per device (check the ONS 15305 > Bridge > SpanningTree > stpType attribute which indicates the current STP type).
- Step 2** Click on the ONS 15305 managed object, and then on the **Bridge** managed object in the topology browser.
- Step 3** Click on the **SpanningTree** attribute in the attribute window.
- Step 4** Set stpEnable to true.
- Step 5** Edit the forwardDelay, helloTime, maxAge, and priority attributes if required.
- Step 6** Click **Save**.
- Step 7** Click on the **SpanningTreePerDevice** attribute in the attribute window.
- Step 8** Edit the BelongToVLAN attribute as required (if this attribute is set to true, only ports members of a VLAN will participate in the STP algorithm).

- Step 9** Click **Save**.
  - Step 10** Optionally, the priority, cost, and portEnable attributes can be edited per port. To do so, click on the SpanningTreePort attribute, and modify the attributes as required.
  - Step 11** Click **Save**.
- 

## 7.2.2 Configure the STP Algorithm per VLAN

Use the following steps to configure the STP algorithm per VLAN.

- Step 1** Make sure that the STP type is perVLAN (check the ONS 15305 > Bridge > SpanningTree > stpType attribute which indicates the current STP type).
  - Step 2** Click the ONS 15305 managed object, and then on the **Bridge** managed object in the topology browser.
  - Step 3** Click on the **SpanningTree** attribute in the attribute window.
  - Step 4** Set stpEnable to true.
  - Step 5** Edit the forwardDelay, helloTime, maxAge, and priority attributes if required.
  - Step 6** Click **Save**.
  - Step 7** Click on the **SpanningTreePerVLAN** attribute in the attribute window.
  - Step 8** Edit the vlanEnable attribute as required (if this attribute is set to true, the VLAN will run the STP algorithm).
  - Step 9** Click **Save**.
  - Step 10** Optionally, the priority, cost and portEnable attributes can be edited per port for a VLAN. To do so, click on the SpanningTreePerVlanPort attribute belonging to the VLAN, and modify the attributes as required.
  - Step 11** Click **Save**.
- 

## 7.3 Rapid Spanning Tree Protocol Configuration

The original STP uses a long time to recalculate paths after a topology change. Because of the growing use of larger switched networks, this has become a potential reason for performance degradation in certain cases. Rapid STP is one of several attempts to improve on this issue. The ONS15302 and ONS15305 support only a partial RSTP implementation which offers the same type of service as, for example, PortFast on Cisco equipment, because RSTP does not support the actual creation of a spanning tree among the bridges. It will however get the ports facing customers to Forwarding mode without having to wait for 2 x Forwarding delay as is the case with the original STP. The regular STP must be running to prevent loops in network. RSTP is to be used only on ports facing end-user equipment. If the ONS15302 or ONS15305 detects normal STP BPDUs on an interface configured for RSTP it will switch back to normal STP for that interface.

Due to the partial implementation, only the Port-Table and its commands are operational at the first release of the ONS 15302 and the ONS 15305.

## 7.3.1 Configure RSTP on a Port

- 
- Step 1** Click on the ONS 15305 managed object, and then on the **Bridge** managed object in the topology browser.
- Step 2** Click on the **RapidSpanningTree** attribute, and then on the **RapidSpanningTreePort** attribute in the attribute window.
- Step 3** Identify the (vlanId, port) pair for which the RSTP is to be configured.



---

**Note** vlanId is relevant only if the network element is running STP per VLAN. If STP per device is run, RSTP can be enabled per port only, and vlanID is always set to 1.

---

- Step 4** Set the status attribute to true for the selected pair.
- Step 5** Click **Save**.
- 

## 7.4 MAC Multicast

Multicast is a method of sending one packet to multiple destinations. Multicasting is used for applications such as video conferences, and for distribution of certain information like some routing protocols. A standard IEEE 802.1D bridge will forward multicast frames on all ports that are members of the same VLAN as the port receiving such frames. This might not be desirable if there is a lot of multicast traffic being transported through a multi-port bridge where the recipients are connected on only one (or a few) of the bridge ports. To alleviate unnecessary bandwidth consumption, the ONS15302 and ONS15305 supports specific tables to control the forwarding of Multicast traffic if desired. Both devices also support IGMP (Internet Group Management Protocol) snooping which is used to update the multicast tables based on the IGMP messaging between end nodes and IP multicast routers.

Note that multicast traffic will be forwarded as usual if this feature is not enabled; the use of these tables are only necessary for performance tuning.

### 7.4.1 Configuring MAC Multicast

The Multicast menu has the following menu options:

- IGMP Snooping
- MacMulticastEnable
- MulticastForwardUnregistered.
- MulticastForwarding.
- MulticastForwardingAll.
- MulticastStatic

The parameter MacMulticastEnable is for enabling/disabling of the MAC Multicast control tables.

### 7.4.1.1 MulticastForwarding

The Forwarding-Table contains multicast filtering information configured into the bridge, or information learned through IGMP Snooping. The Forwarding-Table information specifies the allowed egress ports for a given multicast group address on a specific VLAN, and indicates for which ports (if any) this information has been learnt from IGMP snooping.

**VLAN-TAG-ID:** Identifies the VLAN to which the filtering information applies.

**MULTICAST-ADDRESS:** Identifies the destination group MAC address to which the filtering information applies.

**EGRESS-PORTS:** Indicates the configured egress ports for the specified multicast group address. This does not include ports listed in the Forward All Ports list for this address.

**LEARNT:** Indicates a subset of ports from the Egress Ports list which were identified by IGMP Snooping and added to the multicast filtering database.

### 7.4.1.2 MulticastForwardingAll

The Forward-All-Table allows ports in a VLAN to forward all multicast packets.

**VLAN-TAG\_ID:** Identifies the VLAN to which the filtering information applies.

**EGRESS-PORTS:** Specifies which ports on a VLAN can participate in a Forward Unregistered group. The default setting is all ports.

**FORBIDDEN-PORTS:** Specifies which ports on a VLAN are restricted from participating in a Forward All group.

**STATIC PORTS:** Indicates if the egress ports are static or dynamic configured.

### 7.4.1.3 MulticastForwardUnregistered

The Multicast-Forward-Unregistered-Table defines the behavior of ports regarding forwarding of packets that is not covered by any of the other tables.

**VLAN-TAG\_ID:** Identifies the VLAN to which the filtering information applies.

**EGRESS-PORTS:** Specifies which ports on a VLAN can participate in a Forward Unregistered group. The default setting is all ports.

**FORBIDDEN-PORTS:** Specifies which ports on a VLAN are restricted from participating in a Forward Unregistered group.

**STATIC PORTS:** Indicates if the egress ports are static or dynamic configured.

### 7.4.1.4 MulticastStatic

The Static-Table contains manually configured filtering information for specific multicast group addresses. This includes information about allowed and forbidden egress ports, and is also reflected in the Forwarding-Table.

**VLAN-TAG\_ID:** Identifies the VLAN to which the filtering information applies.

**MULTICAST-ADDRESS:** Identifies the destination group MAC address of a frame to which the filtering information applies.

**STATIC-EGRESS-PORTS:** Indicates a set of ports to which packets received from, and destined to, are always forwarded. This is regardless of the IGMP Snooping setting.

**FORBIDDEN-PORTS:** Indicates the set of ports to which packets received from and destined to a specific port must not be forwarded. This is regardless of the IGMP Snooping setting.

**STATUS:**

The possible values are:

**Permanent**—The table entry is currently in use. When the bridging status is reset this table entry remains in use.

**Delete on Reset**—This table entry is currently in use. However, when the bridging status is reset the entry is deleted

**Delete on Timeout**—This table entry is currently in use. However when the bridge times out the entry is deleted.

## 7.5 Traffic Control

The TrafficControl menu has the following menu options:

- PortPriority
- PriorityGroup
- TrafficClass

### 7.5.1 PortPriority

**BridgePortNumber:** a port number identifying a port on the device. For each row, the information in the row applies to the port identified in this column.

**DefaultPriority:** this is the priority value assigned to frames arriving at this port, when implicit priority determination is used. Any frames arriving at this port, not carrying a priority value in a tag, will get the DefaultPriority value as priority. The value is an IEEE 802.1p priority level. Range is 0 – 7, inclusive.

**NumberOfTrafficClasses:** gives the number of classes of service – that is, the number of output queues, for the port. All ports on the device will always use 4 queues.

### 7.5.2 PriorityGroup

**BridgePortNumber:** a port number identifying one of the on the device. For each row, the information in the row applies to the port identified in this column.

**PriorityGroup:** indicates which ports are located on the same module, and are thus using the same priority configuration. The ONS 15305 has a teoretical maximum of 65 ports, which are all listed in this table whether or not they are present. PriorityGroup 32 indicates that the port is not present (i.e. the corresponding slot holds a STM-n module which has no Ethernet interfaces).

## 7.5.3 TrafficClass

Classification of Ethernet frames is done according to the information in the TrafficClass table. The device uses four queues for differentiating traffic; the eight priorities defined by 802.1p must be mapped into those four queues. The default mapping scheme is as recommended by IEEE, but this is configurable by the operator.

Priority Level	Class of Service
6, 7	3
4, 5	2
0, 3	1
1, 2	0

Recommended mapping when using four queues.

**BridgePortNumber:** a port number identifying one of the on the device. For each row, the information in the row applies to the port identified in this column.

**Priority:** priority value according to 802.1p. Legal values 0-7.

**TrafficClass:** indicates which service queue the selected priority value is to be mapped to. Legal values 0-4 (4 is highest priority).

## 7.6 Manage VLANs

This section explains how to manage a VLAN on the network element.

A network element can be configured to run either VLAN per port or VLAN per port and per protocol.

The section also involves management of the complete life cycle of a VLAN, including:

- Creation, presentation, modification, and deletion of a VLAN.
- Creation, presentation, modification, and deletion of an Ethernet User Defined Protocol.
- Presentation and modification of Generic Attribute Registration Protocol VLAN Registration Protocol (GVRP).

### 7.6.1 Virtual Local Area Networks (VLAN)

A LAN consists of a number of computers that share a common communication line within a small geographical area. A Virtual LAN is a LAN where the grouping of computers are based on logical connections, for example by type of users, by department etc. It is easier than for a physical LAN to add and delete computers to/from a VLAN and to manage load balancing. The management system relates the virtual picture and the physical picture of the network.

The network element supports two types of VLAN

- Per port
- Per port and protocol

Both types of VLANs cannot be run simultaneously on the network element, that means either all VLANs per port or all per port and per protocol. The protocol can either be one from a set of predefined protocols or from Ethernet protocols defined by you. Different Ethernet protocol types can be IP, IPX, Appletalk, etc.

The number of Ethernet-ports in ONS15305 which can be assigned to a VLAN, is limited to 64. The maximum number of Ethernet-ports per slot is 16. See also the “[Question 7](#)” section on page A-2.

There are three steps involved in the definition of VLAN on the network element.

- A common VLAN type is defined for the Bridge.
- A set of common parameters for a new VLAN is defined.
- New ports can be added to a VLAN.

It is assumed you have the appropriate rights to perform management operations.

## 7.6.2 Tagged/Untagged LAN Ports

In order to transport traffic from multiple VLANs over the same LAN port (from one bridge to another) the Ethernet frames must be tagged according to what VLAN they belong to, so that the connected bridge knows what frames are to be forwarded into which VLAN (This is according to the IEEE spec 802.1Q). This is done by inserting four bytes into the Ethernet frame header, with information about the VLAN ID (VID) the frame is associated with. The VID of a specific VLAN is defined at the time the VLAN is created. This tagging can be enabled for each port in a VLAN. This is, however, only used for communication between bridges (and in some cases VLAN aware servers), and not on ports facing regular end user network equipment. A LAN port operating in untagged mode will discard tagged frames on ingress. LAN ports operating in tagged mode will only accept frames tagged in accordance with the VID of the VLAN(s) of which the port is a member.

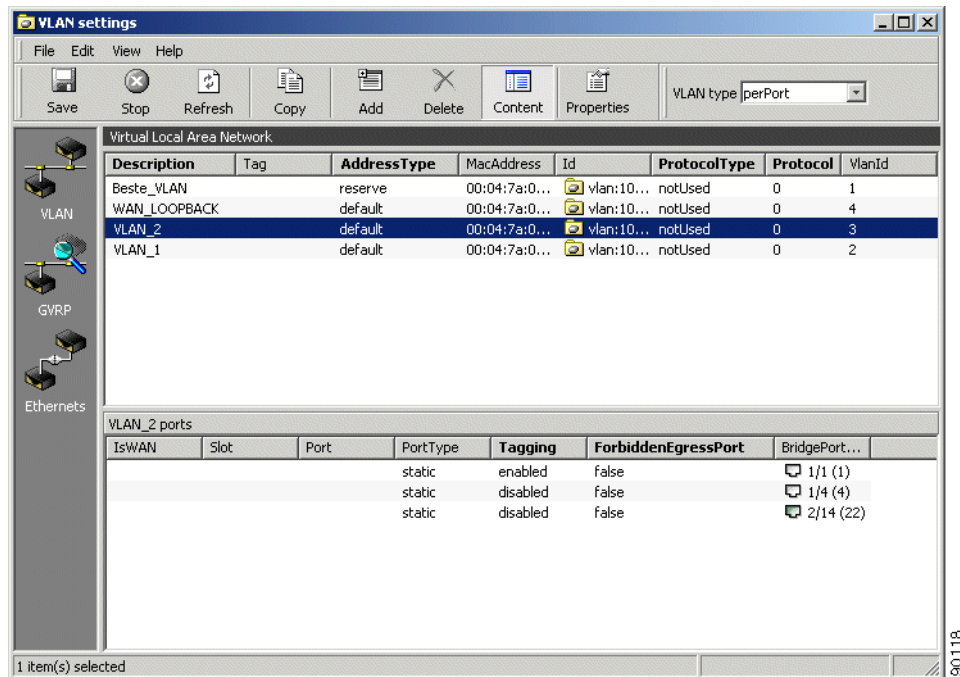
For example, if a port is member of two VLANs with the VIDs of 10 and 20, and the port receives frames tagged according to VID 10, 20 and 30, only the frames with VID 10 and 20 will be accepted and forwarded. The frames with VID 30 will be discarded.

It is possible to have a VLAN where some of the member ports are tagged while others are not. As long as there is traffic from only one VLAN passing through a port, there is no need to enable tagging.

## 7.7 VLAN Provisioning

Cisco Edge Craft has a custom GUI for VLAN provisioning ([Figure 7-4](#)). The VLAN GUI makes VLAN related configuration easier for the user by grouping together a number of managed objects and attributes under a unique GUI.

Figure 7-4 VLAN GUI - Overview



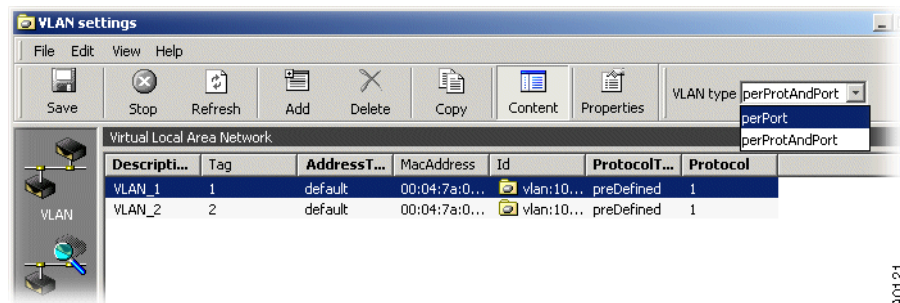
The following examples show how a VLAN perport and per protocol can be created and provisioned by using the custom GUI. The VLAN custom GUI can be opened either by clicking on VLAN Setting under the Bridge menu on the Cisco Edge Craft desktop, or by right-clicking on Bridge MO in the topology browser and then selecting VLAN Setting.

## 7.7.1 Configure a New VLAN Per Port

Use the following steps to create a new VLAN per port.

- Step 1** Verify that the VLAN type on the top right corner of the GUI is set to perPort (Figure 7-5). If not, set **VLAN type** to **perPort** and click **Yes** when asked if the network element should be rebooted.

Figure 7-5 VLAN Settings



- Step 2** Click **Add** in the GUI (Figure 7-6).

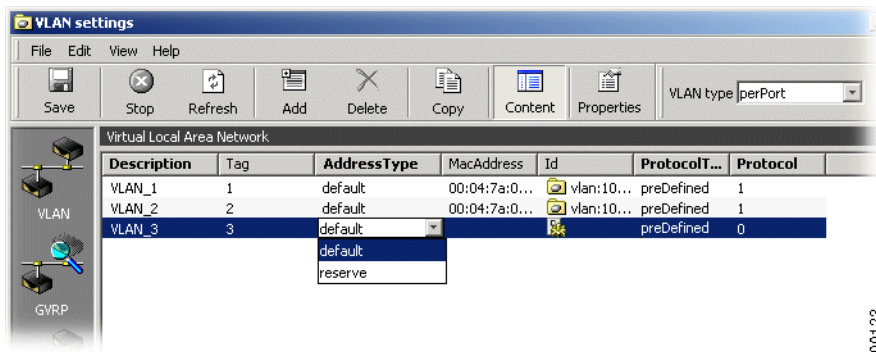


Figure 7-6 Add a VLAN



**Step 3** The GUI suggests default values for all the attributes. Edit the description, tag, and/or addressType attributes if required (Figure 7-7).

Figure 7-7 Set VLAN Attributes

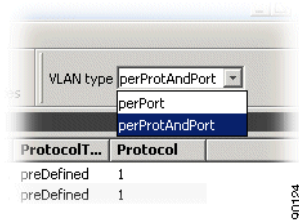


**Step 4** Click **Save**.

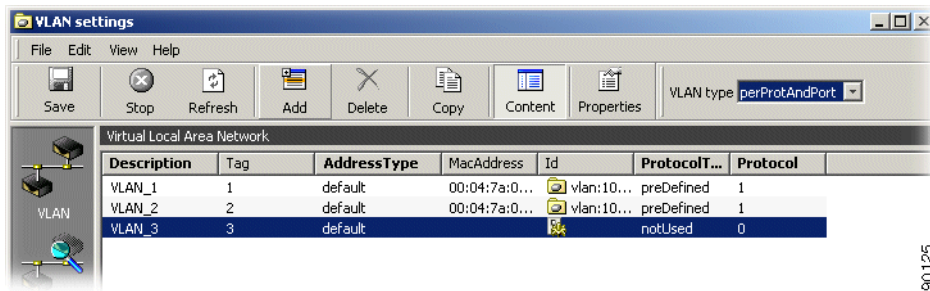
## 7.7.2 Configure a New VLAN Per Protocol and Per Port

Use the following steps to create a new VLAN per protocol and per port.

- Step 1** Verify that the VLAN type on the top right corner of the GUI is set to **perProtAndPort**. If not, set **VLAN type** to **perProtAndPort**, and click **Save**. The network element must be restarted before the change is effective.
- Step 2** Click **Add** on the GUI, Figure 7-8.

**Figure 7-8 Add a VLAN**

- Step 3** Edit the protocolType and protocol attributes to indicate which protocol will be used to determine the VLAN membership of a packet. The user can choose between nine pre-defined protocols, and one Ethernet user defined protocol.

**Figure 7-9 Configure a VLAN****Note**

If protocolType is set to notUsed, and protocol to zero, a VLAN per port is basically defined, that means the protocol carried by a packet does not influence its membership in a VLAN.

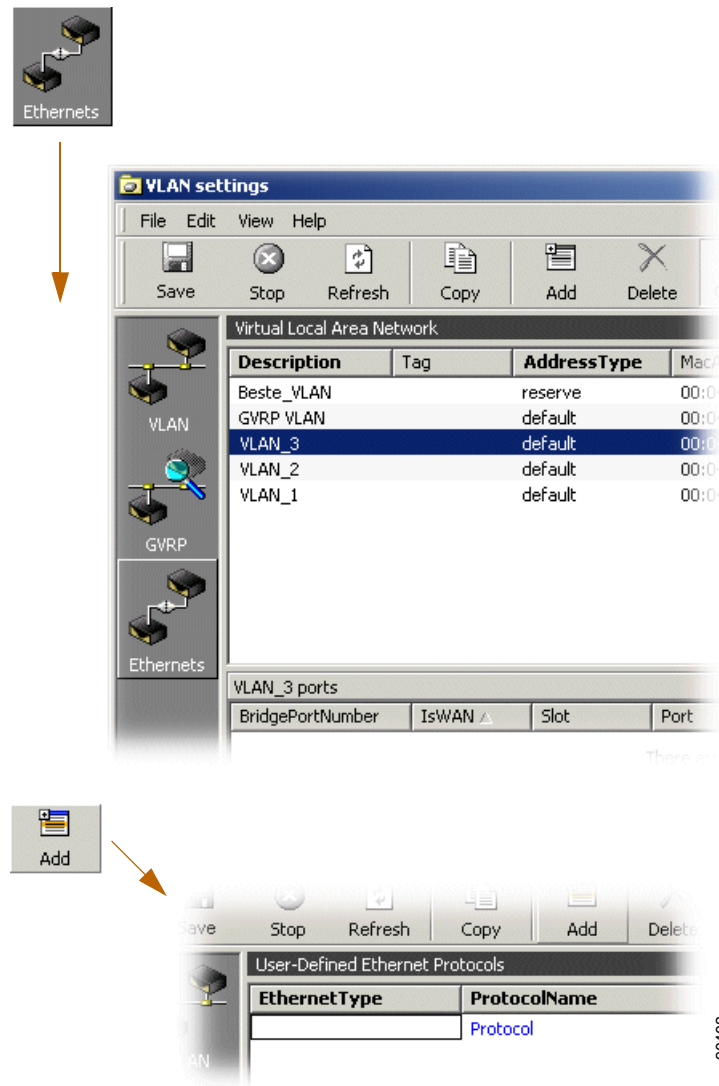
## 7.7.3 Configure an Ethernet User Defined Protocol

### 7.7.3.1 Use the Ethernet User Defined Protocol

The ethernetDefinedProtocol attribute allows you to define a non-predefined protocol based on the etherType field of Ethernet frames. This user-defined protocol is further used to create protocol-based VLANs (Figure 7-10).

- Step 1** Select **VLAN Settings** from the **Bridge** menu.
- Step 2** Click **Ethernets** in the content pane.

Figure 7-10 Configuration of an Ethernet User Defined Protocol



- Step 3** Click **Add** on the toolbar (if no protocol is already defined). If a protocol is already defined, both fields described in [Step 4](#) can be directly edited.
- Step 4** Set the EthernetType attribute to the value of the EtherType indicating the required protocol. The ProtocolName attribute can optionally be used to give a user-friendly name to the protocol.
- Step 5** Click **Save** on the toolbar.



**Note** The EtherType numbers are maintained by the internet assigned numbers authority (IANA), and can be accessed on the Web at the following address:  
<http://www.iana.org/assignments/ethernet-numbers>.

Assuming that a user wants to define a VLAN based on the address resolution protocol (ARP), the ethernetType must be set to 0806 (in hex), and the protocolName attribute could be, for example set to ARP to identify the protocol.

The Ethernet user defined protocol is relevant only when the network element runs VLAN per protocol and port.

Maximum one Ethernet user defined protocol can be currently defined on the network element.

To use the Ethernet user defined protocol as a VLAN protocol for a particular VLAN, set the `protocolType` attribute under Bridge > VLAN to `ethUserDefined`. The `protocol` attribute under Bridge > VLAN, which is used to identify a specific protocol, must then always be set to 1, since there is maximum one Ethernet user defined protocol.

### 7.7.3.2 Use Pre-defined Protocols

**Step 1** Set `protocolType` to `preDefined`.

**Step 2** Set `protocol` to 1 for other, that means the VLAN will include any protocol except the one specified in [Table 7-1](#).

**Table 7-1 VLAN Protocol**

2	for IP protocol
4	for IPX Raw protocol
5	for IPX Ethernet protocol
6	for IPX LLC protocol
7	for IPX SNAP protocol
8	for DECNET protocol
10	for NETBIOS protocol
13	for SNA protocol

**Step 3** Edit the description, tag, and/or `addressType` attributes if required.

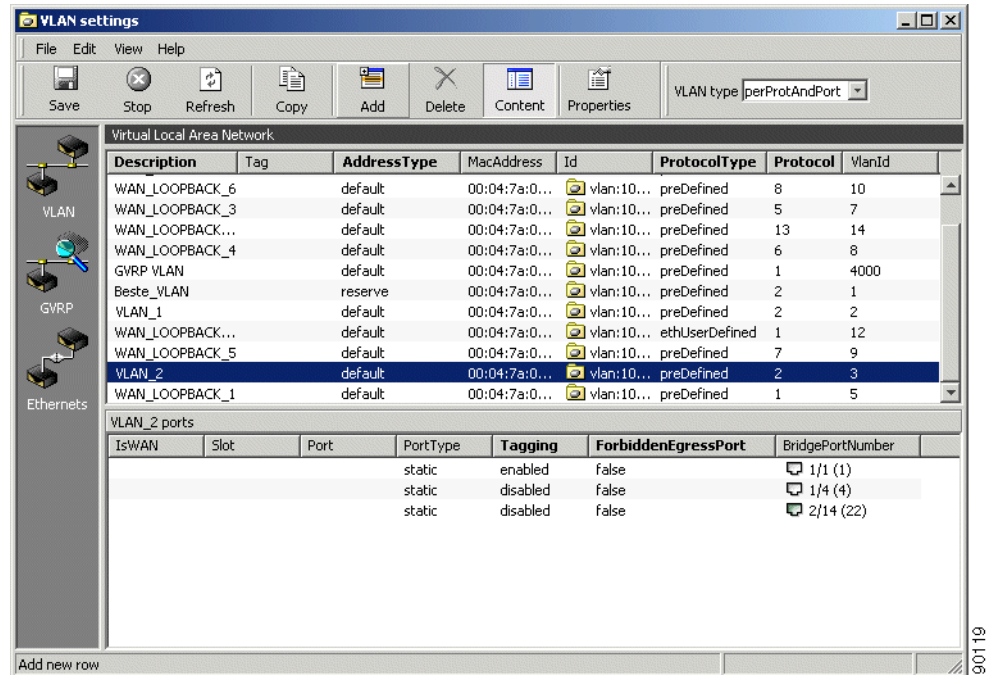
**Step 4** Click **Save**.

### 7.7.4 Configure VLAN Port members

Use the following steps to add port members to an existing VLAN.

**Step 1** Select the VLAN to which ports will be added. The VLAN is highlighted in the virtual local area network window (top window in [Figure 7-11](#)). The list of ports already members of the VLAN is displayed in the VLAN ports window (bottom window in [Figure 7-11](#)).

Figure 7-11 Configuration of VLAN Port members

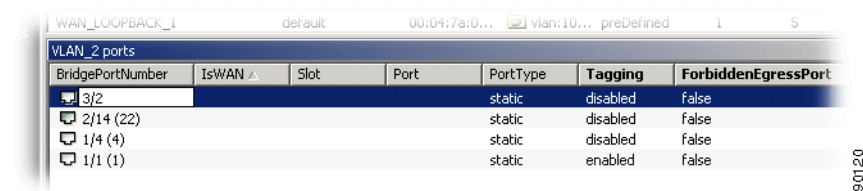


- Step 2** Activate the VLAN ports window by clicking anywhere in the window. The color of the title bar for the VLAN ports window changes to blue to indicate that the window is selected.
- Step 3** Click **Add**.
- Step 4** Edit the bridgePortNumber attribute. The attribute is displayed as slot/port (bridgePortNumber) and can be entered by the user as slot/port or bridgePortNumber (the system will update the display automatically).



**Note** The value of bridgePortNumber for LAN and WAN ports can be found under the LAN and WAN managed objects respectively.

Figure 7-12 Edit the Bridge Port Number



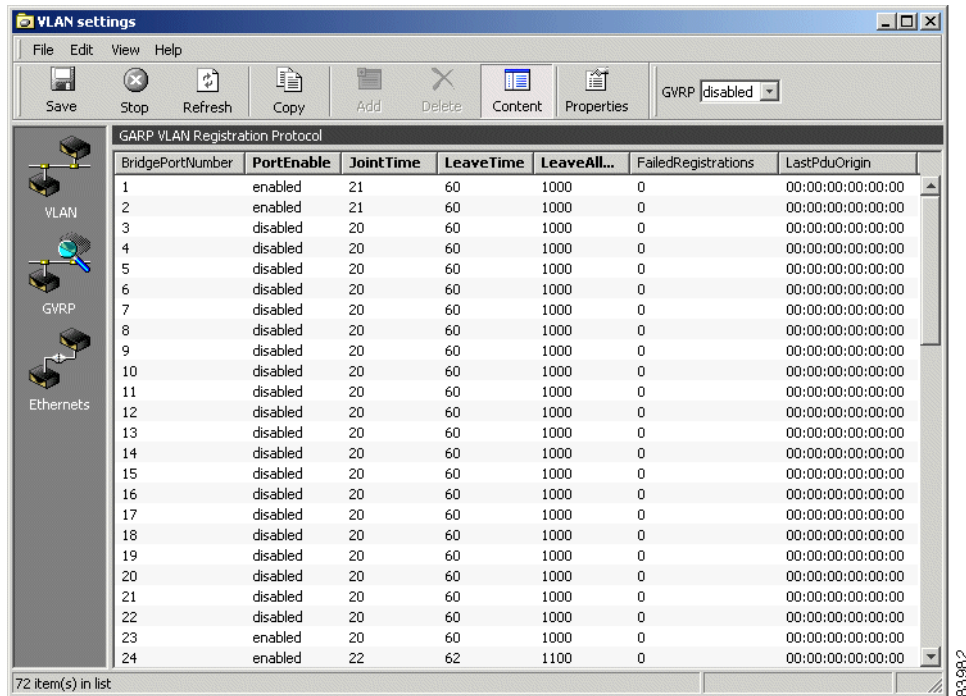
- Step 5** Edit the tagging and forbiddenEgressPort attributes if required.
- Step 6** Click **Save**.

## 7.7.5 GVRP

Use the following steps to modify GARP VLAN registration protocol (GVRP).

- Step 1** Click **GVRP** in the Content pane (Figure 7-13).

**Figure 7-13 GVRP Attributes**

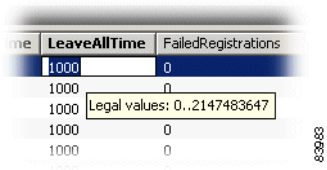


- Step 2** Edit the following attributes as needed:

- PortEnable  
Set to enabled or disabled.
- JointTime  
Set value in centiseconds.
- LeaveTime  
Set value in centiseconds.
- LeaveAllTime  
Set value in centiseconds.

- Step 3** To view legal time values, click in an attribute cell and focus the mouse pointer over the cell. A tooltip will display legal value range for the selected attribute (Figure 7-14).

Figure 7-14 Select Legal Time Values



# 7.8 Examples

This section provides examples for configuring an IP interface, configuring a static route, and configuring an RIP filter.

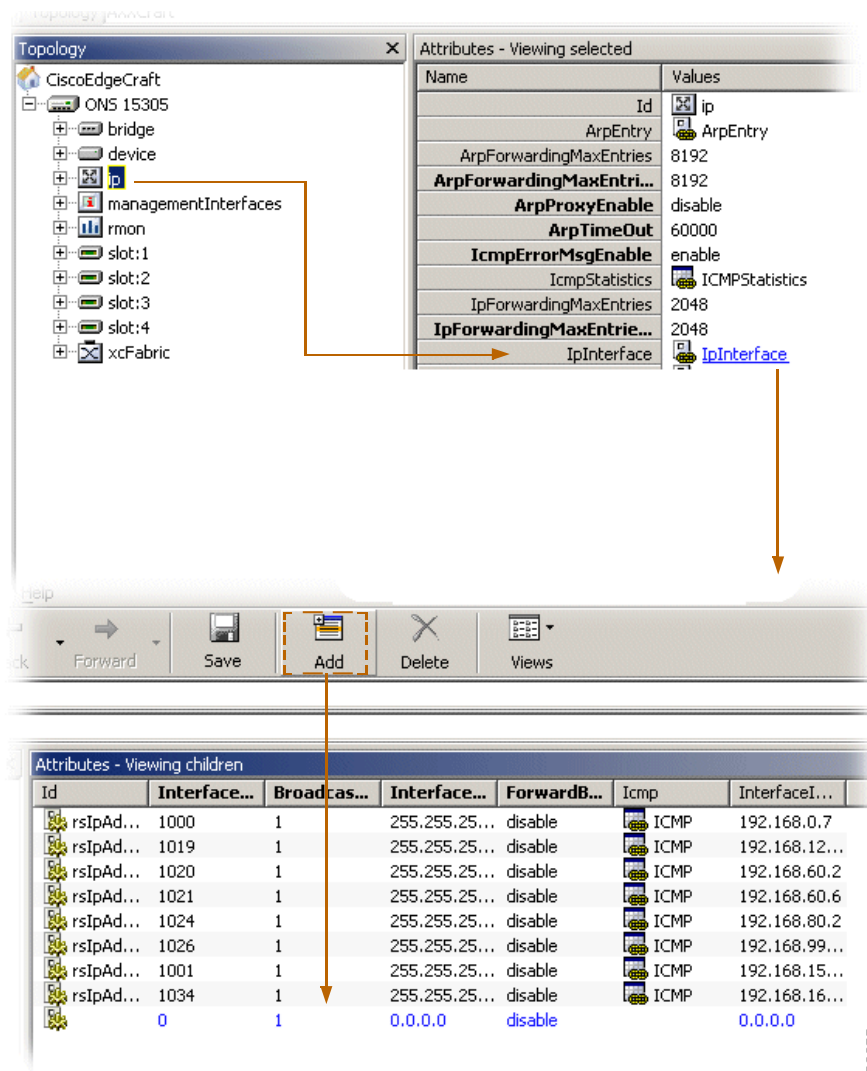
## 7.8.1 Configuration of an IP Interface

An IP interface can be created only for a physical port, a management interface, or a VLAN (port based VLAN or IP-based VLAN only).

The following steps configure an IP interface with an IP address (Figure 7-15).

- Step 1** Click on the ONS 15305 managed object, and then the **ip** managed object in the topology browser.
- Step 2** Double-click on **IpInterface** in the attributes window.
- Step 3** Click **Add** on the toolbar.

Figure 7-15 Configuration of an IP Interface



**Step 4** The following attributes have no default values, and must therefore be defined:

- **interfaceIpAddress**  
set the IP address according to your addressing plan.
- **interfaceNetworkMask**  
set the network mask according to your addressing plan.
- **interfaceNumber**  
the interface number. An IP interface can be defined for a LAN port, a WAN port, the management port, a DCC running IP or a VLAN. The interface number corresponding to these objects is specified by the `ifIndex` attribute present under their respective M.O.

**Step 5** Click **Save** on the toolbar.



**Note**

One interface (identified by a specific ifIndex) can be allocated several IP addresses. This enables the user to connect the interface to a network segment where multiple subnets are defined.

IP addresses and network masks associated with the management interfaces, that means the management port, and the DCC can also be edited via the management interfaces M.O.

## 7.8.2 Configuration of a Static Route

An IP static route is a route defined by the user through the management system. Such a route does not age out, and will stay in the network element routing table as long as it is not explicitly deleted by the user. As any other route, a static route is active, and therefore included in the forwarding table provided that the interface associated with the route is up.

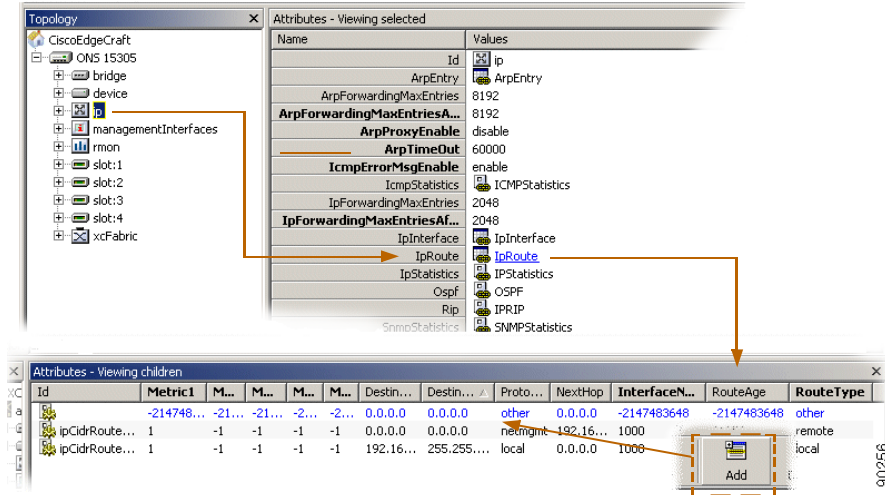
**Note**

The forwarding table is a subset of the routing table. It contains only the active routes, that means routes being used by the network element to forward IP datagrams. Typically, a route becomes inactive, and is removed from the forwarding table when the operational status of its associated interface is down. Only the forwarding table is visible in the Cisco Edge Craft via the ipRoute attribute.

### 7.8.2.1 Create a Static Route

- Step 1** Click on the ONS 15305 managed object, and then on the **IP** managed object in the topology browser, [Figure 7-16](#).
- Step 2** Double click on the **ipRoute** attribute in the attributes window.
- Step 3** Click **Add** on the toolbar.

Figure 7-16 Create a Static Route



- Step 4** Set the destinationIpAddress, destinationNetworkMask, nextHop, interfaceNumber attributes.
- Step 5** Set the **routeType** attribute to either **Remote** if the route is meant to forward traffic, or **Reject** if the route is meant to discard traffic for the specified destination.
- Step 6** Optionally, one or more metric attributes can be set. Metrics are used by the routing process to select a preferential route (the route with the lowest metric) if there are several possible routes for a given destination.
- Step 7** Click **Save** on the toolbar.

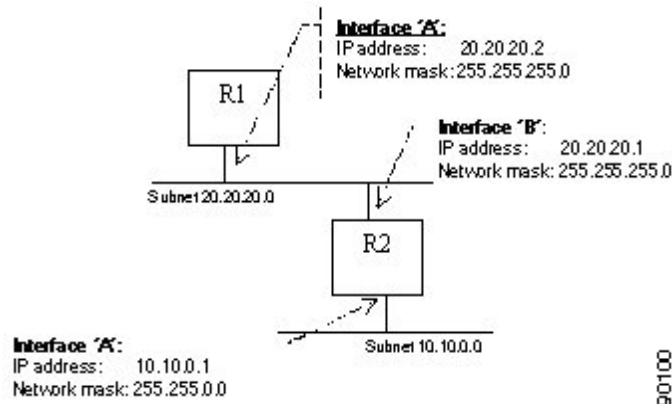
**Note**

The value x set to the destinationNetworkMask attribute will be rejected by the network element if the bitwise logical-and of x with the value of the destinationIpAddress attribute is not equal to the value of the destinationIpAddress attribute.

The IP address of the next router en route specified by the next-hop attribute must be directly reachable via the interface specified by the interfaceNumber attribute, that means the next-hop IP address must belong to the (one of the) subnet(s) defined for the interface identified by the interfaceNumber attribute.

### 7.8.2.2 Static Route Example

To define a static route to the subnet 10.10.0.0 in router R1 (Figure 7-17).

**Figure 7-17** Figure - Static Route in Router R1

- 
- Step 1** Set destinationIpAddress: 10.10.0.0
  - Step 2** Set destinationNetworkMask: 255.255.0.0
  - Step 3** Set nextHop: 20.20.20.1 (one must choose the IP address of router R2 which lies on the same subnet as the interface identified by the interfaceNumber attribute in R1)
  - Step 4** Set interfaceNumber: ifIndex associated with interface A.
  - Step 5** Set routeType: Remote
  - Step 6** Set metric: 1
- 

### 7.8.2.3 Configuration of a Default Route

A default route is a particular static route which is used to by the network element to send all the traffic for which no other routing information exists. If no default route has been defined, and no specific routing information exists for an IP datagrams requesting forwarding, the datagram is discarded.

The default route is created by setting both the destinationIpAddress and the destinationNetworkMask attributes to 0.0.0.0. The router identified by the next-hop attribute is then referred to as default router, also know as default gateway.



**Note**

There exists only one active default route in the network element. The default gateway can also be edited via the Management Interfaces M.O.

### 7.8.2.4 Default Route Example

To create a default route on router R1 using router R2 as default gateway ([Figure 7-17](#)).

- 
- Step 1** Set the destinationIpAddress: 0.0.0.0
  - Step 2** Set the destinationNetworkMask: 0.0.0.0
  - Step 3** Set the nextHop: 20.20.20.1

- Step 4** Set interfaceNumber: ifIndex associated with interface 'A'.
  - Step 5** Set routeType: Remote
  - Step 6** Set metric: 1
- 

## 7.8.3 Configuration of a RIP Filter

An IP RIP filter allows the user to control the propagation of RIP routing information, and eventually to modify the RIP routing by filtering out information about specific routes. In addition, IP RIP filters help reducing the size of the RIP table allowing for a faster table look-up, and releasing memory for other processes.

### 7.8.3.1 Create an IP RIP Global Filter

- Step 1** Click on the ONS 15305 or ONS 15302 managed object, and then on the **IP** managed object in the topology browser.
  - Step 2** Double click on the **rip** attribute in the attributes window.
  - Step 3** Double click on the **ripGlobalFilter** attribute in the attributes window.
  - Step 4** Click **Add** on the toolbar.
  - Step 5** Set the **type**, **networkAddress**, **numberOfMatchBits**, and **filterAction** attributes.
  - Step 6** Click **Save** on the toolbar.
- 

### 7.8.3.2 IP RIP Global Filter Examples

To define a RIP global filter that prevents the network element from advertising any route to the subnet 10.10.0.0, enter the following filter:

Type: output

NetworkAddress: 10.10.0.0

NumberOfMatchBits: 16

FilterAction: Deny

To define a RIP interface filter which prevents the network element from accepting routes for the subnet 192.168.0.0, but still accepts routes for the subnet 192.1680.1.0, enter the following two filters:

#1: Type: input

NetworkAddress: 192.168.0.0

NumberOfMatchBits: 16

FilterAction: Deny

#2: Type: input

NetworkAddress: 192.168.1.0

NumberOfMatchBits: 24

FilterAction: Permit

**Note**

The procedure to define a RIP interface filter is identical to the procedure described above. A RIP interface filter applies only to a specific interface (specified by the ripInterface attribute) instead of applying to every RIP-enabled interface on the network element. RIP interface filters take precedence over RIP global filters.

## 7.9 Open Shortest Path First

The open shortest path first (OSPF) is a link state routing protocol (unlike RIP which is distance vector routing protocol). Configuring the network element to run OSPF can be performed through three basic steps:

- 
- Step 1** Configure one or several OSPF areas.
  - Step 2** Configuring the OSPF interfaces.
  - Step 3** Enable OSPF on the network element.
- 

### 7.9.1 Supported OSPF Areas: Transit and Stub Areas

Three OPSF area types are currently defined by the standards:

- Transit areas (including the backbone area 0.0.0.0) defined in OSPF version 2 (RFC2328). Transit areas accept intra-area, inter-area, and external routes.
- Stub areas defined in OSPF version 2 (RFC2328). Stub areas come in two flavours: they can either accept intra-area, inter-area, and default routes, or only intra-area and default routes. Stub areas which propagate only intra-area and default routes within the area are sometimes referred to as totally-stub areas.
- Not-so-stubby areas (NSSA) defined in OSPF NSSA option (RFC1587). NSSAs are a hybrid between transit and stub areas. They can import a few external routes into the area via an autonomous system border router (ASBR) present in the area.

The network element currently supports only transit and stub areas. In addition, it is currently not possible to configure a stub area to import only intra-are and default routes, tha means it is not possible to configure an area as a totally-stub area.

### 7.9.2 Configure an OSPF Area

Use the following steps to configure a new OSPF area.

- 
- Step 1** Click on the ONS 15305 or ONS 15302 managed object, and then on the **IP** managed object in the topology browser.
  - Step 2** Click on the **OSPF** attribute, and then on the **OspfArea** attribute in the attribute window.

- Step 3** Click **Add**.
- Step 4** Set the **areaID** attribute.
- Step 5** Set the **importAsExternal** and **metric** attributes as required.
- Step 6** Click **Save**.

**Note**

Setting the importAsExternal attribute to importAsExternal define a transit area, while setting the importAsExternal attribute to importNoExternal define a stub area.

**Note**

The metric attribute is only relevant for stub areas, that means when the attribute importAsExternal is set to importNoExternal.

## 7.9.3 Configure an OSPF Interface

Use the following steps to configure an OSPF interface.

- Step 1** Click on the ONS 15305 or ONS 15302 managed object, and then on the **IP** managed object in the topology browser.
- Step 2** Click on the **OSPF** attribute, and then on the **OspfInterface** attribute in the attribute window.
- Step 3** Identify the OSPF interface to configure via its IP address listed under the **interfaceIpAddress** attribute.
- Step 4** Set the **areaId** attribute to the area to which you want to attach the interface. Note that the area must have been previously defined; see the [“7.9.2 Configure an OSPF Area” section on page 7-25](#).
- Step 5** Set the **interfaceType** attribute to the required type, and make sure that the **ospfEnable** attribute is set to **Enabled** (this is the default value).
- Step 6** Edit the **helloInterval**, **metricValue**, **authenticationType**, **authenticationKey**, **transitDelay**, **routerDeadInterval**, **pollInterval**, **retransmissionInterval**, and **priority** attributes if required.
- Step 7** Click **Save**.

## 7.9.4 Enable OSPF on the Network Element

Use the following steps to enable OSPF globally.

- Step 1** Click on the ONS 15305 or ONS 15302 managed object, and then on the **IP** managed object in the topology browser.
- Step 2** Click on the **OSPF** attribute in the attribute window.
- Step 3** Set the **ospfEnable** attribute to **enabled**.
- Step 4** Click **Save**.

## 7.10 DHCP

The network element can be configured as a DHCP server (ONS 15305 > IP > DHCP > dhcpServerEnable set to enable) or as a DHCP relay (ONS 15305 > IP > DHCP > dhcpServerEnable set to disable).

If the network element is configured to relay DHCP requests, the IP address of the next DHCP server must be configured by setting the ONS 15305 > IP > DHCP > **nextServerIpAddress** attribute.

If the network element is configured as a DHCP server, the user can configure the ranges of available IP addresses for every IP interface on the network element; see the [“7.10.1 Configure the Range of IP Addresses for the DHCP Server” section on page 7-27](#). In addition, by using DHCP manual allocation mechanism, the user can define the IP address to be allocated to a host based on its MAC address and optionally its name; see the [“7.10.1.1 Configure the DHCP Server for Manual Allocation” section on page 7-27](#).

### 7.10.1 Configure the Range of IP Addresses for the DHCP Server

Use the following steps to configure the range of IP addresses

- 
- Step 1** Click on the ONS 15305 managed object, and then on the **IP** managed object in the topology browser.
  - Step 2** Click on the **DHCP** attribute, and then on the **dhcpAddressRange** attribute in the attribute window.
  - Step 3** Click **Add**.
  - Step 4** Set the **interfaceIpAddress** attribute to the IP address of the network element on which the range of IP address shall be available.
  - Step 5** Set the **ipAddressFrom** and **ipAddressTo** attributes to the **first** and the **last IP address** allocated for the range respectively.
  - Step 6** Edit the **leaseTime**, **defaultRouter**, and **probeEnable** attributes as required.
  - Step 7** Click **Save**.




---

**Note** The range of available IP addresses [ipAddressFrom; ipAddressTo] must be on the same subnet as the IP address of the interface (interfaceIpAddress) on which the range applies.  
If you want to allocate IP address permanently, that means to use the automatic allocation mode of DHCP, the leaseTime attribute must be set to -1.

---

#### 7.10.1.1 Configure the DHCP Server for Manual Allocation

Configure an IP address for manual allocation

- 
- Step 1** Click on the ONS 15305 managed object, and then on the **IP** managed object in the topology browser.
  - Step 2** Click on the **DHCP** attribute, and then on the **dhcpAllocation** attribute in the attribute window.
  - Step 3** Click **Add**.
  - Step 4** Set the **ipAddress** attribute to the IP address to be allocated via the manual allocation mode of DHCP.
  - Step 5** Set the **mechanism** attribute to **manual**.
  - Step 6** Edit the **macAddress**, **hostName**, **defaultRouter**, **configurationServerIpAddress**, and **configurationFileName** attributes as required.

**Step 7** Click **Save**.

**Note**

To match any incoming MAC address, the macAddress attribute must be to “00:00:00:00:00:00”.





# Performance Management

This chapter provides current and historical G.826 performance data for the SDH paths and section termination points and current values of the various counters available in the network element.

To clear all PM data on the network element, see the [“4.3.10 Logs \(Alarm Logs, Performance Data Logs\)”](#) section on page 4-18.

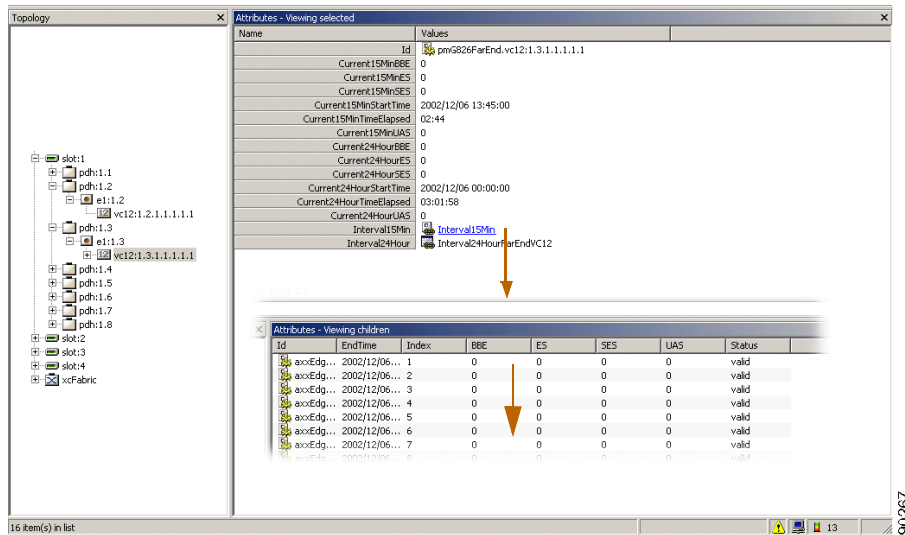
## 8.1 G.826 Performance Monitoring Data

In the topology browser you can select all managed objects that have G.826 performance data ([Table 8-1](#)).

**Table 8-1** *Managed Objects*

Parameter	Description	Objects
RS	Regenerator Section	near end
MS	Multiplex Section	near end and far end
VC-3	Virtual Container 3	near end and far end
VC-4	Virtual Container 4	near end and far end
VC-12	Virtual Container 12	near end and far end

Figure 8-1 View PM - Example



Managed objects have PM attributes as defined in the information model (Figure 8-1).

Available time periods are:

- 15 minutes
- 24 hours

The system presents current data and historical data. The number of historical stored periods are:

- 16x15 minutes
- 1x24 hours

See also the “5.3.7 Monitor PDH Port Performance” section on page 5-11 and the “5.5.9 Monitor WAN Port Performance” section on page 5-25.

## 8.2 Counters

You can use the topology browser to view all managed objects that are monitored objects. These managed objects are:

- LAN ports
- WAN ports
- Bridge
- IP
- RMON

## 8.3 Criteria for Counting Valid-data in the ONS 15305

Criteria for PM counters: for disabled ports, there is no PM-counting (all BBE, ES, SES, UAS have value 0), valid-data flag not affected (data is set as valid if conditions mentioned below are fulfilled).

For Valid-data flag (used for previous 15-min/24-hour intervals) the following rules apply:

The flag will not be set for any 15-min period (for any levels) if 600 seconds (10 minutes) or less are counted (since counter-reset or device-reset).

- The flag will not be set for any 24-hour period (for any levels) if 20 hours or less are counted (since counter-reset or device-reset).
- For RS/MS/VC-4 levels the flag will not be set for any 15-min if the STM-n port was not defined at the beginning of the period (defined meaning that STM-n port was expected in that slot/port position).
- For RS/MS/VC-4 levels the flag will not be set for any 24-hour period if rule 3) was true for 80 15-min intervals (20 hours) or less.
- For VC-4 level the flag will not be set for any 15-min period if the AUG-1 is not structured as AUG\_AU4\_TO\_XC or AUG\_TUG3x3 at the beginning of the period.
- For VC-4 level the flag will not be set for any 24-hour period if rule 5) was true for 80 15-min intervals (20 hours) or less.

In all other cases the valid-data flags are set to

- RS-level valid-data: rules 1,2,3,4
- MS-level valid-data: rules 1,2,3,4
- VC-4-level valid-data: rules 1,2,3,4,5,6
- E3-(/VC-3-) valid-data: rules 1,2
- E1(/VC-12-) valid-data: rules 1,2
- WAN (/VC-12-) valid-data: rules 1,2





## Troubleshooting and FAQ

---

Question one covers troubleshooting and FAQs from [Chapter 4, "General Management."](#)

Questions two to four cover troubleshooting and FAQs from [Chapter 5, "Traffic Port Management."](#)

Questions six to eleven cover troubleshooting and FAQs from [Chapter 7, "Layer 2 Configuration."](#)

### Question 1

- Q.** I cannot configure the Slot for another module type.
- A.** When the Slot Expected Module attribute is set to a specific module type, the Managed Objects for the expected module type are created in ONS 15305. Likewise, when the Expected Module is already set to a module type and we want to configure the Slot for a different module type, the Managed Objects for the configured module will be deleted before the Managed Objects for the new module type can be created.
- In order to avoid unintentional traffic breaks, ONS 15305 checks whether the existing configured module is involved in cross-connections, carrying management traffic or is used for synchronization purposes.

### Question 2

- Q.** Why should I set the Path Trace Identifier attributes?
- A.** You do not have to set the Path Trace Identifier attributes, but it is a very useful tool for checking the connectivity of complex networks. Basically a Path Trace Identifier is inserted at the beginning of a path and extracted at the end of a path. By setting Path Trace Transmitted to a logical value, for example BONN-3-21 you can easily see if this value is received on the other side of the network. If you enter a value for the Path Trace Expected value and enable Path Trace, a TIM alarm will be triggered if the received value is different from the transmitted value.

### Question 3

- Q.** What is a WAN port?
- A.** WAN ports perform the mapping between a traditional Lan Port and the SDH network. The WAN port is an internal interface in ONS 15305.

## Question 4

- Q.** Why does a WAN port have 50 channels when I can achieve the maximum capacity of 100 Mbit/s using 47 channels?
- A.** The WAN port is mapping the ethernet packets into VC12 containers. Each VC12 container always carry 2.16 Mbit/s. However, the mapping process requires some overhead. The overhead will vary with the actual PDU type mapped into the VC12 channels. This means that the bit rate at the Ethernet interface is a bit less than the bit rate of the VC-12 channel. With a certain type of PDUs, 100Mbit/s is achieved using only 47 channels, while some PDUs may require 50.

## Question 5

- Q.** Why is the Mac multicast feature not available in Cisco Edge Craft
- A.** To enable MAC multicast, the user must make sure that the maximum number of VLANs is less than 4000. This is because the maximum number of multicast entries allowed in the network element is fixed by the following equation:

**Figure A-1 VLAN Calculation**

$$(\text{max number multicast entries}) = 4000 - (\text{max number VLANs})$$

Therefore, if the maximum number of VLANs is greater than 4000, no resources can be allocated for MAC multicast entries, and the MAC multicast feature is then disabled.

The maximum number of VLANs is set via the `vlanMaxEntriesAfterReset` attribute (under `Bridge->VlanType`). If this attribute is edited, the network element must be reset before the new value becomes effective.

## Question 6

- Q.** Why is the STP per VLAN (or STP per Device) attribute not available in Cisco Edge Craft.
- A.** Either the `stpPerDevice` or the `stpPerVlan` attribute is available in the Cisco Edge Craft, but both attributes are not available simultaneously. The attribute `stpType` under `Bridge > spanningTree` decides which attribute is available. When the value of the `stpType` attribute is 'perDevice', the `stpPerDevice` attribute is available, and the `stpPerVlan` attribute is not. Reciprocally, when the value of the `stpType` attribute is 'perVLAN', the `stpPerVLAN` attribute is available, and the `stpPerDevice` attribute is not.

The attributes `stpPerDevice` and `stpPerVLAN` allows the user to control the spanning tree process(es) on the network element. The network element can either run one single spanning tree for the whole network element, or one spanning tree per VLAN. The `stpType` attribute is used to indicate which type of spanning tree protocol (per device or per VLN) is currently running. To modify the current type, set the `stpTypeAfterReset` attribute (under `Bridge > spanningTree`) to the desired value, and reset the network element.

## Question 7

- Q.** How many VLAN does the network element support?

- A.** The maximum number of VLANs supported by the network element is configurable by the user, and is indicated by the `vlanMaxEntries` attribute (under `Bridge > VlanType`). The maximum number of VLANs can be set to a new value via the `vlanMaxEntriesAfterReset` attribute (under `Bridge > VlanType`). If this attribute is edited, the network element must be reset before the new value becomes effective. Note that the network element cannot support more than 4000 VLANs.

## Question 8

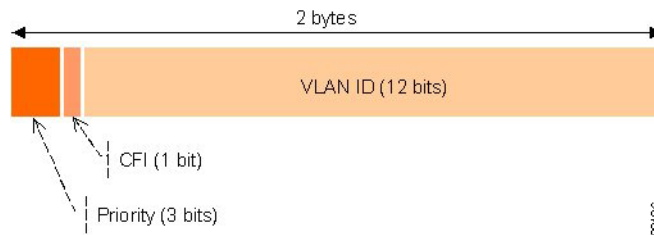
- Q.** What is the VLAN ID?
- A.** IEEE 802.1Q standardizes a scheme for adding additional information, known as VLAN tag, to layer 2 frames in order for a switch to know which VLAN an incoming frame is intended for, and the priority of the frame. The VLAN tag is a two-byte field containing 3 bits for indicating the priority of the frame, 12 bits for indicating the VLAN ID, and 1 bit indicating whether the addresses are in canonical format, [Figure A-2](#).



**Note**

In the standard (IEEE 802.1Q), layer 2 frames carrying both VLAN identification and priority information in a tag are referred to as VLAN tagged frames. Layer 2 frames carrying priority information, but no VLAN identification information are referred to as priority tagged frames.

**Figure A-2 IEEE 802.1Q Tag header (VLAN tag)**



The priority field is interpreted as a binary number, and therefore capable of representing eight priority levels, 0 through 7. The use and interpretation of this field is defined in ISO/IEC 15802-3.

The canonical format indicator (CFI) is a single bit flag value. CFI reset indicates that all MAC address information that may be present in the MAC data carried by the frame is in canonical format.

The VLAN identifier (VLAN ID) field uniquely identifies the VLAN to which the frame belongs. The VLAN ID is encoded as an unsigned binary number. The user can associate any value in the range 1-4095 to a VLAN ID. The value null is reserved for priority-tagged frames, and the value 4096 (FFF in hexadecimal) is reserved for implementation use.



**Note**

Priority tagged frames are layer 2 frames carrying priority information, but no VLAN identification information.

## Question 9

- Q.** How to choose the maximum number of GVRP VLAN?

- A.** The generic attribute registration protocol (GARP) protocol is a general-purpose protocol that registers any network connectivity or membership-style information. GARP defines a set of devices interested in a given network attribute, such as VLAN or multicast address.

The GARP VLAN registration protocol (GVRP) protocol is specifically provided for automatic distribution of VLAN membership information among VLAN-aware bridges. GVRP allows VLAN-aware bridges to automatically learn VLANs to bridge ports mapping, without having to individually configure each bridge, and to register VLAN membership.

To minimize the memory requirements when running the GVRP protocol, two proprietary tuning variables have been added to the standard variables: `gvrpVlanMaxEntries` and `gvrpVlanMaxEntriesAfterReset` which control the number of GVRP VLANs allowed to participate in GVRP operation. The maximum number of GVRP VLANs includes all the VLANs participating in GVRP operation regardless if they are static or dynamic.

The following should be considered when specifying the maximum number of VLANs participating in GVRP by setting the `gvrpVlanMaxEntriesAfterReset` attribute:

- The default maximum number of GVRP VLANs is equal to 0 because of the memory restrictions.
- The maximum number of VLANs (managed through the `bridge> vlanType > maxVlanEntriesAfterReset` attribute) limits the maximum number of GVRP VLANs.
- To ensure the correct operation of the GVRP protocol, users are advised to set the maximum number of GVRP VLANs equal to a value which significantly exceeds the sum of:

The number of all static VLANs both currently configured and expected to be configured.

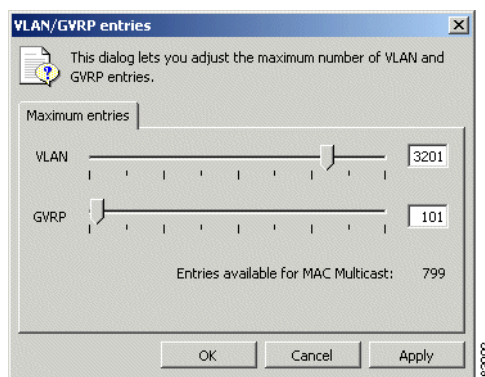
The number of all dynamic VLANs participating in GVRP both currently configured (initial number of dynamic GVRP VLANs is 0) and expected to be configured.

In creasing the value of maximum number of GVRP VLANs to value beyond the sum, allows users to run GVRP, and not reset the device to receive a larger amount of GVRP VLANs. For example, if 3 VLANs exist and another two VLANs are expected to be configured as a result of VLAN static or dynamic registration, set the maximum number of GVRP VLANs after reset to 10.

#### Adjust the maximum number of VLAN and GVRP entries

- Step 1** Click **Properties** in the VLAN Settings window.
- Step 2** The appearing dialog allows you to adjust the maximum number of VLAN and GVRP entries.

**Figure A-3 Adjustment of VLAN/GVRP entries**





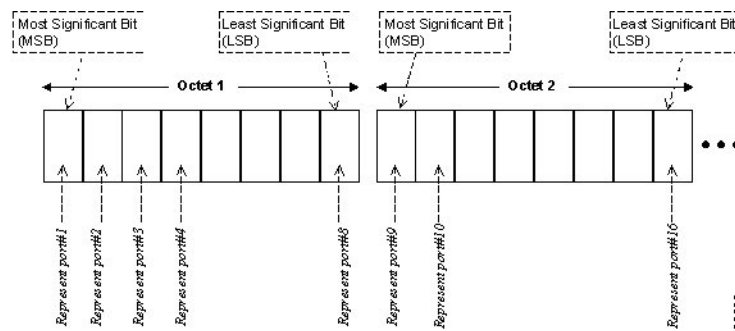

**Note**

To enable GVRP, ensure that the amount of maximum amount of VLANs is less than 4000 (check the bridge > vlanType > maxVlanEntries attribute).

## Question 10

- Q.** How to represent a set of ports with an octet string?
- A.** When an octet string is used to represent a set of ports, each octet within the string specifies a set of eight ports, with the first octet specifying ports 1 through 8, the second octet specifying ports 9 through 16, etc. Within each octet, the most significant bit represents the lowest numbered port, and the least significant bit represents the highest numbered port, [Figure A-4](#). Each port of the bridge is then represented by a single bit within the octet string. If the bit has a value of 1 then the port is included in the set of ports, and the port is not included if the bit has a value of 0.

**Figure A-4 Definition of a Set of Ports Through an Octet String**



[Table A-1](#) presents two examples of octet strings and their corresponding sets of ports.

**Table A-1 Octet String and Corresponding Set of Ports**

Octet String	Binary Representation	Set of port(s)
52	0101 0010	port #2, port #4, and port #7
0c 01	0000 1100 0000 0001	port #5, port #6 and port #16

## Question 11

- Q.** What are the Common UDP Ports?
- A.** The common UDP ports are described in [Figure A-5](#).

**Figure A-5 Common UDP Ports**

UDP Port #	Acronym	Application
37	TIME	Time
42	NAMESERVER	Host Name Server
43	NICNAME	Who Is
53	DOMAIN	Domain Name Server
67	BOOTPS	Bootstrap Protocol Server
68	BOOTPC	Bootstrap Protocol Client
69	TFTP	Trivial File Transfer
111	SUNRPC	Sun Microsystems Rpc
123	NTP	Network time
137	NetBiosNameService	NT Server to Station Connections
138	NetBiosDatagramService	NT Server to Station Connections
139	NetBios SessionService	NT Server to Station Connections
161	SNMP	Simple Network Management
162	SNMP	Simple Network Management Traps
513		Unix Rwho Daemon
514	syslog	System Log
525	timed	Time Daemon

**Q.** What are the different types of Link State Advertisements?

**A.** The different link types are listed in [Table A-2](#).

**Table A-2 Link State Type (according to RFC2328, Appendix A.4.1)**

Link State (LS) Type	Description
1	Router-LSAs
2	Network-LSAs
3	Summary-LSAs (IP network)
4	Summary-LSAs (ASBR)
5	AS-external-LSAs



## **A**

<b>ADM</b>	Add/drop multiplexer
<b>AIS</b>	Alarm indication signal
<b>APS</b>	Automatic protection switching
<b>ARP</b>	address resolution protocol
<b>ASBR</b>	Autonomous system border router
<b>AU-x</b>	Administrator Unit - x

## **B**

<b>BBE</b>	Background block error
<b>BER</b>	Bit error rate

## **C**

<b>CBKLM</b>	Addressing schema for data container
<b>CFI</b>	Canonical format indicator
<b>CLNP</b>	Connection less network protocol
<b>CNLP</b>	Connectionless network rotocol
<b>CPE</b>	Customer premises environment
<b>CTP</b>	Connection termination port
<b>CTS</b>	Clear to send

## **D**

<b>DNU</b>	Do not use
<b>DEG</b>	Degraded signal effect

<b>DCC</b>	Data communications channel
<b>DCN</b>	Data communications network
<b>DHCP</b>	Dynamic host control protocol

## **E**

<b>EMS</b>	Element management system
<b>ETS</b>	European Telecommunications Standard
<b>ETSI</b>	European Telecommunications Standards Institute
<b>ES</b>	Errored seconds

## **F**

<b>FCC</b>	Federal Communications Commission
------------	-----------------------------------

## **G**

<b>GARP</b>	Generic attribute registration protocol
<b>GUI</b>	Graphical user interface
<b>GW</b>	Gateway
<b>GVRP</b>	Generic attribute registration protocol VLAN registration protocol

## **H**

<b>HTML</b>	Hypertext markup language
-------------	---------------------------

## **I**

<b>IANA</b>	Internet assigned numbers authorit
<b>ID</b>	Identifier
<b>IEC</b>	International Electrotechnical Commission
<b>IEEE</b>	Institute of Electrical and Electronics Engineers
<b>IF-DN-0101-R1</b>	Network and service forum (NSIE) standard for IP over DCC

<b>IGMP</b>	Internet group management protocol
<b>IP</b>	Internet Protocol
<b>IPX</b>	Internetwork packet exchange protocol
<b>IS</b>	Intermediate system
<b>ISDN</b>	Integrated services digital network
<b>ISO</b>	International standard organization
<b>ITU</b>	International Telecommunications Union
<b>ITU-T</b>	International Telecommunications Union, Telecommunication standards sector

## **L**

<b>L1 IS</b>	Layer 1 intermediate system
<b>L2 IS</b>	Layer 2 intermediate system
<b>LAP-D</b>	Link access procedure on the D channel
<b>LAN</b>	Local area network
<b>LED</b>	Light emitting diode
<b>LLC</b>	Logical link control layer
<b>LL2/LL3</b>	Local loop 2/3
<b>Log4j</b>	Tool for logging from <a href="http://jakarta.apache.org">jakarta.apache.org</a>
<b>Los</b>	Loss of signal

## **M**

<b>MAC</b>	Medium access
<b>Mbps</b>	Megabits per second
<b>MHz</b>	Megahertz
<b>MIB</b>	Management information base
<b>M.O.</b>	Managed objects
<b>MS</b>	Multiplex section
<b>MSP</b>	Multiplex section protection

## N

<b>NC</b>	not connected
<b>NE</b>	Network element
<b>NET</b>	Network
<b>NMS</b>	Network management system
<b>NSAP</b>	Network Service Access Point
<b>NSSA</b>	Not-so-stubby areas

## O

<b>ONS</b>	Optical networking system
<b>ONSCLI</b>	Optical networking system command line interface
<b>OSPF</b>	open shortest path first

## P

<b>PC</b>	Personal Computer
<b>PDH</b>	Plesiochronous digital hierarchy (ITU-T Rec. G.702)
<b>PIM</b>	Protocol independent multicast
<b>PIM-DM</b>	Protocol independent multicast - Dense mode
<b>PM</b>	Performance monitoring
<b>PPP</b>	Point-to -point protocol
<b>PRC</b>	Primary reference clock

**Q**

<b>QL</b>	Quality Level
<b>QLM</b>	Quality Level minimum

**R**

<b>RFC</b>	Request for comments
<b>RIP</b>	Routing information protocol
<b>RJ-45</b>	Registered jack #45 (8-pin)
<b>RS Layer</b>	Regenerator section layer
<b>RSTP</b>	Rapid spanning tree protocol
<b>RMON</b>	Remote monitoring
<b>Rx</b>	Receive

**S**

<b>SAP</b>	Server advertisement protocol
<b>SASE</b>	Stand alone synchronization equipment
<b>SEC</b>	SDH equipment clock
<b>SES</b>	Severely errored second
<b>SDH</b>	Synchronous digital hierarchy
<b>SNAP</b>	Subnetwork access protocol
<b>SNC</b>	Sub-network connection
<b>SNC/I</b>	Sub-network connection inherent monitoring
<b>SNC/N</b>	Sub-network connection on-intrusive monitoring
<b>SNMP</b>	Simple network management protocol
<b>SNTP</b>	Simple network timing protocol
<b>SSU</b>	Synchronisation supply units
<b>SSM</b>	Synchronisation status message

**STM** Synchronous transport module

**STP** Spanning tree protocol

## **T**

**TAC** Technical Assistance Center

**TCP/IP** Transmission Control Protocol/Internet Protocol

**Trib** Tributary

**TFTP** Trivial File Transport Protocol

**TP** Termination point

**TU** Tributary unit

**Tx** Transmit

## **U**

**UAS** Unavailable seconds

**URL** Uniform Resource Locator (Internet address, including specific document location)

## **V**

**VC-x** Virtual container

**VLAN** Virtual local area network

## **W**

**WTR** Wait to restore

**WAN** Wide area network

**WWW** World Wide Web

## **X**

**XC** Cross connect