



Cisco Edge Craft Software Guide

Software Release 2.0
December 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: 78-xxxxx-xx



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

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

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

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

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

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

- Turn the television or radio antenna until the interference stops.
- Move the equipment to one side or the other of the television or radio.
- Move the equipment farther away from the television or radio.
- Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

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

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

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

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

Cisco Edge Craft Software Guide

CCSP, the Cisco Square Bridge logo, Follow Me Browsing, 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 Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, 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. (0501R)



About This Guide XXIX

CHAPTER 1

Starting the Cisco Edge Craft 1-1

- 1.1 Installation of Cisco Edge Craft 1-1
 - 1.1.1 Uninstall Cisco Edge Craft 1-2
 - 1.1.2 Commissioning of IP Address via VT100 Interface 1-2
 - 1.1.2.1 Commissioning of IP Address via VT100 Interface 1-2
 - 1.1.2.2 Configure Community-Handler 1-5
 - 1.1.2.3 Assign an IP Address 1-6
 - 1.1.2.4 Change Passwords 1-8
 - 1.1.3 IP Unnumbered Mode 1-9
 - 1.1.4 Setting up the element for IP unnumbered, overview 1-10
 - 1.1.4.1 Connect to the element via the serial port 1-11
 - 1.1.4.2 Clear the configuration with ONSCLI 1-11
 - 1.1.4.3 Setting the system mode. 1-11
 - 1.1.4.4 Set an IP address via ONSCLI 1-11
 - 1.1.4.5 Add a user in the community table 1-11
 - 1.1.4.6 Connect to the element with the Management Tree 1-12
 - 1.1.4.7 Configure the DCC interfaces 1-12
 - 1.1.4.8 Create an OSPF area 1-13
 - 1.1.4.9 Assign the OSPF interfaces to the OSPF area 1-13
 - 1.1.4.10 Set LeakStaticRoutes 1-13
 - 1.1.4.11 Enable OSPF globally for the element. 1-13
 - 1.1.4.12 Remove the management port cable. 1-14
 - 1.1.4.13 Verify connectivity 1-14
 - 1.1.4.14 Using the LeakDirectExternalRoutes variable. 1-14
 - 1.1.4.15 Connectivity without OSPF 1-14
 - 1.1.4.16 Changing the IP address 1-15
 - 1.1.5 Set up Connection to a Network Element 1-15
 - 1.1.5.1 Start the Cisco Edge Craft Application on your Computer 1-15
 - 1.1.5.2 Invalid Community String 1-16
 - 1.1.5.3 Non-existent IP Address 1-16
 - 1.1.6 Configuration of VT100 Terminal 1-16
- 1.2 Commissioning Wizard 1-17
 - 1.2.1 Introduction 1-17

1.2.2 Before You Start	1-18
1.2.2.1 Network Element Access And Permissions	1-18
1.2.2.2 Initial set-up	1-18
1.2.2.3 TFTP server	1-18
1.2.2.4 Time protocol	1-18
1.2.3 Basic flow	1-19
1.3 Commissioning Wizard - Step By Step	1-20
1.3.1 Opening The Commissioning Wizard	1-20
1.3.2 Welcome	1-20
1.3.3 Network Element	1-21
1.3.4 Basic Setup	1-21
1.3.4.1 Network Element Information	1-21
1.3.4.2 SNMP Users And Access Rights (Community Table)	1-22
1.3.5 Expected Service Modules	1-23
1.3.6 SDH Synchronization	1-25
1.3.6.1 Edit the SEC (T0) Synchronization	1-25
1.3.6.2 ONS 15305	1-26
1.3.6.3 ONS 15302	1-27
1.3.6.4 Edit 2048 kHz Output (T4) Synchronization	1-27
1.3.7 Alarm Reporting	1-29
1.3.7.1 Power Module Alarms	1-29
1.3.7.2 Alarm Ports	1-30
1.3.7.3 Master Alarm Reporting	1-31
1.3.8 Alarm Configuration	1-31
1.3.8.1 Alarm Configuration (Severity List)	1-31
1.3.8.2 Alarm Persistency	1-32
1.3.8.3 Alarm Thresholds	1-33
1.3.9 Alarm suppression	1-33
1.3.9.1 VC Alarms	1-34
1.3.9.2 TU/AU Alarms	1-34
1.3.9.3 E1 Alarms	1-35
1.3.9.4 AUX Alarms	1-36
1.3.10 Date And Time	1-36
1.3.11 Summary	1-37
1.3.11.1 Commit Configuration	1-37
1.3.11.2 Result Of The Commissioning	1-38
1.3.11.3 Basic Network Element Set-up	1-38
1.3.11.4 TFTP Server	1-38
1.3.11.5 Expected Service Module (ONS 15305 only)	1-38
1.3.11.6 SDH Synchronization	1-38

1.3.11.7 Alarm Reporting	1-38
1.3.11.8 Time	1-38
1.3.11.9 Failures And Exceptions	1-38

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	2-2
2.2.4 Single Network Element	2-2
2.2.5 Graphical User Interface Types	2-3
2.2.5.1 Network Element topology Browser (NETB)	2-3
2.2.5.2 Custom GUI to Support a Specific System Feature	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 and Firmware Download	2-3
2.2.10 User Access	2-3
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 on Network Element	2-4
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

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 3-4
 - 3.1.2.1 File 3-4
 - 3.1.2.2 Edit 3-5
 - 3.1.2.3 View 3-5
 - 3.1.2.4 Equipment 3-6
 - 3.1.2.5 Tools 3-7
 - 3.1.2.6 Help 3-7
 - 3.1.2.7 Log Viewer 3-8
 - 3.1.3 Copy and Paste 3-10
 - 3.1.4 Cell Selection Mode 3-10
 - 3.1.5 Navigation in Tables Using the Keyboard 3-11
 - 3.1.6 Auto Fit Column Width 3-11
- 3.2 Management Tree 3-11
 - 3.2.1 Opening Links in a New Window 3-12
- 3.3 Alarm Display 3-12
 - 3.3.1 View Current Alarms 3-12
 - 3.3.1.1 Subscription of Alarms 3-12
 - 3.3.1.2 Select Alarm 3-14
 - 3.3.1.3 Alarm Lifestyle 3-16
 - 3.3.2 View the Events Reported From the Network Element 3-16
 - 3.3.3 Notification 3-19

CHAPTER 4

General Management 4-1

- 4.1 Manage the Management Interfaces 4-1
- 4.2 MCN Wizard 4-1
 - 4.2.1 Manage the Management Interfaces of the Network Element 4-2
 - 4.2.2 Before you start - Prerequisites 4-2
 - 4.2.2.1 Management Software 4-2
 - 4.2.2.2 NE Requirements 4-2
 - 4.2.2.3 General Requirements 4-2
 - 4.2.3 MCN Wizard - Step by Step 4-2
 - 4.2.3.1 MCN Commissioning Flow Overview 4-3
 - 4.2.3.2 Opening the MCN Wizard 4-3
 - 4.2.4 Welcome to the MCN Wizard 4-3

4.2.5	Network Element	4-4
4.2.6	System Mode	4-5
4.2.6.1	IP Numbered	4-6
4.2.6.2	IP Broadcast	4-6
4.2.6.3	IP Un-Numbered	4-6
4.2.7	Management Port - System Mode IP Numbered	4-6
4.2.8	DCC Encapsulation - System Mode IP Numbered	4-8
4.2.8.1	IP over DCC Encapsulation	4-8
4.2.8.2	Ip Over Ppp Encapsulation	4-8
4.2.9	IP in-band - System Mode IP Numbered	4-9
4.2.10	Global Ip Settings - System Mode Ip Numbered	4-10
4.2.11	System Mode - IP Broadcast	4-11
4.2.11.1	System Mode	4-12
4.2.11.2	Common Settings	4-12
4.2.11.3	Gateway	4-12
4.2.11.4	Management port	4-12
4.2.11.5	Media Access Control (MAC) Filter	4-12
4.2.11.6	Active DCC Channels	4-12
4.2.11.7	Summary	4-13
4.2.12	Summary	4-13
4.2.13	Special Requirements	4-13
4.2.13.1	DCC Usage Limitations	4-13
4.2.13.2	ONS 15305	4-13
4.2.13.3	ONS 15302	4-14
4.2.14	Features Vs. Network Element Types	4-14
4.3	Management Modes and Configuration	4-15
4.3.1	Management Port Configuration	4-15
4.3.1.1	Mode: Not Used	4-16
4.3.1.2	Mode: IP	4-16
4.3.2	DCC Configuration	4-17
4.3.2.1	Mode: Not Used	4-17
4.3.2.2	Mode: IP	4-18
4.3.3	IP Default Gateway Configuration	4-19
4.4	ONS 15305 Scenarios	4-19
4.4.1	Important Note	4-19
4.4.2	Notations Used	4-20
4.4.3	Scenario 1: CEC and ONS 15305 on the Same Subnet	4-20
4.4.4	Scenario 2: CEC and ONS 15305 on Different Subnets	4-22
4.4.5	Scenario 3: IP over DCC	4-23
4.4.6	Scenario 4: IP over PPP	4-24

4.5	Manage Common Parameters	4-25
4.5.1	View Common Parameters	4-25
4.5.2	Modify Common Parameters	4-25
4.5.2.1	Identification of the Network Element	4-25
4.5.2.2	Label	4-26
4.5.2.3	Time Settings	4-26
4.5.2.4	Users	4-28
4.5.2.5	Physical Inventory - ONS 15305	4-29
4.5.2.6	Physical Inventory - ONS 15302	4-31
4.5.2.7	Restart of ONS 15305	4-31
4.5.2.8	Restart of ONS 15302	4-32
4.5.2.9	Logs (Alarm Logs, Performance Data Logs)	4-32
4.5.2.10	Status Reporting	4-34
4.6	Manage Synchronization	4-37
4.6.1	SDH Synchronization	4-38
4.6.1.1	Synchronization Networks	4-38
4.6.1.2	Selecting the Best Synchronization Reference	4-39
4.6.1.3	Synchronizing the SDH Equipment	4-39
4.6.2	ONS 15305	4-40
4.6.2.1	Signal Monitoring	4-40
4.6.2.2	Candidate Selection and Configuration	4-40
4.6.2.3	QL-monitoring and Switching	4-40
4.6.2.4	SEC	4-41
4.6.2.5	Rules	4-42
4.6.2.6	Synchronization Alarms	4-42
4.6.3	View the Synchronization Data (T0 or T4)	4-43
4.6.4	Add Synchronization Source Candidate (T0 or T4)	4-44
4.6.5	Modify Synchronization Source Candidate (T0 or T4)	4-45
4.6.6	Delete Synchronization Source Candidate (T0 or T4)	4-46
4.6.7	Operate Synchronization Switch (T0 or T4)	4-46
4.6.8	View Synchronization Switch (T0 or T4)	4-47
4.6.9	Operate Synchronization on ONS 15302	4-47
4.7	Software download and Configuration- Custom GUI	4-48
4.7.1	Introduction	4-49
4.7.2	Overview	4-49
4.7.3	Software Download Process	4-49
4.7.3.1	Software Upgrade	4-50
4.7.3.2	Firmware Upgrade	4-50
4.7.3.3	ConfiguRation Backup and Restore	4-50
4.7.3.4	Network Element Support	4-50

4.7.3.5	Download Files	4-51
4.7.3.6	TFTP Server Settings	4-52
4.7.4	Presentation of the Software Download GUI	4-53
4.7.4.1	Open the Software Download GUI	4-53
4.7.4.2	Operational and Administrative Software Bank of Network Elements	4-54
4.7.4.3	Manual Switching of Banks	4-55
4.7.4.4	Auto Switch	4-56
4.7.4.5	Repository	4-56
4.7.4.6	Commands	4-57
4.7.4.7	Confirmation Dialog	4-57
4.7.4.8	Restart Options	4-58
4.7.5	How To Install A Downloaded File Into The Management System	4-59
4.7.6	How to Install Download File to the Network Element	4-61
4.7.6.1	How To Upgrade A Network Element With A New Network Release	4-61
4.7.7	How to Backup and Restore Configuration Data	4-64
4.7.7.1	Create Backup File of Data Configuration	4-64
4.7.7.2	Restore Data Configuration From Backup File	4-66
4.8	Download Software to Network Element	4-67
4.8.1	Network Release	4-67
4.8.2	Operational and Administrative Software Bank	4-67
4.8.3	How do Software Upgrades Affect Traffic?	4-68
4.8.4	Download ONS 15305 Network Release	4-68
4.8.5	Software Download to ONS 15305	4-69
4.8.5.1	Manual Switch of Banks	4-72
4.8.6	Software Download to ONS 15302	4-73
4.9	Backup and Restore NE Configuration Data	4-73
4.9.1	Backup Configuration Data	4-73
4.9.2	Restore Configuration Data	4-75
4.10	Alarm and Event Configuration	4-76
4.10.1	Event Forwarding	4-76
4.10.2	Configure General Alarm Reporting	4-76
4.10.2.1	Device Alarm Enabling	4-77
4.10.2.2	Slot Alarm Enabling	4-77
4.10.2.3	Traffic Port Alarm Enabling	4-77
4.10.2.4	Alarm Port Alarm Enabling	4-78
4.10.2.5	Aux Port Alarm Enabling	4-78
4.10.3	Suppress Specific Alarms	4-78
4.10.3.1	Suppress RDI, EXC, DEG, SSF Alarms	4-78
4.10.3.2	Suppress AIS Alarms from SDH Ports	4-79

4.10.3.3	Suppress AIS Alarms from E1 Ports	4-79
4.10.3.4	Suppress AIS Alarms from AUX Port	4-79
4.10.4	Modify Alarm Severity and Description	4-79
4.10.5	Set Signal Degrade Threshold	4-79
4.10.6	Modify Alarm Persistency	4-80
4.10.6.1	Persistency Group 1 (HighOrderLevel)	4-80
4.10.6.2	Persistency Group 2 (Unfiltered)	4-80
4.10.6.3	Persistency Group 3 (LowOrderLevel)	4-80
4.10.7	Modify ONS 15302 Alarm Configuration Attributes	4-81
4.10.7.1	Location of Alarm Configuration Attributes	4-81
4.10.7.2	Modify Alarm Severity and Description	4-81
4.10.7.3	View all Alarm Reporting Instances	4-82
4.10.7.4	Enable Alarm Reporting	4-82
4.10.7.5	Modify Ais Rdi Alarm Reporting	4-83
4.10.7.6	Modify Alarm Persistency	4-84
4.10.7.7	Modify Signal Degraded (Sd) Threshold	4-84
4.11	Manage Slots on ONS 15305	4-85
4.11.1	View Slot	4-85
4.11.2	Modify Slot	4-87
4.11.2.1	ONS 15305 Physical Interface Indices	4-89

CHAPTER 5

Traffic Port Management 5-1

5.1	About Port Types	5-1
5.2	Selecting a Traffic Port	5-1
5.3	SDH Ports	5-2
5.3.1	Configuring ONS 15305 SDH Port Structure (Channelization)	5-2
5.3.1.1	SDH Structuring Wizard	5-2
5.3.1.2	AU4 Termination Points for Cross-connection	5-3
5.3.1.3	Tu3 Termination Points for XC	5-4
5.3.1.4	Tu12 Managed Objects for XC	5-4
5.3.2	Modifying or Removing ONS 15305 SDH Port Structure	5-4
5.3.2.1	Modify between Tu12 and Tu3 Objects	5-5
5.3.2.2	Modify between Au4 and Tu3 or Tu12 Objects	5-5
5.3.3	Setting and Reading Path Trace Identifiers	5-5
5.3.3.1	Set or Read RS Path Trace Identifiers	5-5
5.3.3.2	Set or Read VC-4 Path Trace Identifiers	5-6
5.3.4	Monitoring SDH Port Performance	5-6
5.3.4.1	Read RS PM Counters	5-7
5.3.4.2	Read MS PM Counters	5-7

5.3.4.3	Read VC-4 PM Counters	5-7
5.3.5	Enabling the SDH Port to Carry Traffic and Report Alarms	5-8
5.3.6	ONS 15305 SDH Port Synchronization Quality Output Signaling	5-8
5.3.7	Use the SDH Port as a Synchronization Source Input	5-8
5.3.8	Carry Management Traffic DCC by SDH Port Channels	5-8
5.4	PDH Ports	5-9
5.4.1	Setting the Port Mode for ONS 15305	5-9
5.4.2	Setting a Loop in an ONS 15305 PDH Port	5-9
5.4.3	Setting a Loop in an ONS 15302 PDH port	5-10
5.4.4	Releasing a Loop in a PDH Port	5-10
5.4.5	Assign VC12s in ONS 15302	5-11
5.4.6	Setting and Reading Path Trace Identifiers	5-11
5.4.7	Monitoring PDH Port VC-n Performance	5-12
5.4.8	Monitoring PDH E1 Port Performance	5-13
5.4.9	Enabling the PDH Port to Carry Traffic and Report Alarms	5-14
5.4.10	Cross-connect the ONS 15305 PDH Port to another Port	5-14
5.5	LAN Ports	5-14
5.5.1	ONS 15305 - LAN Port Attributes	5-14
5.5.2	ONS 15302 LAN Port Attributes	5-16
5.6	ONS 15305 SDH Cross-Connection Management	5-16
5.6.1	SDH Layer Network and Cross Connections	5-17
5.6.1.1	SDH Port Structuring	5-17
5.6.1.2	Example	5-20
5.6.1.3	XC Fabric	5-23
5.6.2	Open the Cross Connection GUI	5-23
5.6.2.1	Cancelling a query	5-24
5.6.2.2	Cross-connection GUI - Overview	5-24
5.6.3	Browsing Existing Cross-connections	5-25
5.6.3.1	Browsing all Cross-connections	5-25
5.6.3.2	Browsing Cross-connections of a Port	5-25
5.6.3.3	Filtering the Content of the Cross-connection List	5-26
5.6.3.4	Refreshing the Cross-connect Window	5-26
5.6.4	Setting up Cross-connections	5-27
5.6.4.1	From a 2 Mbps E1 Port to a Timeslot in an SDH Port	5-27
5.6.4.2	From a 45 Mbps E3 (T3) Port to a Timeslot in an SDH Port	5-28
5.6.4.3	Creating a Pass-through Cross-connection	5-28
5.6.5	Modifying Cross Connections	5-28
5.6.6	Protecting Cross Connections	5-28
5.6.6.1	SNC Protection	5-29

5.6.6.2	Modifying Protection Parameters of a Cross-connection	5-30
5.6.6.3	Commanding Cross-connection Protection Switch	5-31
5.6.7	Deleting Cross-connections	5-31
5.6.8	Advanced Cross-connection Operations	5-32
5.6.8.1	Setting up of Multiple Cross-connections by Multiple Selection	5-32
5.6.8.2	Setting up Multiple Cross-connections by Repeated Operations	5-32
5.6.8.3	Entering Termination Points Manually	5-33
5.7	ONS 15305 SDH Protection Management	5-33
5.7.1	Introduction	5-33
5.7.1.1	Multiplex Section Protection	5-34
5.7.2	Protect Section by MSP	5-35
5.7.3	Modify MSP	5-36
5.7.4	Delete MSP	5-37
5.7.5	Command MSP Switch	5-37
5.7.6	Legal combinations of SNCP and MSP	5-38
5.7.7	SubNetwork Connection Protection	5-39
5.7.7.1	Protect Connection by SNCP	5-39
5.7.7.2	Modify SNCP	5-39
5.7.7.3	Command SNCP Switch	5-39
5.8	ONS 15302 SDH Protection Management	5-39
5.8.1	Multiplex Section Protection	5-39
5.8.1.1	Modify MSP Parameters	5-39
5.9	Ethernet Standardized Mapping	5-41
5.9.1	Introduction	5-41
5.9.2	GFP Alarm and Event Conditions	5-42
5.9.3	GFP Performance Monitoring	5-42
5.9.4	VCAT - Virtual Concatenation	5-43
5.9.5	VC Level for VCAT	5-43
5.9.6	LCAS- Link Capacity Adjustment Scheme	5-43
5.9.7	VCAT and LCAS Alarms and Events	5-44
5.10	VCAT and LCAS Configuration Modes	5-44
5.10.1	VCAT with LCAS Enabled- Mode 1	5-45
5.10.2	VCAT Without LCAS Enabled- Mode 2	5-45
5.11	Administrative Bandwidth for VCAT	5-45
5.11.1	Bandwidth for uni-directional VCAT	5-45
5.11.1.1	Bandwidth for Bi-directional VCAT	5-46
5.12	Circuit Protection for VCAT	5-46
5.12.1	CirCuit Protection For Uni-directional Modes For ONS 15305	5-46
5.12.2	Circuit proTection For Symmetrical VCAT	5-47

5.13	Establish a standardized Mapping With CEC	5-47
5.13.0.1	BeFore You Start	5-48
5.13.0.2	Uni- directional VCAT with LCAS	5-48
5.14	Bi-directional VCAT Without LCAS	5-52
5.15	ONS 15305 Proprietary NxVC-12 EoS Mapping	5-53
5.15.1	Introduction	5-53
5.15.1.1	WAN Ports and the Mapping	5-53
5.15.2	WAN to SDH mapping- Custom GUI	5-55
5.15.2.1	Open WAN to SDH Mapping	5-55
5.15.2.2	List Available Termination Points	5-57
5.15.2.3	Cancelling a Query	5-57
5.15.3	Add Initial WAN Port Capacity	5-57
5.15.4	Modify WAN Port Capacity	5-60
5.15.4.1	Increasing Capacity in the SDH Server Layer:	5-60
5.15.4.2	Decreasing Capacity in the SDH Server Layer	5-61
5.15.5	Protecting a WAN Port	5-61
5.15.6	Modifying Protection Parameters of the WAN Port	5-63
5.15.7	Commanding WAN Port Protection Switch	5-64
5.15.8	Setting Path Trace Identifiers for WAN Port	5-65
5.15.9	Reading Path Trace Identifiers for WAN Port	5-65
5.15.10	Monitoring WAN Port Performance	5-66
5.15.11	Advanced WAN Port Operations	5-66
5.15.11.1	Selection and Insertion of Multiple Termination Points	5-66
5.16	ONS 15302 Proprietary NxVC-12 EoS Mapping	5-67
5.16.1	WAN ports and the Mapping	5-68
5.16.2	Differences between ONS 15305 and ONS 15302	5-68
5.16.3	Force LAN Down	5-69
5.16.3.1	Force LAN down on WAN down alarm	5-69
5.16.3.2	Cross-connect the WAN Channels	5-70
5.16.4	Increase Capacity in the SDH Server Layer	5-72
5.16.5	Decrease Capacity in the SDH Server Layer	5-73
5.16.6	Setting Path Trace Identifiers for WAN Port	5-73
5.16.7	Reading Path Trace Identifiers for WAN Port	5-74
5.16.8	Monitoring WAN Port Performance	5-74
5.16.9	Advanced WAN Port Operations	5-75

CHAPTER 6

Link Aggregation - ONS 15305 6-1

6.1	View Link Aggregation	6-1
6.1.1	Modify Link Aggregation	6-2

6.1.1.1 Assigning a Port to a Trunk	6-4
6.1.2 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 Examples	7-1
7.1.1.1 Configuration of Static Unicast Forwarding Information	7-1
7.1.2 Configuration of Static Multicast Forwarding Information	7-3
7.1.3 IGMP Snooping	7-4
7.1.3.1 Enabling IGMP Snooping	7-4
7.2 Miscellaneous	7-5
7.2.1 Spanning Tree Protocol (STP) Configuration	7-5
7.2.1.1 Configuring the STP Algorithm per Device	7-6
7.2.2 Rapid Spanning Tree Protocol (RSTP) Configuration	7-6
7.2.2.1 Configure RSTP on a port.	7-7
7.2.3 MAC Multicast	7-7
7.2.3.1 Enabling MAC Multicast Control Tables	7-7
7.2.3.2 MulticastForwarding	7-8
7.2.4 Traffic Control	7-9
7.2.4.1 PortPriority	7-9
7.2.4.2 PriorityGroup	7-10
7.2.4.3 TrafficClass	7-10
7.3 Manage VLAN	7-10
7.3.1 Virtual Local Area Networks (VLAN)	7-11
7.3.1.1 Tagged/untagged LAN ports	7-11
7.4 VLAN Provisioning	7-12
7.4.1 Configuration Of A New VLAN Per Port	7-12
7.4.2 Configuration Of A New VLAN Per Protocol And Per Port	7-13
7.4.3 Configuration of an Ethernet User Defined Protocol	7-14
7.4.3.1 Use The Ethernet User Defined Protocol	7-14
7.4.3.2 Use One Of The Pre-defined Protocols	7-16
7.4.4 Configuration of VLAN Port Members	7-16
7.4.5 GVRP	7-17
7.4.5.1 Legal time values	7-18
7.4.6 Provider VLAN (IEEE 802.1Q, Q in Q)	7-19
7.4.6.1 Overview	7-19
7.4.6.2 Definitions	7-19
7.4.6.3 Applications - examples	7-19
7.4.7 Provider VLAN	7-22

7.4.7.1	Setting up Provider VLAN - ONS 15305	7-22
7.4.7.2	Setting up Provider VLAN - ONS 15305 with FE/GE+SMAP modules	7-23
7.4.7.3	ProtocolTunneling	7-24
7.4.7.4	ProviderTagPrioritySource	7-25
7.4.7.5	VLANProviderID	7-25
7.4.7.6	ProviderTagPriority	7-25
7.4.7.7	ProviderTags	7-25
7.4.7.8	Setting up Provider VLAN - ONS 15302	7-25
7.4.7.9	Enabling Protocol Tunneling	7-26
7.4.7.10	Setting up Q in Q - ONS 15305	7-29
7.4.7.11	Setting up Q in Q - ONS 15302	7-31
7.5	Examples	7-32
7.5.1	Configure an IP Interface	7-32
7.5.2	Configure a Static Route	7-33
7.5.2.1	Create a Static Route	7-33
7.5.2.2	Configure a Default Route	7-35
7.5.3	Configure a RIP Filter	7-36
7.5.3.1	Create an IP RIP Global Filter:	7-36
7.6	Miscellaneous	7-37
7.6.1	Open Shortest Path First	7-37
7.6.1.1	Supported OSPF Areas: Transit and Stub Areas	7-37
7.6.1.2	Configuring an OSPF Area	7-38
7.6.1.3	Configuring an OSPF Interface	7-38
7.6.1.4	Enabling OSPF on the Network Element	7-38
7.6.2	DHCP	7-39
7.6.2.1	Configure the Range of IP Addresses for the DHCP Server	7-39
7.6.2.2	Configure the DHCP Server for Manual Allocation	7-39

CHAPTER 8

Performance Management 8-1

8.1	Introduction	8-1
8.1.1	Definitions	8-1
8.1.2	Present G.826 PM data	8-2
8.1.2.1	Background	8-2
8.1.3	View Counters	8-3
8.1.4	Criteria for Counting Valid-data	8-4
8.2	Manage RMON	8-4
8.2.1	About Rmon Measurements In Cisco Network Elements	8-4
8.2.2	RMON Overview	8-5
8.2.3	Create RMON Event Monitor	8-5

8.2.3.1 Define RMON Event Types	8-6
8.2.4 Configure an RMON Event Monitor	8-6
8.2.4.1 Define A Monitor Source	8-6
8.2.5 Create RMON History Monitor(s)	8-8
8.3 View RMON Data	8-8
8.3.1 View Statistical Data	8-9
8.3.1.1 Inspection Of Current Statistical Data	8-9
8.3.1.2 Inspection of History Statistics Per Port	8-10
8.3.2 View logged events	8-10
8.3.2.1 Inspection of the Event Log	8-10
8.3.2.2 Inspection of the Event Log	8-11
8.3.2.3 Delete RMON Monitor	8-11

CHAPTER 9

Troubleshooting and FAQ 9-1



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	Network configuration example 1	1-9
Figure 1-6	Network configuration example 2	1-10
Figure 1-7	Starting Cisco Edge Craft	1-15
Figure 1-8	Selection of IP Address - Logon Window	1-16
Figure 1-9	VT 100 available from Cisco Edge Craft Desktop	1-17
Figure 1-10	Commissioning wizard - Basic flow	1-19
Figure 1-11	Equipment menu	1-20
Figure 1-12	Commissioning wizard- Welcome window	1-20
Figure 1-13	Example of Current Configuration	1-21
Figure 1-14	Network element information	1-21
Figure 1-15	SNMP Community table	1-22
Figure 1-16	Example of current slot configuration	1-24
Figure 1-17	Example - current synchronization status	1-25
Figure 1-18	Alarm Reporting	1-29
Figure 1-19	Alarm reporting - power modules	1-30
Figure 1-20	Alarm reporting - external alarm input ports	1-30
Figure 1-21	Master alarm reporting	1-31
Figure 1-22	Overview - alarm configuration choices	1-31
Figure 1-23	Example - alarm suppression	1-34
Figure 1-24	Date and time - example	1-36
Figure 1-25	Summary report - example	1-37
Figure 2-1	Cisco Edge Craft Connection Possibilities	2-1
Figure 3-1	Cisco Edge Craft Desktop Overview	3-2
Figure 3-2	Move Toolbars	3-3
Figure 3-3	Lock Toolbars	3-4
Figure 3-4	Pull Down Menu File	3-4
Figure 3-5	Pull Down Menu Edit	3-5

Figure 3-6	Pull Down Menu View	3-6
Figure 3-7	Pull Down Menu Equipment	3-7
Figure 3-8	Pull Down Menu Tools	3-7
Figure 3-9	Pull Down Menu Help	3-8
Figure 3-10	The About box - Example	3-8
Figure 3-11	Log Viewer	3-9
Figure 3-12	Log Viewer - Tool tip	3-10
Figure 3-13	Example Copy and Paste	3-10
Figure 3-14	Editable Types and Tables - Hyperlinks	3-11
Figure 3-15	Setting the TrapsEnable Attribute	3-12
Figure 3-16	Current Tab - Alarm List	3-13
Figure 3-17	Latest Alarm	3-13
Figure 3-18	Notification History	3-14
Figure 3-19	Select Single Alarm	3-14
Figure 3-20	Select All Alarms	3-14
Figure 3-21	Select Alarms - Continuous Range	3-15
Figure 3-22	Select Alarms - None Continuous Range	3-15
Figure 3-23	Lifecycle Instance of Alarm Point	3-16
Figure 3-24	Select Events	3-16
Figure 3-25	Current Events	3-16
Figure 3-26	Event History	3-17
Figure 3-27	Visible Columns 1	3-17
Figure 3-28	Visible Columns 2	3-18
Figure 3-29	Column Order	3-18
Figure 3-30	Column Resize	3-19
Figure 3-31	Column Sorting	3-19
Figure 3-32	Trap to Notification Mapping	3-22
Figure 4-1	Welcome to the MCN Wizard	4-4
Figure 4-2	MCN Current configuration	4-5
Figure 4-3	System mode	4-5
Figure 4-4	Configure VLAN	4-9
Figure 4-5	IP In-band	4-9
Figure 4-6	Add Row	4-10
Figure 4-7	Routing Table	4-10
Figure 4-8	System Mode - IP Broadcast	4-12

Figure 4-9	Summary	4-13
Figure 4-10	Management Interfaces - Managed Object	4-16
Figure 4-11	ManagementPort - Attributes	4-16
Figure 4-12	ManagementPort - Mode Selector	4-16
Figure 4-13	ManagementPort - IP Address Attribute	4-17
Figure 4-14	ManagementPort - Add IP Address	4-17
Figure 4-15	Management Interfaces - Dcc Attribute	4-18
Figure 4-16	IPencapsulation - Encapsulation Selector	4-18
Figure 4-17	Cisco Edge Craft and ONS 15305 on the Same Subnet	4-20
Figure 4-18	Cisco Edge Craft and ONS 15305 on Different Subnets	4-22
Figure 4-19	IP over DCC	4-23
Figure 4-20	IP over PPP	4-24
Figure 4-21	Identification of Network Element	4-26
Figure 4-22	Time Settings - Time Attribute	4-27
Figure 4-23	Time Attribute - Values	4-27
Figure 4-24	Time Attributes - System Time	4-27
Figure 4-25	Add a New User - Overview	4-28
Figure 4-26	Physical Inventory - Overview	4-30
Figure 4-27	Restart of Network Element - Overview	4-31
Figure 4-28	Clear Alarm- and Performance Data Log	4-33
Figure 4-29	LEDs - Severity Selector	4-33
Figure 4-30	Ping Mechanism	4-34
Figure 4-31	Alarm Ports	4-35
Figure 4-32	AUX Port	4-36
Figure 4-33	AUX port - Timeslots	4-36
Figure 4-34	Power Module - Attributes	4-37
Figure 4-35	Example Synchronization Network	4-38
Figure 4-36	T0 Selection	4-39
Figure 4-37	T4 Selection	4-41
Figure 4-38	Synchronization - Selecting Managed Object	4-44
Figure 4-39	Synchronization - T0 SynchSources attribute	4-44
Figure 4-40	Add Synchronization Source	4-45
Figure 4-41	Operate Synchronization Switch 1	4-46
Figure 4-42	Operate Synchronization Switch 2	4-47
Figure 4-43	View Synchronization Switch	4-47

Figure 4-44	Select Synchronization	4-48
Figure 4-45	Select AdministrativeSynchSource	4-48
Figure 4-46	Software download process overview	4-50
Figure 4-47	Software directory - location of download files	4-52
Figure 4-48	TFTP server settings - Interface IP example	4-53
Figure 4-49	Open the Software Download GUI	4-53
Figure 4-50	Software Download GUI - overview	4-54
Figure 4-51	General illustration of switching Software banks	4-55
Figure 4-52	.Select inactive bank- example	4-56
Figure 4-53	Bank switch- example	4-56
Figure 4-54	Visible Repository columns	4-57
Figure 4-55	Download Command	4-57
Figure 4-56	Download Confirmation dialog box - Example Device	4-57
Figure 4-57	Show Confirmation Dialog.	4-58
Figure 4-58	Restart options	4-58
Figure 4-59	Connection Lost During Restart	4-59
Figure 4-60	Restart Calendar	4-59
Figure 4-61	Packet Installer- browser example	4-60
Figure 4-62	Summary of file transfer	4-60
Figure 4-63	Select Download File- Example R1.1 Network Release lcs05	4-62
Figure 4-64	Download Confirmation Dialog Box	4-62
Figure 4-65	Download session and progress- example device	4-63
Figure 4-66	Restart- example device	4-63
Figure 4-67	New Software installed on network element- example network release	4-64
Figure 4-68	Backup Confirmation dialog box	4-64
Figure 4-69	Upload session- example configuration back- up	4-65
Figure 4-70	Configuration folder and file- locations	4-65
Figure 4-71	Restore Confirmation Dialog Box	4-66
Figure 4-72	Restore data configuration- example	4-66
Figure 4-73	Example of Switching Software Banks	4-68
Figure 4-74	Download of Release Files	4-69
Figure 4-75	Select Device	4-70
Figure 4-76	Select Destination	4-70
Figure 4-77	Select Filetype	4-70
Figure 4-78	Select IP Address	4-71

Figure 4-79	Set Restart Date	4-71
Figure 4-80	Select Delayed Restart	4-71
Figure 4-81	Set Software Download File Name	4-72
Figure 4-82	Select Switch Bank Attributes	4-72
Figure 4-83	Select ConfigData	4-74
Figure 4-84	Select Device	4-75
Figure 4-85	General Alarm Reporting Filters.	4-77
Figure 4-86	Select Device	4-81
Figure 4-87	Select Alarm Config	4-82
Figure 4-88	Select AlarmReportingAll	4-82
Figure 4-89	Select AlarmReporting	4-83
Figure 4-90	Select AlarmreportingAisRdi	4-83
Figure 4-91	Select AIS Attributes	4-83
Figure 4-92	Set Alarm Persistency Attributes	4-84
Figure 4-93	Select SDTreshold	4-84
Figure 4-94	Set SDTreshold	4-84
Figure 4-95	Slot on the Network Element	4-85
Figure 4-96	Select Slot	4-85
Figure 4-97	Slot Module - Port Concept	4-86
Figure 4-98	Relation between Installed and Expected Module in a Slot.	4-86
Figure 4-99	Select Target Slot	4-87
Figure 4-100	Set View Mode to Children	4-88
Figure 4-101	IF-indices for physical/logical ports on the ONS 15305	4-89
Figure 5-1	Open The Structuring Wizard	5-2
Figure 5-2	SDH Structuring Wizard	5-3
Figure 5-3	Select the Aug1 Managed Object	5-3
Figure 5-4	Set the Structure Attribute	5-4
Figure 5-5	Set the E1 Mode Attribute	5-9
Figure 5-6	Set Admin Loop Mode Attributes	5-10
Figure 5-7	Assign VC 12 Port	5-11
Figure 5-8	Select Interval24Hour	5-13
Figure 5-9	Set Interval24Hour Attributes	5-13
Figure 5-10	LAN Port Attributes	5-15
Figure 5-11	LAN Port Attributes - ONS 15302	5-16
Figure 5-12	SDH Layer Network	5-17

Figure 5-13	SDH Multiplexing Structure	5-18
Figure 5-14	Slot - Port - CTP Relations	5-20
Figure 5-15	Largest Possible Cross Connect Matrix	5-20
Figure 5-16	Unidirectional XC, Unprotected	5-21
Figure 5-17	Uni-directional XC, Protected	5-21
Figure 5-18	Bidirectional XC, Unprotected	5-22
Figure 5-19	Bidirectional, Protected	5-22
Figure 5-20	Example of Bidirectional, Unprotected, Point-to-point XC	5-22
Figure 5-21	Example of Bidirectional, Protected, Point-to-point XC	5-23
Figure 5-22	XC Fabric	5-23
Figure 5-23	Select Cross Connect	5-24
Figure 5-24	Select SDH Port Cross Connect	5-24
Figure 5-25	Cross-connection GUI - Overview	5-25
Figure 5-26	Example of Filtering Criteria - Cross-connections	5-26
Figure 5-27	Select the VC/TU12 Tab	5-27
Figure 5-28	Select the VC/TU12 Tab	5-28
Figure 5-29	Select Enabled Attributes	5-30
Figure 5-30	Select SNCP Command	5-31
Figure 5-31	1+1 MSP between two ONS 15305	5-34
Figure 5-32	Protection Switching Scenarios	5-34
Figure 5-33	Select SDH Port	5-35
Figure 5-34	Select MSP Object	5-35
Figure 5-35	Select Protection Port Attributes	5-36
Figure 5-36	Select MspCommands Attribute	5-38
Figure 5-37	Select SDH1/MSP1 Attributes	5-40
Figure 5-38	Set MSP Command	5-40
Figure 5-39	VCAT with SNC- Illustration	5-47
Figure 5-40	standardized mapping- GUI overviews	5-48
Figure 5-41	Slot configuration- ONS 15305 example	5-49
Figure 5-42	Ethernet port - VC Group view	5-49
Figure 5-43	VC Group concatenation- Example VC level	5-49
Figure 5-44	Enable LCAS	5-50
Figure 5-45	Administrative Capacity- Symmetrical Uni- directional VCAT	5-50
Figure 5-46	Operational Capacity- example asymmetrical capacity	5-50
Figure 5-47	WAN- to- SDH Mapping- LCAS Traffic Status	5-51

Figure 5-48	LCAS traffic set for one VC Channel	5-51
Figure 5-49	Lcas Operation Mode	5-52
Figure 5-50	Bi- directional VCAT- Example VC- level 12	5-52
Figure 5-51	The 8 x STM-1 Module with WAN Ports	5-54
Figure 5-52	View of one WAN Port and its Logical View	5-54
Figure 5-53	Sequence Numbers for Correct Order of TU-12 to VC-12 Cross Connects.	5-55
Figure 5-54	WAN- to- SDH Mapping- GUI Overview	5-56
Figure 5-55	WAN port search- example uni- directional	5-56
Figure 5-56	WAN channels list- example VC/ TU 12	5-57
Figure 5-57	Set Bandwidth	5-58
Figure 5-58	Select WAN Port Attributes	5-58
Figure 5-59	Set WAN Port Attributes	5-59
Figure 5-60	Select Available VC/TU12	5-59
Figure 5-61	Select WAN Channels	5-61
Figure 5-62	Select Protected Mode	5-62
Figure 5-63	Set SNCP Properties Enabled	5-63
Figure 5-64	Set SNCP Properties Protection	5-64
Figure 5-65	Set SNCP Properties Command	5-64
Figure 5-66	View of the WAN Ports and their Logical View	5-68
Figure 5-67	VLAN entry- example	5-70
Figure 5-68	Force LAN down on WAN down	5-70
Figure 5-69	Select a WAN port	5-71
Figure 5-70	Set WAN Attributes	5-71
Figure 5-71	Select Available VC/TU12 Container	5-72
Figure 5-72	Delete WAN Port	5-73
Figure 6-1	Attributes related to Link Aggregation	6-2
Figure 6-2	Creating and Editing a trunk to a VLAN	6-5
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	7-18
Figure 7-15	Application Example 1	7-20
Figure 7-16	Application Example 2	7-21
Figure 7-17	Application Example 3	7-22
Figure 7-18	VlanEtherType	7-23
Figure 7-19	VlanEtherType	7-24
Figure 7-20	Provider VLAN	7-24
Figure 7-21	Provider Tags Setting	7-26
Figure 7-22	Protocol Tunneling	7-27
Figure 7-23	SpanningTreePerDevice	7-27
Figure 7-24	SpanningTreePort.	7-28
Figure 7-25	PortEnable	7-28
Figure 7-26	Protocol Tunneling	7-28
Figure 7-27	ProviderTags	7-29
Figure 7-28	Configuration of an IP Interface	7-32
Figure 7-29	Create a Static Route	7-34
Figure 7-30	Figure - Static Route in Router R1	7-35
Figure 8-1	View PM - Example	8-3
Figure 8-2	RMON - GUI overview	8-5
Figure 8-3	RMON Events-GUI example	8-6
Figure 8-4	Select RMON Alarms	8-7
Figure 8-5	Add Monitor Entry	8-7
Figure 8-6	RMON History Monitor- example	8-8
Figure 8-7	RMON Statistics- GUI overview	8-9
Figure 8-8	Select History Control	8-10
Figure 8-9	RMON History statistics - example	8-10
Figure 8-10	RMON Logs-view	8-11
Figure 8-11	Alarm monitor- example	8-11
Figure 8-12	RMON Event log to alarm monitor-view	8-11

<i>Figure 9-1</i>	VLAN calculation	9-2
<i>Figure 9-2</i>	IEEE 802.1Q Tag header (VLAN tag)	9-3
<i>Figure 9-3</i>	Adjustment of VLAN/GVRP entries	9-5
<i>Figure 9-4</i>	Definition of a set of ports through an octet string	9-5
<i>Figure 9-5</i>	Common UDP Ports	9-6



TABLES

Table 1-1	CLI Connector Pinout (RJ-45 to DS-9)	1-3
Table 1-2	Network element description attributes	1-21
Table 1-3	User description attributes	1-22
Table 1-4	Slot attributes	1-24
Table 1-5	SEC (T0) synchronization - ONS 15305 - parameters	1-26
Table 1-6	SEC (T0) synchronization - ONS 15302 - parameters	1-27
Table 1-7	2048 kHz Output (T4) synch - ONS 15305 - parameters	1-28
Table 1-8	Alarm reporting - power modules	1-30
Table 1-9	Alarm reporting - alarm ports	1-30
Table 1-10	Alarm severity - parameters	1-31
Table 1-11	Alarm persistency - parameters	1-32
Table 1-12	Persistency category	1-32
Table 1-13	Alarm threshold - parameters	1-33
Table 1-14	Alarm suppression - VC	1-34
Table 1-15	Alarm suppression - TU/AU	1-34
Table 1-16	Alarm suppression - E1	1-35
Table 1-17	Alarm suppression - AUX	1-36
Table 2-1	Cisco Edge Craft Capabilities	2-2
Table 3-1	Toolbar buttons	3-2
Table 3-2	Menu File	3-5
Table 3-3	Menu Edit	3-5
Table 3-4	Menu View	3-6
Table 3-5	Menu Equipment	3-7
Table 3-6	Menu Tools	3-7
Table 3-7	Menu Help	3-8
Table 3-8	Log Viewer Icons	3-9
Table 3-9	Notification Types	3-20
Table 3-10	Events Notifications	3-21
Table 4-1	System mode vs. network element	4-6
Table 4-2	Management port modes	4-7
Table 4-3	Features Supported by ONS 15302 and ONS 15305	4-14

Table 4-4	Management Modes Versus Management Interface	4-15
Table 4-5	Cisco Edge Craft and ONS 15305 on the Same Subnet - Settings	4-21
Table 4-6	Cisco Edge Craft and ONS 15305 on Different Subnet - Settings	4-22
Table 4-7	IP over DCC - Settings	4-23
Table 4-8	IP over PPP- Settings	4-24
Table 4-9	Alarms related to SDH Synchronization Events	4-43
Table 4-10	Persistency Group 1 (HighOrderLevel)	4-80
Table 4-11	Persistency Group 2 (Unfiltered)	4-80
Table 4-12	Persistency Group 3 (LowOrderLevel)	4-81
Table 5-1	C.B.K.L.M Value Usage	5-18
Table 5-2	VCAT and LCAS Alarm and Event Conditions	5-44
Table 5-3	Mapping to VC-n	5-53
Table 5-4		5-68
Table 6-1	Valid Link Aggregation configuration for 16xFE port module	6-3
Table 7-1	VLAN Protocol	7-16
Table 8-1	Managed Objects	8-2
Table 9-1	Octet string and corresponding set of ports	9-5
Table 9-2	Link state type (according to RFC2328, Appendix A.4.1)	9-6



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](#)
- [Cisco Product Security Overview](#)
- [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 is organized into the following chapters:

- [Chapter 1, “Starting the 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 - ONS 15305”](#) 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.
- [Chapter 9, “Troubleshooting and FAQ”](#) provides information in case of problems with the system.

Related Documentation

Use this Cisco Edge Craft Software Guide 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.

Convention	Application
screen font	Examples of information displayed on the screen.
boldface screen font	Examples of information that the user must enter.
< >	Command parameters that must be replaced by module-specific codes.



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



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



Warning

IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. 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 Edge Craft Software Guide that accompanied the product. This publication describes the international agency compliance and safety information for the Cisco ONS 15302 and ONS 15305 systems. It also includes translations of the safety warnings that appear in the ONS 15302 and ONS 15305 system documentation.

Obtaining Documentation

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

Cisco.com

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

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

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

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

Documentation DVD

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

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

Cisco Ordering tool:

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

Cisco Marketplace:

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

Cisco Optical Networking Product Documentation CD-ROM

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_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/>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

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

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

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

We appreciate your comments.

Cisco Product Security Overview

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

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

From this site, you can perform these tasks:

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

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

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

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

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

Reporting Security Problems in Cisco Products

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

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



Tip

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

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

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

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

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

Obtaining Technical Assistance

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

Cisco Technical Support Website

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

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

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

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



Note

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support Website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

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

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

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

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

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

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

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

Definitions of Service Request Severity

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

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

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

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

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

Obtaining Additional Publications and Information

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

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

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

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

<http://www.ciscopress.com>

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

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

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

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

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

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

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

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



Starting the Cisco Edge Craft

1.1 Installation of Cisco Edge Craft

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

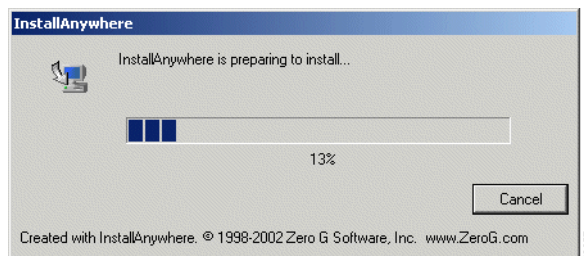
Step 1 Insert the Cisco Edge Craft Software CD in desired drive on target PC.



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

Step 2 Run `ciscocraft.exe` and 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*

1.1.1 Uninstall Cisco Edge Craft

Select Start>Programs>Cisco Edge Craft>uninstall and follow instructions given on screen.

or:

Select Start>Settings>Control Panel>Add/Remove Programs.

1.1.2 Commissioning of IP Address via VT100 Interface

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

1.1.2.1 Commissioning of IP Address via VT100 Interface

ONSLCI 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 bit/s,
- no parity,
- 8 bits,
- 1 stop bit,

- and 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. The cable for connecting the VT100-port to the serial-port on the PC can be provided, [Table 1-1](#).

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**

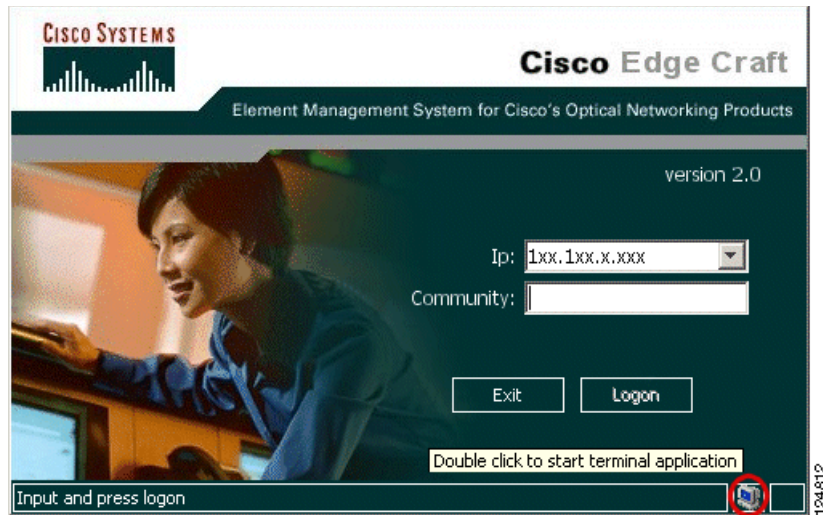
Pin 4, 5 and 7 are only used for debug purposes.

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**

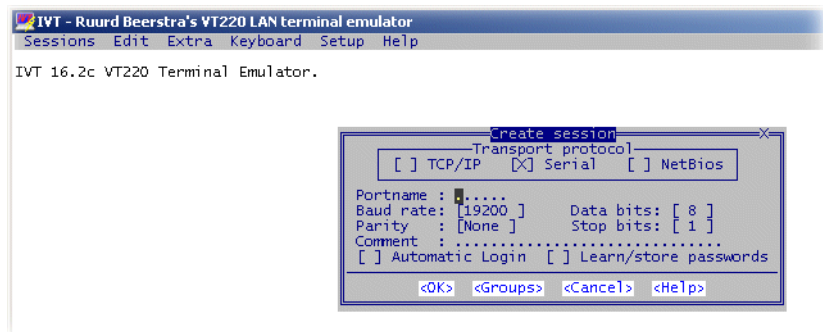
Step 3 Double-click the VT100 icon in the lower right corner of the Logon window, [Figure 1-3](#).

Figure 1-3 Logon Window



Step 4 The terminal application launches, [Figure 1-4](#).

Figure 1-4 Start Window



Step 5 Enter **COM** port name and select **OK**.

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

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

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


Step 7 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 may 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 you. All the other parameters (except default gateway) are defaulted to pre-defined values if they are not specified.

1.1.2.2 Configure Community-Handler



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

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

ONS 15305

Step 1 ONSCLI>com

Step 2 Press **Enter**.

Step 3 ONSCLI>Community-handler\

Step 4 Press **Enter**.

```
Add:    Add Community entry
Edit:    Edit Community entry
Remove:  Remove Community entry
Show:    Show Community entry
Exit:
```

```
ONSCLI>Community-handler\
```

Step 5 ONSCLI>Community-handler\add man=0.0.0.0 com=public acc=super traps=disable

Step 6 Press **Enter**.

```
MANAGER:    0.0.0.0
COMMUNITY:  public
ACCESS:     super
TRAPS:      disable
```

```
ONSCLI>Community-handler\
```

ONS 15302

Factory pre-configured community:

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

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

To add your own community string you can use the following command:

Step 1 `ONSCli>Security\Community-Table\add manager=10.0.0.20 community=admin access=super traps=enable`

Step 2 Press **Enter**.

1.1.2.3 Assign an IP Address**ONS 15302**

The ONS 15305 supports remote management solutions by means of Telnet and SNMP. The possibilities that regard to connectivity can be rather advanced for the ONS 15305, so the only explained solution in this document is when directly connected the management-port (MNGT). For more information refer Cisco EdgeCraft User Guide and the ONS 15305 Installation and Operations Guide.

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

System Mode

In ONS 15305 R2.0 an additional management mode, system mode, is added. System mode has two options IP and IPUNNUMBERED.

Prior to configuring the IP settings on the ONS 15305 the desirable system mode should be set, since this is a strategically choice to align with the existing design of management data communication network. By default the system mode is IP, which means that all physical indices must have a unique IP address and subnet mask. For more information refer Cisco EdgeCraft User Guide and the ONS 15305 Installation and Operations Guide.

Step 1 `ONSCli>Management-modes\sys?`

Step 2 Press **Enter**.

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

System Mode - IP (default)

-
- Step 1** ONSCLI>Management-modes\sys sys=ip
Change management configuration, are you sure? (y/n)?
- Step 2** Press y.
If system mode is ip the command for assigning an IP address is:
- Step 3** ONSCLI>Device\Management-Configuration\IP-Configuration
IP-ADDRESS=193.69.136.104, SUBNET-MASK=255.255.255.0
- Step 4** Press Enter

System Mode - IP Unnumbered

-
- Step 1** ONSCLI>Management-modes\sys sys=ipun
Change management configuration, are you sure? (y/n)?
- Step 2** Press y.
Assign an IP-address:
If system mode is IP unnumbered the command for assigning an IP address is:
- Step 3** ONSCLI>Device\Management-Configuration\IP-Configuration
IP-ADDRESS=193.69.136.104, SUBNET-MASK=255.255.255.0
- For most commands, if no parameters are supplied then all the current parameter values are displayed.
- ```

ONSCLI>IP-Configuration
IP-ADDRESS: 10.0.0.1
SUBNET-MASK: 255.255.255.0
DEFAULT-GATEWAY: 10.0.0.254 (optional)

```
- 

## ONS 15302

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

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

## System Mode

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

- 
- Step 1** ONSCLI>...\Management-Configuration\sys?
- Step 2** Press Enter
- Step 3** The description is displayed:
- ```

Usage:
  System-Mode

```

```
[SYSTEM-MODE=<ip|ipunnumbered>]
```

System Mode - IP

Step 1 `ONSCli>...\Management-Configuration\sys sys=ip`
 Change management configuration, are you sure? (y/n)?

Example 1-1 Assign an IP-address:

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

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

System Mode - IP Unnumbered

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

Example 1-2 Assign an IP-address:

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

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

1.1.2.4 Change Passwords

ONS 15305

```
ONSCli>ch?
Usage:
Change-Passwords
[ONSCli -PASSWORD=<string[6:12]>]
[TELNET-PASSWORD=<string[6:12]>]
```

By this command, TELNET and ONSCLI passwords can be changed. Both passwords can be changed in the same command or they can be changed one by one.

ONS 15302

```
ONSCli>Security\Community-Table>ch?
Usage:
Change-Passwords
[ONSCli -PASSWORD=<string[6:12]>]
[TELNET-PASSWORD=<string[6:12]>]
```

By this command, TELNET and ONSCLI passwords can be changed. Both passwords can be changed in the same command or they can be changed one by one.

1.1.3 IP Unnumbered Mode

This chapter focus on using ONS 15302 and ONS 15305 in IP un-numbered mode.

The following examples are valid for these NE releases:

ONS 15302 R2.0

ONS 15305 R2.0

In the traditional IP numbered mode, each DCC connection is an IP network, and both ends of the DCC connection have an IP address in that network.

In IP-unnumbered mode, all management interfaces of an element will have the same IP address. The DCC interfaces inherit the address of the management interface. This makes configuration of a set of elements connected via DCC simpler.

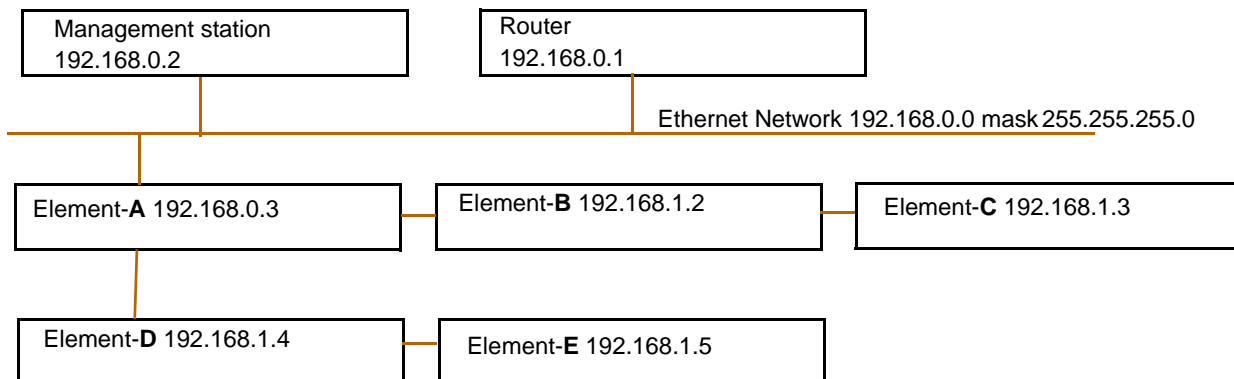
Routing between the elements will be taken care of by the OSPF routing protocol, using host routes pointing to the interfaces.

Planning the Network

In a typical IP-unnumbered network, one element will be connected to the outside world via the management port. This is the IP unnumbered gateway. The other elements are connected to the first element via DCC channels. As an alternative to DCC channels, it is possible to use LANx ports in layer 1 mode.

Example 1

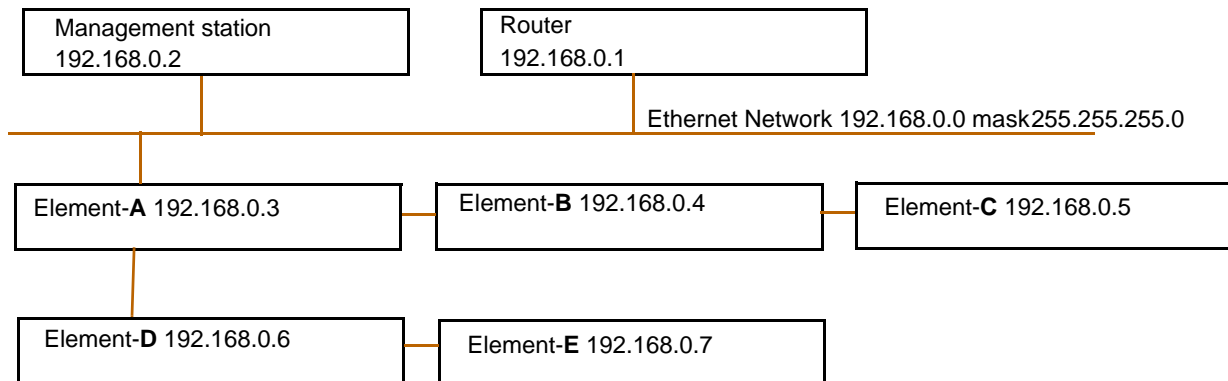
Figure 1-5 Network configuration example 1



In this configuration, the network elements, except the gateway element, will have an IP address on a separate network.

The management station and the router will have a static route for all the elements in the 192.168.1.0 network via 192.168.0.3.

Example 2

Figure 1-6 Network configuration example 2

In this example, all elements, including the gateway element, will have addresses on the same network as the other hosts on the Ethernet. The gateway element acts as an ARP proxy. That is, when a host, for instance the router, broadcasts a “who has address 192.168.0.7” on the Ethernet, the gateway element, Element-A, responds on behalf of Element-E. The following IP packets from the router to Element-E is sent to Element-A's hardware address.

1.1.4 Setting up the element for IP unnumbered, overview

- Step 1** Connect to the element via the serial port
- Step 2** Clear the configuration with ONSCLI function **erase cdb** (configuration database), unless the element is a new, unconfigured element.
- Step 3** Set the **system mode** via ONSCLI.
- Step 4** Optionally, set the IP unnumbered gateway to true, if the element is going to be the gateway element.
- Step 5** Set an **IP address** via ONSCLI.
- Step 6** Add a **user** in the community table
- Step 7** **Connect** to the element with the Management Tree
- Step 8** Use the Management Tree to configure the **DCC interfaces**
- Step 9** Create an **OSPF area**
- Step 10** Assign the **OSPF interfaces** to the OSPF area.
 - Add static route entries (if needed).
 - Set LeakStaticRoutes (if intended).
 - Set LeakExternalDirectRoutes (if intended).
- Step 11** Enable **OSPF globally** for the element.
- Step 12** **Remove** the management port cable.

The above steps are explained more detailed in the following sub-sections.

1.1.4.1 Connect to the element via the serial port

Connect the elements serial port (marked VT100) to a management station with the supplied serial cable. Use the Cisco EdgeCraft's terminal emulation program or another terminal program to connect to the elements command line interface.

1.1.4.2 Clear the configuration with ONSCLI

If the element has been configured in IP numbered mode, the configuration has to be reset.

At least, all OSPF-related entries must be removed, and all static routes, including the default route, must be deleted.

1. Enter the ONSCLI menu
2. Enter the **erase cdb** command. The element will now restart.

1.1.4.3 Setting the system mode.

When the element is unconfigured or the element has been cleared with the function "erase cdb", it initially is in IP numbered mode. Changing the system mode to IP unnumbered is done via the command line interface.

Optionally set gateway enable

If the element is the gateway element, consider setting the gateway enable to true. The effect of this variable is to create a route for the local network on the management port, and to leak this route via OSPF to the other ip unnumbered elements. Also, it ensures that static routes to gateways on the Ethernet are pointed to the correct interface.

This provides connectivity from all IP unnumbered elements in to any host on the Ethernet, see "Example 1" on page -9 or "Example 2" on page -9 configurations.

See also "Using the LeakDirectExternalRoutes variable." on page -14.

1.1.4.4 Set an IP address via ONSCLI

Use the ONSCLI to set an IP address. If this is the gateway element, a default gateway can also be set. If this is not the gateway element, a default route need not be set, as the proper routes will be configured by OSPF.

1.1.4.5 Add a user in the community table

Use the command line interface to add a line in the community table. In the ONS 15305, the community table is found in the "Community table" menu directly below ONSCLI.

Enter this command:

add manager=0.0.0.0 community=public access=super traps=disable

1.1.4.6 Connect to the element with the Management Tree

The network element must now be connected to a management station running the Management Tree using the management port. The easiest way is to use a straight unshielded twisted pair cable with RJ45 connectors in each end, and connect it directly between the element and the management station.

Configure the management station's interface to have a static IP address in the same network as the element. For instance, if the element's IP address is 192.168.1.5 and the netmask is 255.255.255.0, select for example address 192.168.1.100 for the management station (select an unused address).

Alternatively, if example 2 configuration is used, the element can be temporarily connected to the Ethernet with a cable from the management port to the switch representing the Ethernet. If this method is chosen, special care must be taken when the cable is removed after the configuration is complete. At this time, the IP traffic that till now have used the management port, is supposed to continue using the gateway element's management port.

But the other hosts, like the management station in the example and the router, will continue to send to the mac-address of the management port, now unsuccessfully.

Therefore the ARP-tables of the management station and the router have to be manually deleted.

After that, the gateway element will answer the ARP requests for the elements, and communication can continue. The ARP command is for instance **arp -d 192.168.0.5** in MS Windows and the same in Solaris.

Alternatively, if a configuration like example 1 is used, the management port of the element can be connected to the Ethernet, then the management station's interface is changed to an unused address in the same IP network as the element.

Example

The element to be configured is 192.168.1.3, its management port is connected to the switch representing the Ethernet. The management station's IP address is changed to 192.168.1.100.

Now we are running on IP-networks on the same Ethernet. There will be no connectivity to the router when this is going on, and the ARP table on the management station will be reset when its IP address is changed back to the normal, 192.168.0.2, so there will be no problems with ARP tables in this case.

If the element to be configured is the gateway element (Element-A in both examples), the management port is supposed to be connected permanently, and connectivity should be ensured with no special arrangements.

1.1.4.7 Configure the DCC interfaces

Use the Management Tree to configure the DCC interfaces (alternatively, the DCC interfaces can be configured in ONSCLI).

- Find the SDH port you are going to use
- Find rs
- Find dccR
- Set the variable **Mode** to **ipOverDcc**.
- The IpEncapsulation should be set to ppp/crc32, which is the default for ONS 15305 R 2.0.

Alternatively, find the dccM interface under ms under rs, and set Mode to ipOverDcc.

The DCC interfaces are also available in table form in managementInterfaces, DCC.

Unless the optical cables are connected to the SDH ports, and the DCC interfaces at the other ends are configured accordingly, the DCC interfaces will have OperStatus "down". This is ok for the moment, but the interfaces will have to be brought "up" for the OSPF interface configuration in a later step.

1.1.4.8 Create an OSPF area

In the Management Tree,

- Find `managementInterfaces`
- Then `DCNRouter`
- Then `OSPF`
- Then `AreaOSPF`. In this table, add a row, accept all the default entries
- Then save. This will create an area with id 0.0.0.0.

1.1.4.9 Assign the OSPF interfaces to the OSPF area

The OSPF interfaces for the DCC channels will automatically be created when the DCC channels are in “up” operational status. At this point, it is therefore necessary to connect the optical cables, where the DCC channels of the other ends of the cables are configured accordingly.

If this is not practical, it is possible to temporarily interconnect two ports on the same element, configuring the DCC channels of each port. The DCC interface will then reach “up” `OperStatus`, and the OSPF interfaces are visible in the `AreaInterface` table.

In the Management Tree,

- find **`managementInterfaces`**,
- then `DCNRouter`
- then `OSPF`
- then **`AreaInterface`**. For each of the interfaces, select the area to which the interface attaches, 0.0.0.0 in our example.

A third possibility is to skip this step entirely, deploy the element to its final location, connect the cables and restart the element. When the element is restarted and the DCC interfaces have **`OperStatus`** up, the startup procedure will assign each OSPF-interface to the first area it finds. If this method is used, it is still necessary to enable OSPF globally for the element (see “Enable OSPF globally for the element.” on page -13).

1.1.4.10 Set `LeakStaticRoutes`

If this is the gateway element (Element-A in the examples), the variable **`LeakStaticRoutes`** should be set to **`true`**. The default route, or any other static routes set in the element will then be announced to all the other elements in the IP unnumbered network, enabling connectivity outside the network. If this is not the gateway element, this variable should normally be set to **`false`**.

1.1.4.11 Enable OSPF globally for the element.

In the Management Tree,

- find `managementInterfaces`
- then `DCNRouter`
- then `OSPF`
- Change variable `AdminStatus` to “enabled”.

1.1.4.12 Remove the management port cable.

Unless this is the gateway element, remove the management cable.

If a separate IP network was used, as in example 1, the hosts on the Ethernet should have a route to the elements via the gateway element.

Example, MS Windows

```
route add 192.168.1.0 mask 255.255.255.0 192.168.0.3
```

Example, Solaris:

```
route add -net 192.168.1.0/24 192.168.0.3
```

Delete ARP entries in the management station or the router, if appropriate, see “Connect to the element with the Management Tree” on page -12.

1.1.4.13 Verify connectivity

It should now be possible to ping the element from anywhere, and to connect Cisco EdgeCraft to the element.

All the elements should now have a route to the new element, see managementInterfaces, DCNRouter, RoutingTable.

The gateway element Element-A, should now answer ARP requests for the new element, see Element-A's **ArpProxy** table found under management interfaces, DCNRouter.

1.1.4.14 Using the LeakDirectExternalRoutes variable.

Consider one of the example networks. If a management station is connected to any element in the network, for example Element-E, and the management station's IP-address is configured with a compatible IP address, connectivity to the first element is enabled.

If additionally the LeakDirectStaticRoutes in Element-E is set to “enabled”, the direct route to the workstation is announced through OSPF to the other elements in the network, enabling connectivity between the directly connected workstation and all the elements in the IP unnumbered network.

A direct static route is created when the element receives an ARP-request on the management port.

1.1.4.15 Connectivity without OSPF

For the first elements behind the IP-unnumbered gateway, Element-B and Element-D in the above examples, OSPF is strictly not necessary to enable connectivity. A simple routing protocol called IPCP (IP Control Protocol) that works over PPP, will ensure connectivity to neighboring elements. The router or the management station in the examples will be able to connect to Element-B and Element-D without OSPF, but a static route in Element-B and Element-D is necessary.

Consider also a situation with many CPE (Customer Premises Equipment) elements connected to one node at the edge of the network. OSPF can be turned off on each of the CPE elements, the neighbor has LeakDirectExternalRoutes turned on. This will reduce the number of nodes running OSPF, and therefore also the OSPF traffic.

1.1.4.16 Changing the IP address

To change the IP address of an element, the global OSPF must first be turned off using the Management Tree, variable AdminStatus in OSPF. After that, the IP address has to be changed via ONSCLI using the serial cable. Alternatively, the IP address could be changed via the Management Tree, if routes are in place to cover both addresses. After that, Cisco EdgeCraft has to be reconnected using the new address.

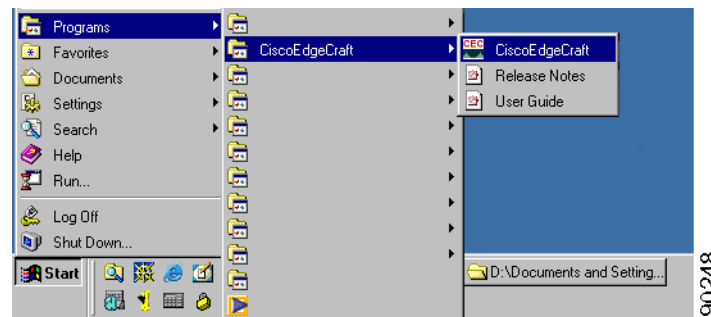
1.1.5 Set up Connection to a Network Element

The purpose of this section is to describe the tasks involved in setting up a connection between the Craft Terminal and any network element from Cisco. See also the “[1.1.2 Commissioning of IP Address via VT100 Interface](#)” section on page 1-2.

1.1.5.1 Start the Cisco Edge Craft Application on your Computer

- Step 1** Select Program>Cisco Edge Craft>Cisco Edge Craft, [Figure 1-7](#).

Figure 1-7 Starting Cisco Edge Craft



- Step 2** A logon window is presented for you.
- Step 3** Enter Community **password**.
- Step 4** If present, select desired network element from **Ip** pull-down menu, [Figure 1-8](#)

Figure 1-8 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.

Step 5 Click **Logon** to continue.

Community access levels:

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.

Step 6 The system validates the community string and IP address combination. If valid, that means combination correct and valid SNMP community string, the craft terminal sets up a connection to the specified IP address. The desktop of the craft terminal with its working windows is presented to you.

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

1.1.5.2 Invalid Community String

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

1.1.5.3 Non-existent IP Address

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

1.1.6 Configuration of VT100 Terminal

The VT100 terminal can be launched from both the Cisco Edge Craft desktop and the logon window. You can change the terminal Software to be launched.

Figure 1-9 VT 100 available from Cisco Edge Craft Desktop

This is done by editing the VT 100 path description in the ExternalApplications.xml file, found in the folder: install\dir\CISCOEDGE CRAFT\res\config\

Example of the ExternalApplications.xml:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
- <ExternalApplications>
  <vt100 file=".external/IVT_VT220_Telnet/ivt.exe" />
  <exec file="rundll32 url.dll,FileProtocolHandler" />
  <web file="rundll32 url.dll,FileProtocolHandler" />
  <help file="rundll32 url.dll,FileProtocolHandler" params=".res/help/OL-5383-01.pdf" />
  <releasenotes file="rundll32 url.dll,FileProtocolHandler" params=".res/help/CECrn12.pdf" />
</ExternalApplications>
```

1.2 Commissioning Wizard

This section describes the workflow of a Cisco network element basic set-up using the Commissioning wizard. The Commissioning wizard is a user-friendly option to provide guidance for common configuration tasks of a Cisco network element.

1.2.1 Introduction

Cisco's definition of Commissioning is that the network element is configured from scratch and is to be installed in a network for the first time.

Even though the wizard is primarily meant to cover first time installation, you may use it to change software configuration at a later stage or maybe just as a step-wise status of your configurations.



Note

The basic configuration needed for a Cisco NE varies dependently of application(s) and network roles. Other settings not available in this wizard can be found in the "Management tree" or other wizards available for software configuration. E.g. the Management Communication Network (MCN) wizard will provide you a user-friendly option to configure the IP management connectivity part for remote supervision and maintenance.



Note

The Commissioning wizard available in this release of Cisco Edge Craft supports ONS 15302 and ONS 15305.

1.2.2 Before You Start

Please read through the different prerequisites listed in this section.

1.2.2.1 Network Element Access And Permissions

Make sure you are assigned sufficient permissions to perform the required tasks. For CEC it is mandatory to have SNMP “super” (refer initial setup) rights to configure all parameters available in wizard. Otherwise, if just permission to write, you will not be able to change or add users in the community table.

1.2.2.2 Initial set-up

All SNMP based network elements within the Cisco product portfolio require initial configuration via VT100 emulating software (for example HyperTerminal). Enclosed in box there is a special cable to connect a COM-port on a PC to VT100 port on the device. As a minimum, two configuration tasks need to be performed via local CLI, the management port needs an IP address and the community table must have an instance to enable SNMP access.

Further “how to” are explained in the Quick Reference Guide provided in paper format together with HW.

1.2.2.3 TFTP server

The TFTP server must be installed, configured and accessible to the network element and the Cisco EdgeCraft prior to running the wizard. This server may be any 3rd party TFTP server running on any computer in your network, but the CEC built-in server is recommended, as it provides all the features required by the Cisco EdgeCraft to initiate and perform a user-friendly file transfer. The Cisco EdgeCraft must be aware of the relevant TFTP server attributes (IP address, optionally default input/output directories (TFTP-root)). This is required for the system to initiate file downloads and uploads during:

- Software/firmware downloads
- Configuration backup/restore
- General block data transfers to/from the network element¹

1.2.2.4 Time protocol

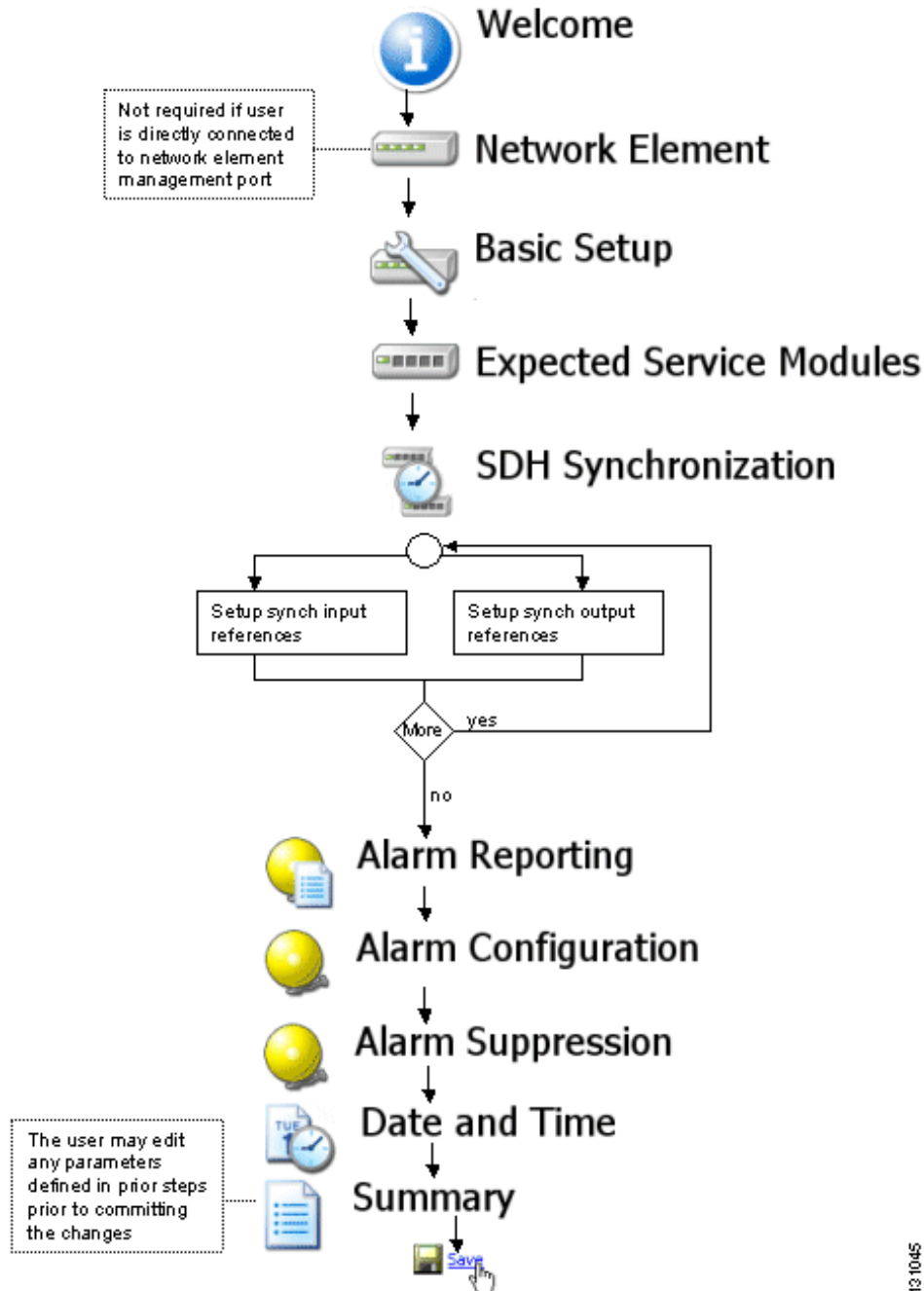
The network elements support automatic NE clock adjustments via RFC868 Time Protocol. If an external Time Protocol server is used, it must be installed, configured and accessible to the network element prior to running the Wizard.

There are various Time Protocol servers available, but following this URL web site provides a freeware Server, which can be used: <http://www.bttsoftware.co.uk/>

1. Depending on network element type and version. Used for G.826 performance data and large information model attribute tables (XC matrixes etc.)

1.2.3 Basic flow

Figure 1-10 Commissioning wizard - Basic flow

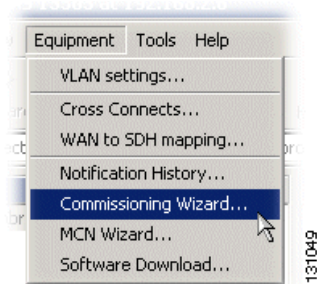


1.3 Commissioning Wizard - Step By Step

1.3.1 Opening The Commissioning Wizard

Step 1 Select **Equipment > Commissioning Wizard** in the menu bar like in the figure below.

Figure 1-11 Equipment menu



1.3.2 Welcome

Please read the introduction found in the appearing Welcome window (see figure below).

Figure 1-12 Commissioning wizard- Welcome window

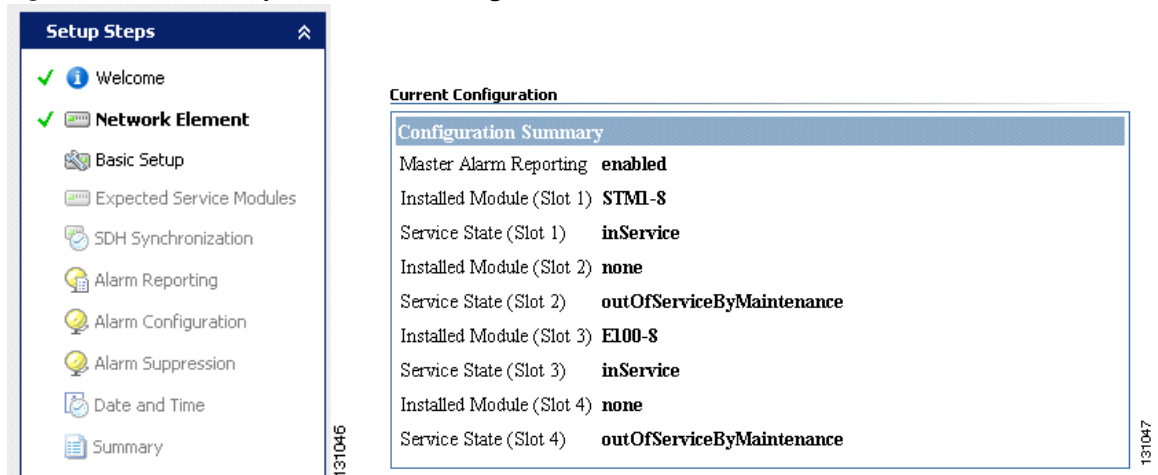


Step 2 Click “Next” to proceed.

1.3.3 Network Element

This step lists the current configuration

Figure 1-13 Example of Current Configuration



Step 1 View current configuration summary.

Step 2 Click **Next** to proceed.

1.3.4 Basic Setup

In this step you define the privileges of the SNMP users, and allows you to input a network element description. The order of the steps is not significant.

1.3.4.1 Network Element Information

The system presents the current network element instance description (default: blank text fields).

Figure 1-14 Network element information

Table 1-2 Network element description attributes

Parameter	Purpose	Comment
Native Name	Administratively assigned name for this managed NE.	0-160 characters.

Setup Steps

- ✓ Welcome
- ✓ Network Element
- ✓ **Basic Setup**
 - Expected Service Modules
 - SDH Synchronization
 - Alarm Reporting
 - Alarm Configuration
 - Alarm Suppression
 - Date and Time
 - Summary

Network Element Information

Native Name

Location

Owner

Edit the **network element description attributes**; Location, Native Name and Owner.

Table 1-2 Network element description attributes

Parameter	Purpose	Comment
Location	The physical location of NE.	Anything written in this field will replace the associated IP-address in management tree and graphical presentations. When entering value for location, avoid special characters such as apostrophe and quotation marks. Only use letters. 0-160 characters.
Owner	Contact person for this managed NE.	0-160 characters.

1.3.4.2 SNMP Users And Access Rights (Community Table)

In the Basic Setup windows you can also define the CEC managers that are allowed to access the network element. The system also presents the currently defined SNMP users defined in the network element.

Figure 1-15 SNMP Community table

SNMP Users and Access Rights

Id	IpAddress	Password	AccessRight	TrapsEnable
0	0.0.0.0	public	super	<input type="checkbox"/>
1	10.20.4.1	public	super	<input checked="" type="checkbox"/>

Add Row Delete Row

Step 1 You edit (create, delete, modify) each user by editing the following attributes:

Table 1-3 User description attributes

Parameter	Purpose	Comment
IpAddress	IP address of manager / trap receiver.	IP address <0.0.0.0> for an instance in community table, means that any host can connect only limited by password. Removing this address will increase security in open networks.
Password	This is a selectable password to be decided by the operator.	1-20 characters.

Table 1-3 *User description attributes (continued)*

Parameter	Purpose	Comment
AccessRights	This controls the access to MIB attributes: “readOnly”, “readWrite” and “super”.	At least one instance in the table should have super access to be able to maintain SNMP permissions for NE. Otherwise, if this is not desirable, you may configure the SNMP community table via commands in CLI via local console or Telnet.
TrapsEnable	Option to enable traps to be sent continuously to a specific host.	Current products and Software versions limit the maximum of instances in community table to 16. It is recommended no more than 3-4 with trap=enabled.

Step 2 Click **Next** to proceed to the next wizard step.

1.3.5 Expected Service Modules

In this step you set up the slots of the network element to accept their designated plug-in modules. See the [“4.11.1 View Slot” section on page 4-85](#) for details on slot management.

**Note**

This flow is valid only for Cisco network elements that support slots for plug-in modules; ONS 15305 (four slots).

The system presents the current slot configurations. The slot attributes available for presentation are:

Figure 1-16 Example of current slot configuration

Setup Steps

- Welcome
- Network Element
- Basic Setup
- Expected Service Modules**
- SDH Synchronization
- Alarm Reporting
- Alarm Configuration
- Alarm Suppression
- Date and Time
- Summary

Slot 1 Slot 2 Slot 3 Slot 4

Module State

Installed Module: STM1-8

Expected Module: STM1-8

Install State: installedAndExpected

Service State: inService

Alarm Reporting: ☐

Description: TEST

Module Hardware

Type: STM1-8

Name: 15305-51.1-8-LC

Product Number: 74-3105-01

ICS Number: A0

Serial Number: 0403009508

Module Software

Id	Name	SwType	SwVersion	Bank1productNumber	Bank1ics
1	8xSTM-1 FW	internalFirmware	05C	45004-72AA	05C

Table 1-4 Slot attributes

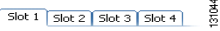
Parameter	Purpose	Comment
Slot ID	Selectable tabs for each available slot. 	Slot 1-4 for ONS 15305
Installed Module	Displays current installed module.	
Expected Module	To select desired service module from pull down menu. Enumerated list.	
Install State	Displays install state.	Possible states: <ul style="list-style-type: none"> - Empty - InstalledAndExpected - ExpectedAndNotInstalled - InstalledAndNotExpected - MismatchOfInstalledAndExpected
Service state	Displays service state.	Possible states: <ul style="list-style-type: none"> - InService - OutOfService (Fault condition present in service slot) - OutOfServiceByMaintenance (Module shutdown via Hardware switch or software) - NA (empty) - OutOfServicePending (Shutdown in progress)
Alarm Reporting	Option to enable alarm reporting of module.	If disabled this will suppress alarms related to this module.

Table 1-4 Slot attributes (continued)

Parameter	Purpose	Comment
Description	Administratively assigned name for this service module.	0-63 characters.
Hardware Inventory	Display Hardware serial no., product no., version (ICS) and type.	
Software Inventory	Display loaded Software versions in respective banks and administratively used bank.	Notice that not all Ethernet service modules have software loaded on the module itself, and hence not an applicable view for all modules.

1.3.6 SDH Synchronization

In this step you set up the reference sources for the network element built-in SDH Equipment Clock (SEC) and the network element synchronization output reference signal. See the [“4.6.1 SDH Synchronization” section on page 4-38](#) for details.

Figure 1-17 Example - current synchronization status

SEC (T0) Synchronization

Id	Slot	Port	Type	Ssm	Priority	AdminQuality	OperQuality	HoldOffTime	WaitToRestoreTime	Lockout	PortDescription
0	0	0	external	enabled	1	sec	failed	300 ms	1 min	clear	
1	5	5	stmN	enabled	1	sec	failed	300 ms	1 min	clear	

2048 kHz (T4) Synchronization

Id	Slot	Port	Type	Priority	Ssm	AdminQuality	OperQuality	HoldOffTime	WaitToRestoreTime	Lockout	PortDescription
0	0	0	internal	1	enabled	sec	sec	300 ms	1 min	clear	

Minimum Quality Level:

131048

You can read or edit (create, delete, modify) the following synch interfaces:

- The SEC (T0) reference source candidates
- The 2048 kHz (T4) reference source candidates (if applicable)
- The administrative and operative status of T0/T4 synchronization

1.3.6.1 Edit the SEC (T0) Synchronization

The synchronization source alternatives are:

- Any network element STM-1 frame
- Any network element E1 frame
- An external 2 Mb/s synch signal
- None (free running)

1.3.6.2 ONS 15305

Step 1 Define a number of synchronization sources. Parameters per source are:

Table 1-5 SEC (T0) synchronization - ONS 15305 - parameters

Parameter	Purpose	Comment
Slot	Identifier of the originating source slot position.	
Port	Identifier of the originating source port position.	
Type	Type of synchronization source. STM-n, E1-port or External Synch-port.	Notice, if desirable to use an E1-port as sync. source, PRA mode is required.
SSM	Activation of Synchronization Status Messaging.	Only applicable for STM-n type.
Lockout	Set / Clear	Set - This command is used to temporarily exclude a specified synchronization source from the selection process. Clear - This command is used to re-include a previously locked out reference source.
HoldOffTime	SEC will enter holdover mode for the specified Hold-Off time if an alarm is detected on the selected sync. reference. After the Hold-Off time the selection process will switch to the error free reference with the highest QL.	Range 300 - 1800 ms.
Wait-to-restore Time	When a nominated synchronization source recovers from an alarm condition, the signal shall be free for faults for the wait to restore time before taken into consideration by the selection process. WTR timer is configurable in the range 0-12 minutes (one minute step).	The WTR time does not apply to changes in the QL reflected by the received SSM-value (QL-PRC, QL-SSU-T, QL-SSU-L, QL-SEC, QL-DNU).
AdminQuality	Assigned quality for this reference.	Not applicable when SSM is used. Options available: - SEC - SSUL - SSUT - PRC
Priority	Source priority.	1-5.

Table 1-5 SEC (T0) synchronization - ONS 15305 - parameters (continued)

Parameter	Purpose	Comment
OperQuality	Actual state for the reference.	States: - Failed - DoNotUse - SEC - SSUT - SSUL - PRC
PortDescription	Displays description assigned the port.	

1.3.6.3 ONS 15302

Step 1 Select one synchronization source from the list of available synchronization sources.

Table 1-6 SEC (T0) synchronization - ONS 15302 - parameters

Parameter	Purpose	Comment
Administrative	Option to select the synchronization source.	Options: - Local - Active SDH (recommended when using MSP 1+1) - SDH: 1 - SDH: 2 (Hardware dependent) - PDH (E1); 1 - 12 Notice, if desirable to use an E1-port as sync. source, PRA mode is required.
Operational	Display operational synchronization source.	

1.3.6.4 Edit 2048 kHz Output (T4) Synchronization



Note

ONS 15305 only.

Step 1 Define desired number of synchronization sources. The parameter structure is equal to the T0 source structure, but the synchronization source type selection is limited to the choices SDH port or Internal Clock.
See the [“4.6.1 SDH Synchronization”](#) section on page 4-38 for more details.

Table 1-7 2048 kHz Output (T4) synch - ONS 15305 - parameters

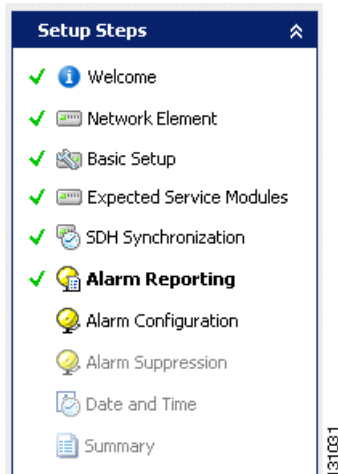
Parameter	Purpose	Comment
Slot	Identifier of the originating source slot position.	
Port	Identifier of the originating source port position.	
Type	Type of synchronization source. STM-n or Internal Clock	
SSM	Activation of Synchronization Status Messaging.	Only applicable for STM-n type. STM-n port will by default send DoNotUse. Consider this parameter changed to fit your configuration.
Lockout	Set / Clear	Set - This command is used to temporarily exclude a specified synchronization source from the selection process. Clear - This command is used to re-include a previously locked out reference source.
HoldOffTime	SEC will enter holdover mode for the specified Hold-Off time if an alarm is detected on the selected sync. reference. After the Hold-Off time the selection process will switch to the error free reference with the highest QL.	Range 300 - 1800 ms.
Wait-to-restore Time	When a nominated synchronization source recovers from an alarm condition, the signal shall be free for faults for the wait to restore time before taken into consideration by the selection process. WTR timer is configurable in the range 0-12 minutes (one minute step).	The WTR time does not apply to changes in the QL reflected by the received SSM-value (QL-PRC, QL-SSU-T, QL-SSU-L, QL-SEC, QL-DNU).
AdminQuality	Assigned quality for this reference.	Not applicable when SSM is used. Options available: - SEC - SSUL - SSUT - PRC
Priority	Source priority.	1-5.

Table 1-7 2048 kHz Output (T4) synch - ONS 15305 - parameters (continued)

Parameter	Purpose	Comment
OperQuality	Actual state for the reference.	States: - Failed - DoNotUse - SEC - SSUT - SSUL - PRC
PortDescription	Displays description assigned the port.	

1.3.7 Alarm Reporting

In this step you configure the base unit alarm reporting enable/disable. Power modules are considered as a part of base unit.

Figure 1-18 Alarm Reporting
Note

Slot/module alarm reporting settings (enable/inhibit) is included in the “Expected service module” setup (see the [“1.3.5 Expected Service Modules”](#) section on page 1-23), and not this step.

The system presents the standard mode alarm configuration settings.

You can edit the following standard alarm configuration:

1.3.7.1 Power Module Alarms

Power module alarm settings for up to two power modules. (ONS 15305 only).

Figure 1-19 Alarm reporting - power modules

Power Module1 Type 48V DC Alarm Reporting <input type="checkbox"/> Input A <input type="checkbox"/> Input B <input type="checkbox"/>	Power Module2 Type 48V DC Alarm Reporting <input type="checkbox"/> Input A <input type="checkbox"/> Input B <input type="checkbox"/>
---	---

131034

Table 1-8 Alarm reporting - power modules

Parameter	Purpose	Comment
Type	-48VDC or 230 VAC.	Read only
Alarm Reporting	Enable/disable alarm reporting	Master Alarm per power module
Input A	Enable/disable alarm reporting from input A	
Input B	Enable/disable alarm reporting from input B	

1.3.7.2 Alarm Ports

Alarm ports (4 external alarm input ports) setup.

Figure 1-20 Alarm reporting - external alarm input ports

Alarm Port 1 Alarm Reporting <input checked="" type="checkbox"/> Triggered When opens Description opens closes	Alarm Port 2 Alarm Reporting <input checked="" type="checkbox"/> Triggered When closes Description
Alarm Port 3 Alarm Reporting <input type="checkbox"/> Triggered When closes Description	Alarm Port 4 Alarm Reporting <input type="checkbox"/> Triggered When closes Description

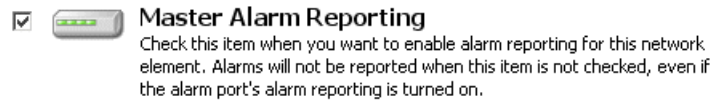
131033

Table 1-9 Alarm reporting - alarm ports

Parameter	Purpose	Comment
Alarm Reporting	Alarm port enable/disable	
Triggered When	Alarm when alarm loop opens/closes	Alarm triggering strategy
Description	Alarm port description	0-63 characters

1.3.7.3 Master Alarm Reporting

Figure 1-21 Master alarm reporting

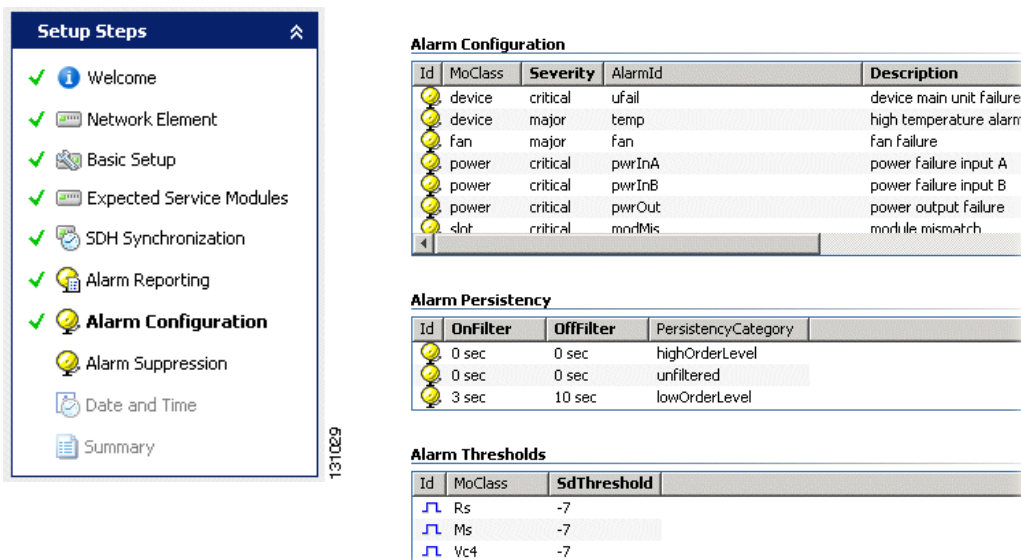


131032

1.3.8 Alarm Configuration

This step makes it possible for an operator to modify default settings of severity, description, threshold and suppression of alarms. The following configuration choices is presented by the system:

Figure 1-22 Overview - alarm configuration choices



131030

1.3.8.1 Alarm Configuration (Severity List)

Table 1-10 Alarm severity - parameters

Parameter	Purpose	Comment
MoClass	Display object type	
AlarmId	Abbreviation of alarm type	Identified as “ProbCause” in alarm table.

Table 1-10 Alarm severity - parameters (continued)

Parameter	Purpose	Comment
Severity	Set alarm severity	minor-major-critical
Description	Provide explanatory text for alarm.	Identified as “ProbCauseQ” in alarm table.0-64 characters.

1.3.8.2 Alarm Persistency

Alarm persistency defines how long time an alarm has to be stable until the network element will generate an alarm notification, or how long time an alarm situation must have ceased until the network element will generate an alarm cleared notification. Persistency is configured separately for alarm and alarm clear situations, and is implemented by the two filters `highorderlevel` and `loworderlevel`:

Table 1-11 Alarm persistency - parameters

Parameter	Purpose	Comment
PersistencyCategory	Displays category	Applicable categories: - <code>highorderlevel</code> - <code>unfiltered</code> - <code>loworderlevel</code>
OnFilter	Seconds to wait until an alarm is raised.	0 - 30 seconds.
OffFilter	Seconds to turn off an alarm when cleared.	0 - 30 seconds.

Table 1-12 Persistency category

Persistency category	Alarm types	Managed objects
High order level	LOS	SDH Port, PDH Port
	LOF	RS
	AIS	MS
	EXC,DEG	RS, MS
	TIM	RS
	RDI	MS
	CDF	RS, MS
	AUX	Aux Port

Table 1-12 *Persistency category (continued)*

Persistency category	Alarm types	Managed objects
Unfiltered	LOP	TU4, TU3, TU12
	LOM	VC4
	LOF-RX, LOF-TX	E1
Low order level	AIS	TU4, TU3, TU12, E1, E3
	EXC, DEG	VC4, VC3, VC12
	SSF	VC3, VC12
	TIM, RDI, UNEQ, PLM	VC4, VC3, VC12

1.3.8.3 Alarm Thresholds

Some alarms are generated when a performance measurement crosses a predefined threshold. In the Cisco network elements, this threshold is configured, quality measurements on the SDH frames are associated with alarm threshold according to the listing below:

Table 1-13 *Alarm threshold - parameters*

Parameter	Purpose	Comment
MoClass	Display object type	
SD Threshold	Threshold for a DEG alarm to be reported.	<p>10E-6 to 10E-9.</p> <p>For example, if set to 10E-7, an alarm is raised when BER exceeds this threshold.</p> <p>To clear, the BER level must be improved by a factor 10.</p>

1.3.9 Alarm suppression

The alarm suppression is invoked per alarm instance or per class/group of alarms.

Figure 1-23 Example - alarm suppression

Setup Steps

- Welcome
- Network Element
- Basic Setup
- Expected Service Modules
- SDH Synchronization
- Alarm Reporting
- Alarm Configuration
- Alarm Suppression
- Date and Time
- Summary

VC Alarms

Id	MoClass	DegAlarms	SsfAlarms	ExcAlarms	RdiAlarms
Vc4		allow	allow	allow	supress
Vc3		allow	allow	allow	supress

TU/AU Alarms

Id	AisAlarms
	allow
	allow

E1 Alarms

Id	Slot	Port	MoClass	AisAlarms
3	1	E1		supress
3	2	E1		supress

AUX Alarms

Id	RaiAlarms	AisAlarms
	allow	supress
		allow
		supress

1.3.9.1 VC Alarms

Table 1-14 Alarm suppression - VC

Parameter	Purpose	Comment
MoClass	Display object type.	
DegAlarms	Suppress or allow BER-DEG alarms to be reported.	
SsfAlarms	Suppress or allow signal server failure to be reported.	
ExcAlarms	Suppress or allow BER-EXC alarms to be reported.	10E-5 threshold level for the EXC alarms to be reported.
RdiAlarms	Suppress or allow RDI alarms to be reported.	

1.3.9.2 TU/AU Alarms

Table 1-15 Alarm suppression - TU/AU

Parameter	Purpose	Comment
AisAlarms	Suppress or allow AIS alarms to be reported.	

1.3.9.3 E1 Alarms

Table 1-16 *Alarm suppression - E1*

Parameter	Purpose	Comment
MoClass	Display object type.	
Slot	Identifier of the E1 slot position.	
Port	Identifier of the E1 port position.	
AisAlarms	Suppress or allow AIS alarms to be reported.	

1.3.9.4 AUX Alarms

Table 1-17 Alarm suppression - AUX

Parameter	Purpose	Comment
RaiAlarms	Suppress or allow RAI alarm to be reported.	Not supported by ONS 15302.
AisAlarms	Suppress or allow AIS alarm to be reported.	Not supported by ONS 15302.

1.3.10 Date And Time

Figure 1-24 Date and time - example

Date and Time

This step allows you to set the date and time of the selected network element. If desired, the date and time can be automatically synchronized to an IETF RFC 868 Time Protocol Server.

☒ **No Change**
Select this item if you do not wish to set the date and time for the selected network element.

☐ **Synchronize to Server Time**
Sets Network Element real time clock to the time of the machine running element manager/network manager.
Current Server Time: 2004/04/19 12:51:54

☐ **Synchronize to Time Protocol Server**
Select this item if you want to automatically synchronize the Network Element clock with a Time Protocol server. You will need to specify the IP address of the server and the synchronization interval.

IP Address:

Synchronization Interval:

Current Date and Time on Network Element

Date and Time: 2004/04/19 12:52:48
Total Up-time: 5 days, 23 hours, 42 minutes, 24 seconds

In this step you manually set the time and date of the network element, or set up the system for automatic time synchronization to an IETF RFC868 Time Protocol server.

The system presents the available time and date relevant attributes:

- Total up-time
- Time and Date

Automatic setting of time/date:

- IP address of RFC868 Time Protocol sever
- Time synchronization interval

Step 1 Select time/date reference sources: **Server Time, Time Protocol Server or No Change.**

Step 2 If **Server Time** is selected, the system uses the TMN local time/date settings to set the network element time/date attributes. Network Element time/date is set when committing the commissioning flow.

- Step 3** If **Time Protocol Server** is selected, you specify the **IP address** of the RFC868 Time Protocol server, and the **synchronization interval** (how often the TP server is accessed by the network element) in minutes.
- Step 4** **Other settings** than Time Server based or Local Time based is not supported by the commissioning wizard, and must be set up through the **Management Tree**.

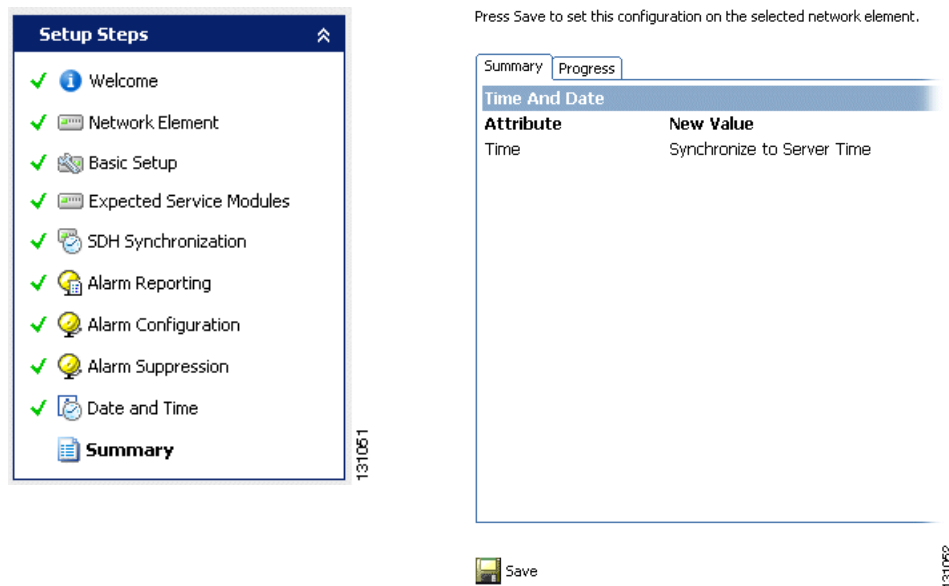
**Note**

Setting the TP server synchronization interval to 0 is equal to selecting disabling Time Server controlled configuration of time and date.

The network element does not support daylight savings time (summer time). Switching between summer and winter time will be the task of the time protocol.

1.3.11 Summary

Figure 1-25 Summary report - example



When the Commissioning wizard sequence is completed you should review the configuration before committing the changes to the network element.

The wizard presents a report of all configuration changes registered to the configuration during the Commissioning wizard flow.

Review the configuration and do one of the following:

1.3.11.1 Commit Configuration

- Step 1** If further editing of the configuration is required, you may return to any step for re-configuration before returning to this step and finally committing the configuration or,
- Step 2** If the configuration is satisfactory, click “**Save**” to commit the configuration to the network element.

- When commissioning a new network element, the system downloads the entire configuration to the network element.
- 2When editing an existing configuration, the system only downloads the configuration changes to the network element.

1.3.11.2 Result Of The Commissioning

The network element basic configuration is completed. The network element is ready to be set up for use in a network.

1.3.11.3 Basic Network Element Set-up

The connected IP address and sub-net address of the network element is defined. Site specific information is specified for the network element.

1.3.11.4 TFTP Server

The network element is ready to use a specific TFTP server for file upload/download.

1.3.11.5 Expected Service Module (ONS 15305 only)

The network element is set up and ready to receive its designated plug-in module.

1.3.11.6 SDH Synchronization

The network element T0 and T4 clocks are set up with their designated synchronization references and synchronization strategies.

1.3.11.7 Alarm Reporting

The network element alarm system is configured according to the alarm notification strategy of the network.

1.3.11.8 Time

The network element is configured to use an external time protocol server, or the time and date is set manually.

1.3.11.9 Failures And Exceptions

When committing the configuration, the system register all configuration failures and provides an error log/report at completion, specifying what went wrong, if anything.



Software Description

This section gives an overview of the Cisco Edge Craft with its features.

2.1 Introduction

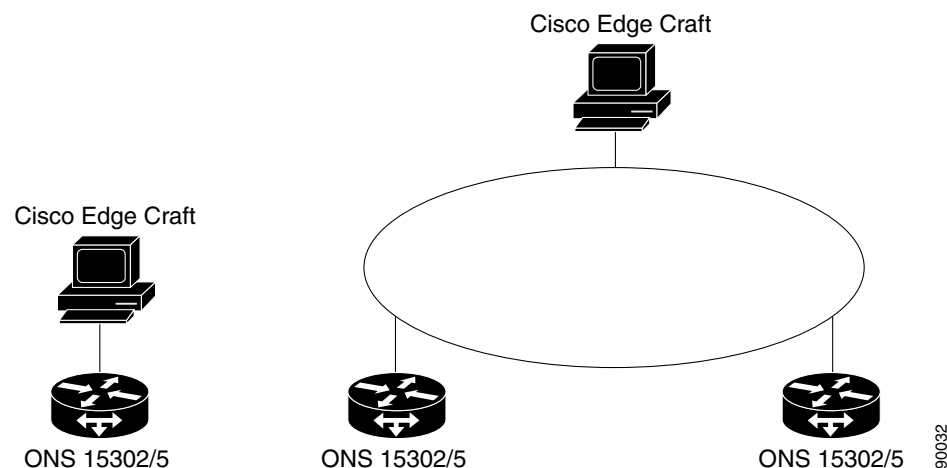
Cisco Edge Craft is used to get one, single network element at the time into operation. Cisco Edge Craft can only present and work on information that are stored on the network element. A user must be logged onto Cisco Edge Craft graphical user interface (GUI) for it to function. The GUI present alarms as long as Cisco Edge Craft is connected to the network element. Performance data can be loaded from the network element and presented.

The Cisco Edge Craft presents the current (a snapshot) situation on the network element, and has very little added value functions apart from the functions on the network element.

Cisco Edge Craft is a single user system. It is a standalone application running on Windows platform or Solaris platform.

Cisco Edge Craft is a totally self contained product. It is not dependent on any other system to be able to perform its tasks. The laptop or a PC, at which 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



It can co-exist together with other management products from Cisco. The SNMP Agent used by Cisco Edge Craft for communication with the network element, handles multiple SNMP Managers.

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 if the feature is available on the network element. In the remaining part of this chapter, Cisco Edge Craft is called “the system”.

2.2.1 Network Element Access

The system communicates with the network element through the embedded SNMP Agent. To establish this communication line the network element must have been assigned an IP address. In situations where assignment has not been done a separate communication line on the serial port is used to perform the assignment of the IP address and other related parameters.

2.2.2 Information Model

The system 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 products in the Cisco Family.

2.2.3 Single User

Only one user can be logged onto the system at the time.

2.2.4 Single Network Element

The system can only communicate with one network element at the time. The user closes the connection with one element before connecting to a new network element.

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.

GUI cannot be customized by the user.

The system has two different types of graphical user interfaces (GUI).

2.2.5.1 Network Element topology Browser (NETB)

A hierarchical presentation of the managed objects in the network element.

2.2.5.2 Custom GUI to Support a Specific System Feature

A GUI developed to support a specific task/function.

2.2.6 No Persistency

The system has no persistent storage of operations and notifications.

2.2.7 List of Possible Network Element IP Addresses

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

2.2.8 Configuration Download and Upload

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

The system 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 can not be edited.

2.2.9 Software and Firmware Download

The system can initiate download of software and firmware onto the network element. The location of the software and firmware can either be on the same computer as the system is running on, or on a remote computer. The remote computer is identified by its IP address and 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

The system 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

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

The system 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

The system has no analysis of performance management data.

The user can read the current registered performance data on the network element, get it presented in a GUI, and copy it to file. The file can be read or edited in any tool, for example Microsoft Excel.

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

2.2.13 Management Configuration

The system supports configuration of the DCN management traffic settings.

2.2.14 Physical Inventory

The physical inventory gives an overview of the physical installed parts on the network element and the currently running software or firmware. Eventual downloaded not yet activated software and firmware packages are also presented.

2.2.15 Logical Inventory

The logical inventory gives an overview of the managed entities that the network element consists of. The logical entities may concur 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 of the network element. These are parameters like location, owner, time server, LED settings, power modules, etc.

2.2.17 Alarm and Event Filtering Configuration on Network Element

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

2.2.18 SDH Ports Configuration

The system 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

The system supports configuration of PDH ports properties. The properties can be viewed and edited.

2.2.20 MSP and SNCP Configuration

The system supports configuration of MSP and SNCP set-up, that means 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. The system helps the user in the set-up of these rules.

2.2.22 LAN Ports Configuration

The system supports configuration of LAN ports properties. The properties can be viewed and edited.

2.2.23 WAN Ports Configuration

The system supports configuration of WAN ports properties. The properties can be viewed and edited. The system also supports configuration of WAN bandwidth.

2.2.24 Test Loops Configuration

The system supports configuration of test loops.

2.2.25 Cross Connect (XC) Configuration

The system supports cross connection management for the SDH ports. The XCs can be set, deleted, updated. Two supported XC's are:

- Point-to-point
- WAN to SDH mapping

2.2.26 Bridge Configuration

The system supports the set-up of the bridge.

2.2.27 VLAN Configuration

The system supports configuration of VLAN, that means, create, remove, and update VLANs.

2.2.28 Security

The security of Cisco Edge Craft is based on the SNMP v.1 security, that means community string.

2.2.29 Data Communication

Cisco Edge Craft can communicate with the network elements

- Directly on the management port
- The management port can be connected to a VLAN
- Inband DCC

2.2.30 Reliability

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

Redundancy

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

Bugs

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.

Debugging

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

System Logging

- All system errors are logged.

- The system 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.

New Releases and Patches

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



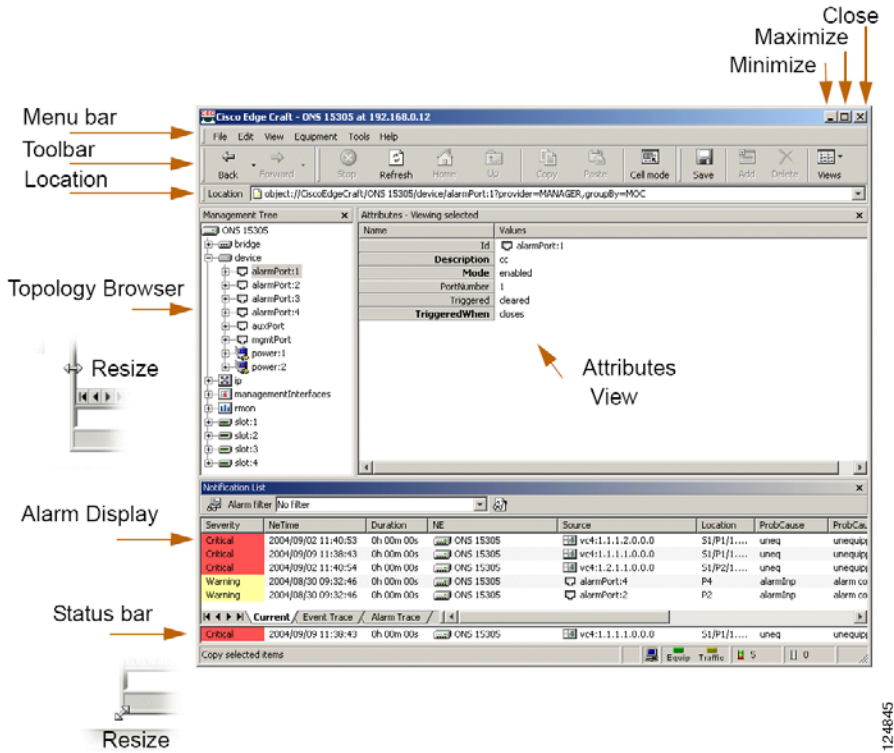
Using Cisco Edge Craft

This chapter contains information about how to use the Cisco Edge Craft software. You will learn how to navigate on the Desktop and use the Management Tree, Attributes view and the Alarm view.

3.1 Cisco Edge Craft Desktop

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 Management Tree, 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. [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 button or menu item.

Figure 3-1 Cisco Edge Craft Desktop Overview



3.1.1 Toolbar Buttons

The table below shows the functionality of the icons which are used in the Cisco Edge Craft.

Table 3-1 Toolbar buttons

	Move up one level in topology.
	Stop the current operation.
	Refresh the active view.
	Copy selected row(s) to the system clipboard.
	Move Forward in Attributes Viewer.
	Move Backward in Attributes Viewer.
	Save the content of the Attributes View on the equipment.
	Add a new row to the Attributes View.

124845




	Move up one level in topology.
	Delete selected item(s).
	By default, entire rows are selected in table, but single cells can easily be selected using the cell-mode toggle button.

Figure 3-2 and Figure 3-3 show the functionality how to Move and Lock toolbars.

Figure 3-2 Move Toolbars

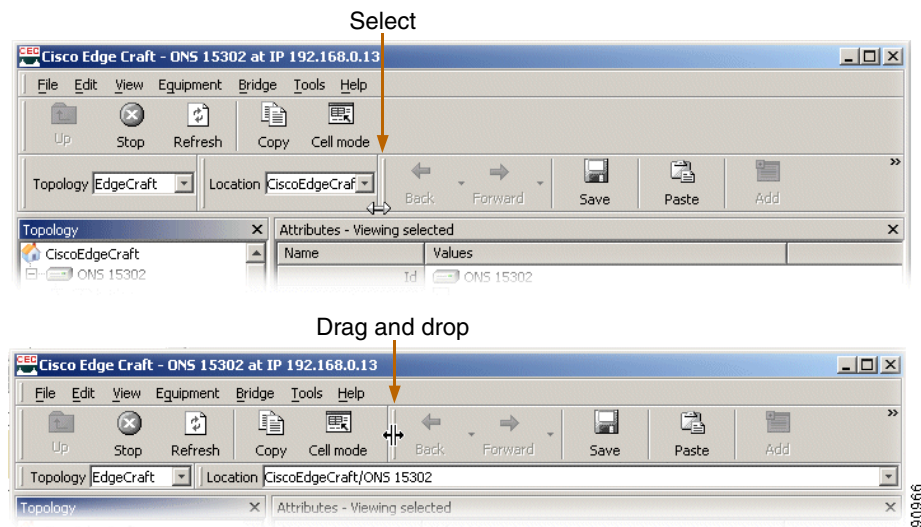
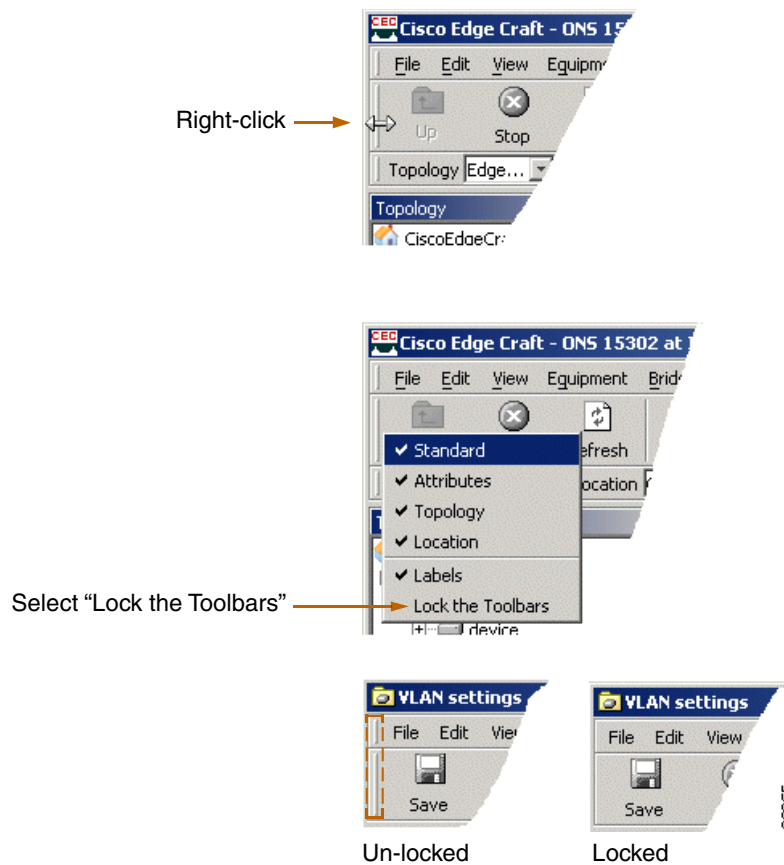


Figure 3-3 Lock Toolbars

3.1.2 Menu Items

This section gives an overview and explains the different menu items.

3.1.2.1 File

Figure 3-4 and Table 3-2 show and explain the functionality of the menu File.

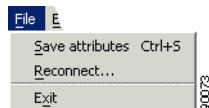
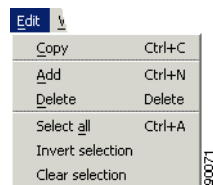
Figure 3-4 Pull Down Menu File

Table 3-2 **Menu File**

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

3.1.2.2 Edit

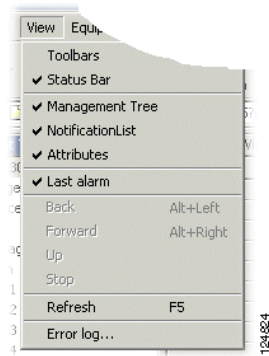
Figure 3-5 and Table 3-3 show and explain the functionality of the menu edit.

Figure 3-5 **Pull Down Menu Edit****Table 3-3** **Menu Edit**

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

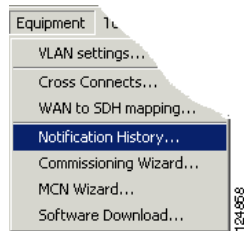
Figure 3-6 and Table 3-4 show and explain the functionality of the Menu View.

Figure 3-6 Pull Down Menu View**Table 3-4 Menu View**

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.
Management Tree	Check to make Management Tree an active application on the desktop.
Attributes	Check to make attributes viewer an active application on the desktop.
Columns	Toggle visible columns in alarm display. Please see the “Visible Columns” section on page 3-17 for details.
Last Alarm	Check to view last alarm in separate window in the alarm display.
Back	Move back.
Forward	Move forward.
Up	Move up one level.
Stop	Stop current operation.
Refresh	Refresh the active view.
Error Log	Open error log. The log is also available from the status bar. These symbols indicates severity in the status bar. Double-click current symbol to view log.

3.1.2.4 Equipment

Figure 3-7 and Table 3-5 show and explain the functionality of the menu Equipment.

Figure 3-7 Pull Down Menu Equipment**Table 3-5 Menu Equipment**

Menu item	Action
VLAN Settings	Open VLAN Settings GUI. Please see the “7.4 VLAN Provisioning” section on page 7-12 for details on VLAN Settings.
Cross Connect	Open Cross connect GUI. Please see the “5.6 ONS 15305 SDH Cross-Connection Management” section on page 5-16 for details on Cross Connects
WAN to SDH mapping	Open WAN to SDH mapping GUI. Please see the “5.15.3 Add Initial WAN Port Capacity” section on page 5-57 for details.
Notification History	Open Notification History GUI. Please see the “History” section on page 3-13 .

3.1.2.5 Tools

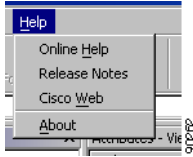
[Figure 3-8](#) and [Table 3-6](#) show and explain the functionality of the menu Tools.

Figure 3-8 Pull Down Menu Tools**Table 3-6 Menu Tools**

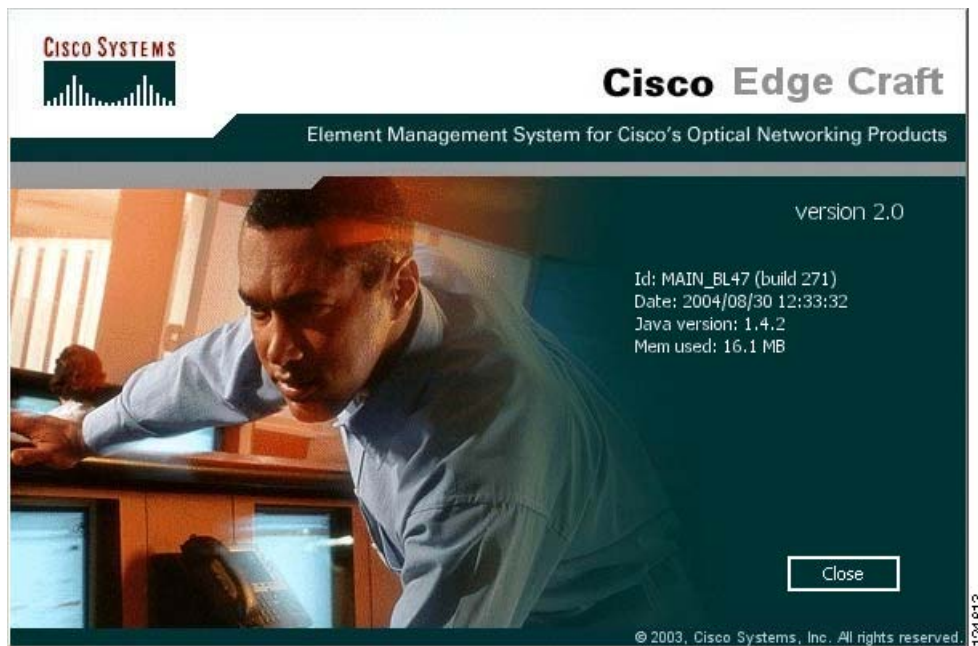
Menu item	Action
VT 100 Terminal	If configured, the VT100 terminal launches. Please see the “1.1.6 Configuration of VT100 Terminal” section on page 1-16 for details.
Text Editor	Open Text Editor.

3.1.2.6 Help

[Figure 3-9](#) and [Table 3-7](#) show and explain the functionality of the menu Help.

Figure 3-9 Pull Down Menu Help**Table 3-7 Menu Help**

Menu item	Action
Online Help	Launches Cisco Edge Craft User Guide online.
About	Launches information of installed Cisco Edge Craft software, Figure 3-10 .






Figure 3-10 The About box - Example

3.1.2.7 Log Viewer

[Table 3-8](#) shows and explains the functionality of the log viewer icons.

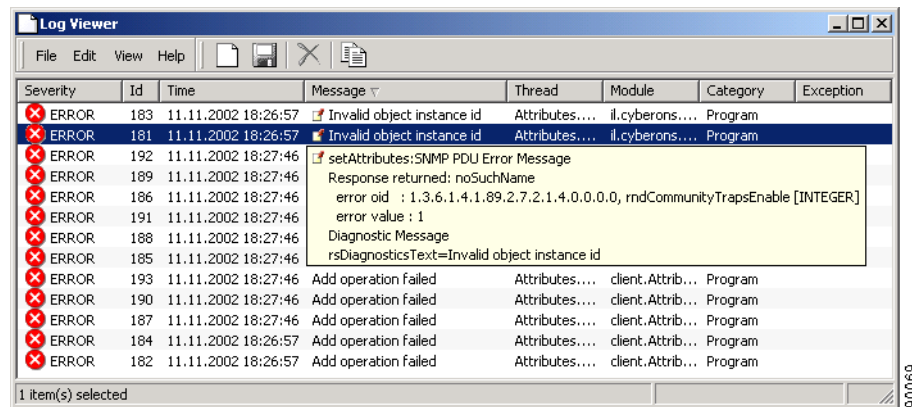
These symbols indicate severity in the status bar, if the log contains messages:

Table 3-8 Log Viewer Icons

	An error messages occurs.
	A warning message occurs.
	Information is available.
	Unmapped severity information is available.
	If this icon occurs additional information is available.

- Step 1** Double-click current symbol to view log.
- Step 2** Messages marked with the note icon contain additional information.
- Step 3** Click note icon to view hyper link.

Figure 3-11 and Figure 3-12 show details of the lock viewer function.

Figure 3-11 Log Viewer

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

Figure 3-12 Log Viewer - Tool tip








:

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 cells copied from. If not, you are asked if you would like to copy the data based on the column names. Only editable columns with the same name and data type will be then be pasted. This enables copying and pasting between tables with the same data but with different column order, [Figure 3-13](#).

Figure 3-13 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 table, but single cells can easily be selected using the cell-mode toggle button.

The feature enables copying one table cell, selecting the entire column, press Paste and copying the value into all selected cells. Copy and paste of ranges are also supported. Thus you can copy values A and B and paste them into a large range in order to get the A and B values repeated throughout the range.

Copy and paste to an external applications such as Microsoft Excel.

3.1.5 Navigation in Tables Using the Keyboard

Cell in focus is easily spotted and the arrow-keys can be used to move the cursor (applies for editable tables only). Editing of selected cell is easily available via Enter or F2. The Tab-key can be used for moving to the next editable cell (from left to right and top to bottom). The selection is circular, meaning when last editable cell on the last row is reached, the first editable cell in the first row will be activated.

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

3.1.6 Auto Fit Column Width

Double-clicking on 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 this can be achieved by holding down the Shift key while double-clicking.

3.2 Management Tree

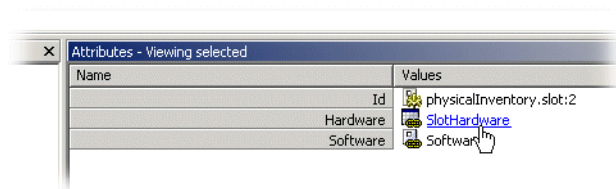
The Management Tree shows the hierarchy of managed entities, for example, LAN ports, VLANs, bridge, etc. on the current network element. The operator can view the entire hierarchy, or use any of the pre-defined views to only view managed entities of a certain type, for example only view the LAN ports.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

Clicking on the device folder in the Management Tree shown in [Figure 3-1](#), will display all alarm-, aux- and management port(s). Clicking on 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 different configuration tasks using the Management Tree are thoroughly shown in the following chapters.

The combination of the Management Tree and attribute panes will work similar to Windows Explorer, only that it shows the contents of a network element instead of files in the file system.

Figure 3-14 Editable Types and Tables - Hyperlinks



All links to editable complex types and tables are visualized as hyperlinks, [Figure 3-14](#).

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

3.2.1 Opening Links in a New Window

By selecting a managed object instance and right clicking you can select **Open in new window**. A new AttributesViewer displaying selected managed object is opened. This enables you to easily compare values on different managed objects.

3.3 Alarm Display

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

In addition the history of all alarms are presented. 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 duration. Events report other situations in the network element that are not failures. An event has a status, [Figure 3-1](#).

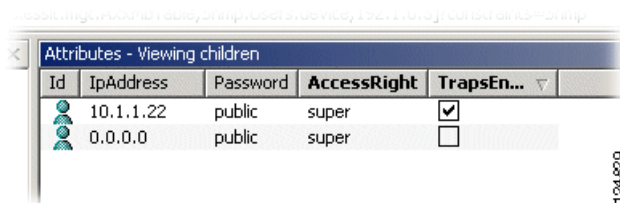
3.3.1 View Current Alarms

To view the current alarms, follow the steps described below.

3.3.1.1 Subscription of Alarms

-
- Step 1** Log in to target network element, see section Set up the connection to a network element.
- Step 2** You must manually register Cisco Edge Craft a subscriber to alarms and events from the network element. The registration is done by setting the device>users>snmp>**TrapsEnable** attribute to trapsEnable, [Figure 3-15](#).

Figure 3-15 *Setting the TrapsEnable Attribute*



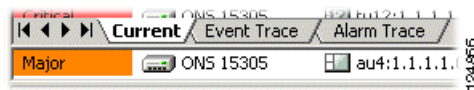
- Step 3** Click **Save**.
- Step 4** When the registration has been done, Cisco Edge Craft polls the element for all current alarms and starts sending alarms and events to the IP address of Cisco Edge Craft.

The SNMP traps are mapped to Notifications in Cisco Edge Craft. The mapping philosophy is described in the [“3.3.3 Notification” section on page 3-19](#).

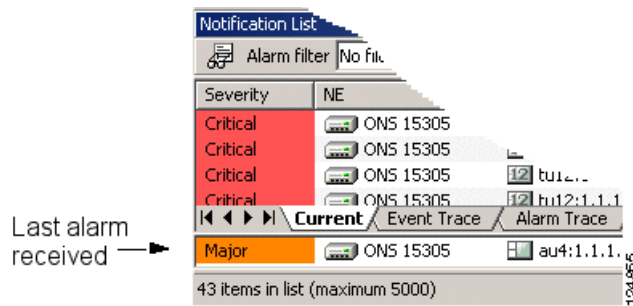
You can view the list of current alarm notifications by selecting current alarm in the notification list.

3.3.1.1.1 View Alarms

Click on the **Current** tab to view current alarms, [Figure 3-16](#).

Figure 3-16 Current Tab - Alarm List

The latest alarm is visible in lower part of the Alarm List, [Figure 3-17](#).

Figure 3-17 Latest Alarm

Refresh

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

History

To get 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


Select **History** in the notification list to get 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.

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.

The history log on the network element can be cleared through an action on the log administration attribute of the device. See the [“4.5 Manage Common Parameters”](#) section on page 4-25.

Step 1 Select **Notification History** in the **Equipment menu**, [Figure 3-18](#).

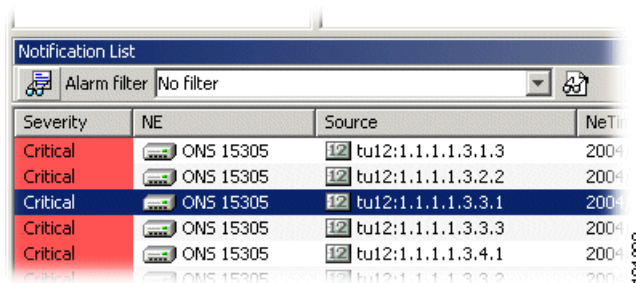
Step 2 Select **Refresh**.



The screenshot shows the 'Equipment' menu with the following options: 'VLAN settings...', 'Cross Connects...', 'WAN to SDH mapping...', 'Notification History...' (highlighted with a blue bar), 'Commissioning Wizard...', 'MCN Wizard...', and 'Software Download...'. A black arrow points to the 'Notification History...' option. The IP address '124.96.8' is visible in the bottom right corner of the screenshot.

Single Selection

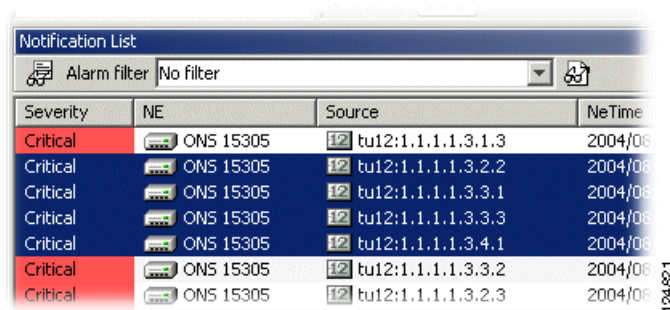
Figure 3-19 Select Single Alarm



Step 1 Right click and choose **Select all**, [Figure 3-20](#).

- Copy
- Refresh
- Select all
- Invert selection
- Clear selection

Step 2 Click on first alarm in a continuous range, hold Shift key and click on last alarm in desired range, [Figure 3-21](#).

Figure 3-21 Select Alarms - Continuous Range


Severity	NE	Source	NeTime
Critical	ONS 15305	tu12:1.1.1.1.3.1.3	2004/08
Critical	ONS 15305	tu12:1.1.1.1.3.2.2	2004/08
Critical	ONS 15305	tu12:1.1.1.1.3.3.1	2004/08
Critical	ONS 15305	tu12:1.1.1.1.3.3.3	2004/08
Critical	ONS 15305	tu12:1.1.1.1.3.4.1	2004/08
Critical	ONS 15305	tu12:1.1.1.1.3.3.2	2004/08
Critical	ONS 15305	tu12:1.1.1.1.3.2.3	2004/08

or

- Step 3** Click on first alarm, hold Ctrl key and click on desired alarms to make a none continuous selection, [Figure 3-22](#).

Figure 3-22 Select Alarms - None Continuous Range


Severity	NE	Source	NeTime
Critical	ONS 15305	tu12:1.1.1.1.3.1.3	2004/08
Critical	ONS 15305	tu12:1.1.1.1.3.2.2	2004/08
Critical	ONS 15305	tu12:1.1.1.1.3.3.1	2004/08
Critical	ONS 15305	tu12:1.1.1.1.3.3.3	2004/08
Critical	ONS 15305	tu12:1.1.1.1.3.4.1	2004/08
Critical	ONS 15305	tu12:1.1.1.1.3.3.2	2004/08
Critical	ONS 15305	tu12:1.1.1.1.3.2.3	2004/08
Critical	ONS 15305	tu12:1.1.1.1.3.2.1	2004/08
Critical	ONS 15305	tu12:1.1.1.1.3.1.2	2004/08

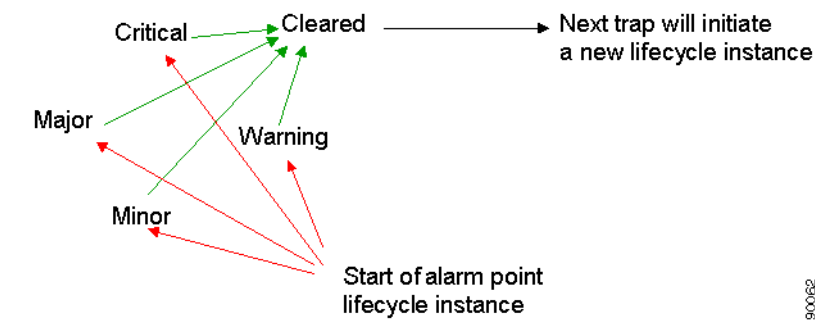
You can also choose **Invert selection** or **Clear selection**.

Copy alarm(s)

- Step 1** Select desired alarm(s).
- Step 2** Click **Copy**.
- Step 3** The content of your selection is copied to the clipboard and can be pasted to other applications, for example Notepad.

3.3.1.3 Alarm Lifestyle

Figure 3-23 Lifecycle Instance of Alarm Point



The notification list presents one row for each alarm point, that means, an alarm source and an alarm identification combination. When a new alarm notification for the same alarm point is being presented, the row is possibly updated with the severity of the new alarm and new timestamp(s) unless the alarm has been cleared. A new row is created if the alarm point starts a new lifecycle instance, [Figure 3-23](#). Each new alarm notification might cause a transition from one severity to another or to the cleared severity, which ends the lifecycle.

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

3.3.2 View the Events Reported From the Network Element

Current Events

To view current events reported from the network element, you select **Event Trace** in the notification list, [Figure 3-24](#) and [Figure 3-25](#).

Figure 3-24 Select Events

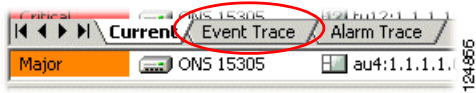


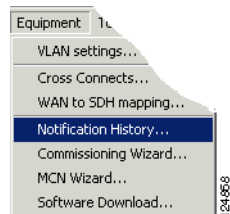
Figure 3-25 Current Events

Alarm display			
Id	Moid	Description	EventType
985	mgmtPort	Link Up	equip
986	dccR:1.1.1.1	Link Down	equip
987	dccM:1.1.1.2	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

Event History

Select **Notification History** from the **Equipment Menu** and click **Event tab** to view event history, [Figure 3-26](#).

Figure 3-26 Event History



Details about the attributes of the event notifications are found in [Table 3-9 on page 3-20](#).

Visible Columns

You can decide which columns you want to be visible in the alarm display.

-
- Step 1** Select **View > Columns**
- Step 2** Uncheck desired column and this column will not be visible in the alarm display.
- Current alarms and history of alarms is available in [Figure 3-27](#).
- Events and events history is displayed in [Figure 3-28](#).

Figure 3-27 Visible Columns 1

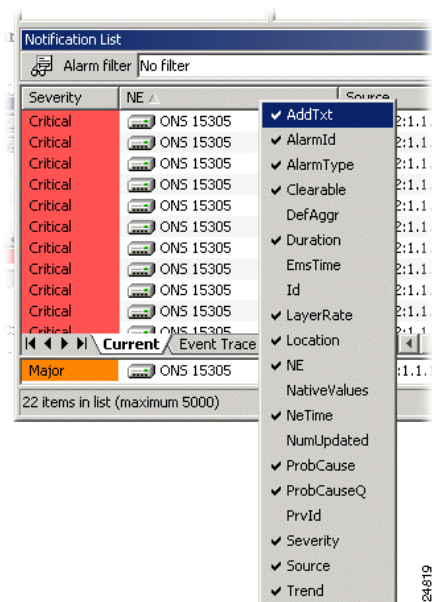
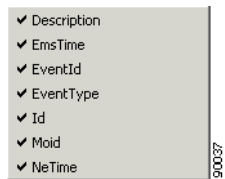


Figure 3-28 Visible Columns 2

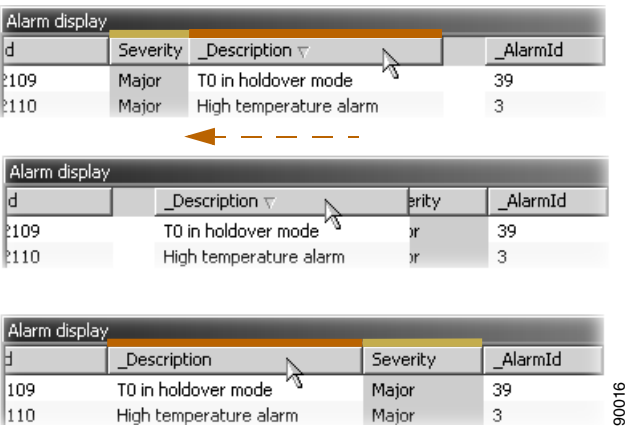


Change Column Order

The order of selected columns can be easily changed, [Figure 3-29](#).

- Step 1** Click on desired column heading.
- Step 2** Drag column to new position.

Figure 3-29 Column Order



Column Resize

- Step 1** Rest the mouse pointer to the right of desired column header. The mouse pointer turns into a double-arrow, [Figure 3-30](#).
- Step 2** Click and drag to suitable column-size.

Figure 3-30 Column Resize

Alarm display

NeTime	Moid	AlarmId	Clear
25.11.2002...	vc12:2.9.1...	Mi... 1.1.19	true
25.11.2002...	vc12:2.9.1...	Mi... 1.1.19	true
25.11.2002...	vc12:2.9.1...	Mi... 1.1.19	true
25.11.2002...	vc12:2.9.1...	Mi... 1.1.19	true
25.11.2002...	vc12:2.9.1...	Mi... 1.1.19	true
25.11.2002...	vc12:2.9.1...	Mi... 1.1.19	true

Alarm display

NeTime	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

Sort Columns

- Step 1** Click on desired column to sort ascending, [Figure 3-31](#).
- Step 2** Click again to sort descending

Figure 3-31 Column Sorting

Severity

Major
Major
Major
Critical

Severity

Major
Major
Major
Critical

Severity

Critical
Major
Major
Major

3.3.3 Notification

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

- Current alarm notification, [Table 3-9](#).
- Event trace notification, [Table 3-10](#).
- Alarm trace notification

Notification Types

Table 3-9 Notification Types

Attribute		Legal Values
Name	Description	
AckSign	Acknowledge signature	Userid (automatic)
AckTime	Acknowledge time	yyyy/mm/dd hh:mm:ss (server time)
Acked	A check when alarm is acknowledged	Checked/ Unchecked
AddTxt	Additional text (free form text description)	
AlarmId	Unique identification of alarm	
AlarmType	Alarm grouped into categories	Equip(-ment), env(-ironment), comm(-unication), process
Clearable	Boolean value to indicate if the alarm can be cleared or not. Some alarms does not have duration and therefore no Cleared severity	Checked/ Unchecked
Comment	Manual added text as comment to alarm	Text (latest only) (appear in history log)
DefAggr	N/A	
Duration	Time interval: From alarm was received to cleared alarm	hh:mm:ss
Ems Time	Timestamp set by Cisco EdgeCraft when the alarm was received	yyyy/mm/dd hh:mm:ss (server time)
Id	Unique sequence number to identify the alarm	
Layer rate	The layer rate in which the managed object belongs if applicable.	Not Applicable (any other layer rate supported by the network element) See Map viewer and Map Designer
Location		
NE	Identification of the network element	
NativeValues	Unmapped trap data	(legal values depends on the network element)
NeTime	Timestamp from network element (if available)	yyyy/mm/dd hh:mm:ss
NumUpdated	How many times the alarm has been updated from a given Alarm Point (defined by Source and Alarm Identifier)	Numbers (1- n)
ProbCause	The probable cause of the alarm	(legal values depends on the network element)

Table 3-9 Notification Types (continued)

Attribute		Legal Values
Name	Description	
ProbCauseQ	A probable cause qualifier if the probable cause itself is not sufficient to determine the exact error and source	(legal values depends on the network element)
PrvId	Previous Identification of notification	Sequence number
Severity	Severity of alarm	Critical, Major, Minor, Warning, Cleared, Indeterminate
Source	Identification of the network element that contains the source of the alarm.	Every managed objects available in Management Tree
Trend	Indication to report trends on severity change.	No Change, Less Severe, More Severe

Events Notifications

Table 3-10 Events Notifications

Attribute		Legal Values
Name	Description	
AddTxt	Additional text to explain the event	
Description	Additional text	
Ems Time	Timestamp set by CiscoEdgeCraft when the alarm was received	yyyy/mm/dd hh:mm:ss (server time)
EventId	Unique identification of event	
EventType	Event grouped into categories	Equip(-ment), env(-ironment), comm(-unication), process
Id	Unique sequence number to identify the event	
Moid	Identification of the network element that contains the source of the event.	A M.O in the Information Model for the equipment
Native Values	Unmapped trap data	(legal values depends on network element)
NE	Identification of the network element	
NeTime	Timestamp from network element (if available)	yyyy/mm/dd hh:mm:ss

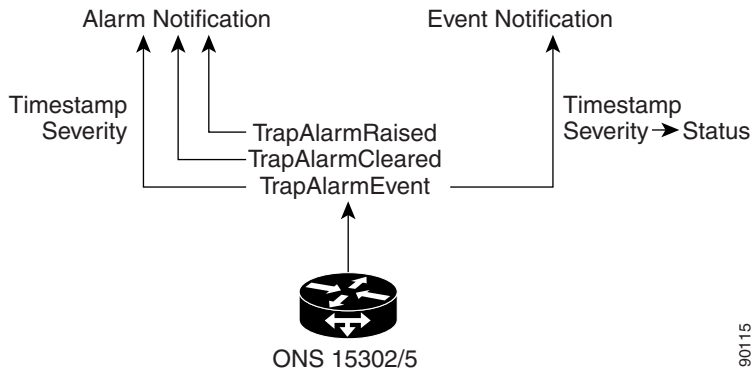
Alarm Notification Severity

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

Trap to Notification Mapping

The interpretation of alarm and event is slightly different in the network element and Cisco Edge Craft. The mapping rules applied to the SNMP traps are illustrated in [Figure 3-32](#).

Figure 3-32 Trap to Notification Mapping



90115

The TrapAlarmRaised and TrapAlarmCleared traps are mapped to alarm notification. The timestamp in the trap will be used together with the severity. ONS 15305 and ONS 15302 have severity in the trap. This severity is used in notification.

One attribute in an alarm notification is called clearable. If set to true, this attribute 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 attribute clearable 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, confirm etc. The severity in the trap might be used as the status in the event notification.

Unknown Traps

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



General Management

4.1 Manage the Management Interfaces

This chapter describes the configuration operations supported by the Management Interfaces managed object (MO). It is organized by the following sections:

- Introduction
- MCN Wizard. This section describes how to configure management connectivity for a Cisco network element using the MCN wizard.
- ONS 15305 management modes and configurations. This section describes the management modes supported by the management interfaces, and how they can be configured.
- ONS 15305 scenarios. This section is a repository of simple, but yet typical configuration scenarios. These can be applied in combination to specific networks.
- Manage common parameters
- Download Software to network element (NE)
- Up/download of NE configuration data
- Alarm and event configuration
- ONS 15305 manage slots

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

4.2 MCN Wizard

MCN - Management Communication Network

4.2.1 Manage the Management Interfaces of the Network Element

The purpose of this chapter is to describe how to configure management connectivity for a Cisco network element, taking advantage of the configuration tool - MCN wizard. The advantage of using the MCN wizard for configuration of your MCN, is that you will have guidance through a logical step-by-step process instead of doing all software configurations via the “management tree”.

See the “[4.2.13 Special Requirements](#)” section on page 4-13 for a description of MCN features supported by the different network elements.

4.2.2 Before you start - Prerequisites

Please read through the different preconditions listed in this section.

4.2.2.1 Management Software

Make sure you are assigned sufficient permissions to perform the required tasks available in the MCN wizard. If using Cisco EdgeCraft you will only be limited by the SNMP community string (login rights) configured on NE. Write access is minimum required.

4.2.2.2 NE Requirements

As a minimum, the Management Port must have a valid IP configuration and an instance in the SNMP community table enabling **write** access.

**Note**

When management connectivity is supposed to be obtained via interfaces on traffic modules, make sure that they are installed and expected or minimum as “expected”.

4.2.2.3 General Requirements

The network design and planning must be maintained and the strategy of network element management interface usage must be decided. IP addresses and subnets must be available prior running the wizard.

4.2.3 MCN Wizard - Step by Step

The following procedure describes the main sequences of flow required to configure a network element for management. MCN commissioning (initial setup) is typically done through the network element management port, while MCN maintenance is done through an existing, operative MCN through the management port, any active DCC channel or in-band management channels.

The Management Interface managed objects allows you to configure:

- The mode (type of encapsulation for the management traffic) run by a management interface.
- Mode-specific parameters for the DCC interfaces, e.g. PPP configuration.

- The IP address(es) allocated to a management interface.
- The IP address of a default gateway.

The exact steps and the sets of attributes to access, will differ for the different Cisco network element variants installed. See the [“4.2.13 Special Requirements” section on page 4-13](#) for details.

See the [“4.11 Manage Slots on ONS 15305” section on page 4-85](#) for details on creation, deletion and setup of a DCC interface.

4.2.3.1 MCN Commissioning Flow Overview

The commissioning flow has two main flows for setting up the network element for management.

- IP Broadcast setup (ONS 15302)
- IP numbered (PPP or HDLC encapsulated IP)

**Note**

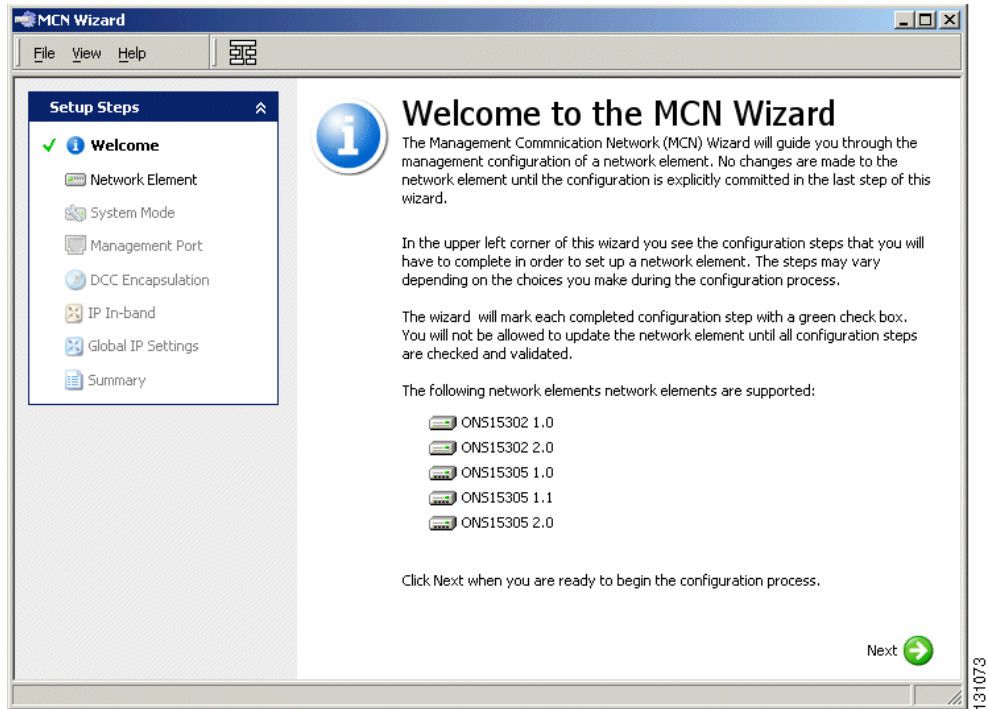
None of the configuration is sent to the network element until the end of the wizard-flow, where you are presented an overview of the configuration

4.2.3.2 Opening the MCN Wizard

Step 1 Select **Equipment > MCN Wizard** from the menu.

4.2.4 Welcome to the MCN Wizard

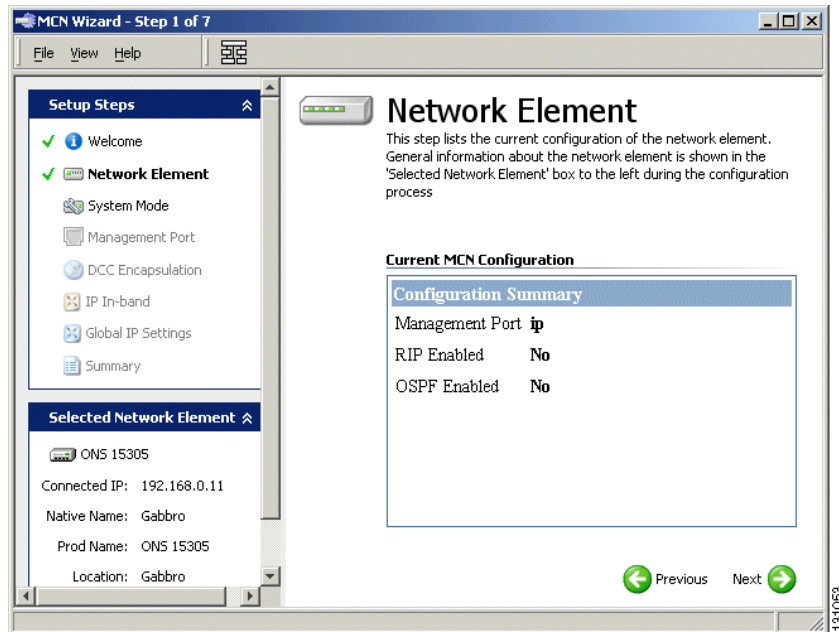
Please read the introduction found in the “Welcome” window before proceeding with the configuration process.

Figure 4-1 *Welcome to the MCN Wizard*

Step 1 Click **Next** to proceed.

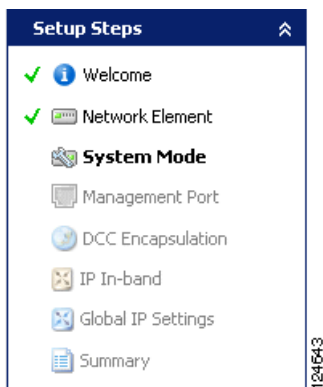
4.2.5 Network Element

Step 1 The system presents the current MCN configuration of the network element:

Figure 4-2 MCN Current configuration

- Step 2** The presented IP address is the “connected IP address”, the IP address Cisco EdgeCraft uses to access the network element. This address can be any of several possibilities, depending on the current MCN configuration and MCN route to the network element: Management Port IP address, a DCC channels IP addresses, a VLAN IP address or an in-band IP port address.
- Step 3** Click **Next** to continue.

4.2.6 System Mode

Figure 4-3 System mode

The system presents the current system mode set-up, and the system mode choices.



Note

Not all network elements support every mode. Only valid modes for the current selected network element are listed here.

Step 1 Select **system mode**.

4.2.6.1 IP Numbered

Select this mode if you want to configure the network element to use IP protocol stacks. Each management interface has an IP address (the network element is a multi-homed host), the DCCs, any in-band channels and the Management Port. The routing table can be maintained by static or dynamic routing. Supported routing protocols are RIP and OSPF.

4.2.6.2 IP Broadcast

Select this item if you want to configure the network element to use the proprietary IP Broadcast protocol. See further description in the [“4.2.11 System Mode - IP Broadcast” section on page 4-11](#). The network element is assigned one IP address only (management port IP address). The network element uses forwarding mechanisms to dispatch traffic between the active DCC channel and the Management Port. This mode is typically used for back-to-back configurations of two ONS 15305's or ONS 15302's.

4.2.6.3 IP Un-Numbered



Note

This system mode is only supported by ONS 15302 R2.0 and ONS 15302 R2.0. This system mode can only be set using ONSCLI and will deactivate MCN wizard from the Cisco EdgeCraft desktop equipment menu.

Select this mode if you want to share the management port's IP address with DCC management interfaces. The network element is assigned only one IP address that is valid for all of its management interfaces (DCC channels and management port). Routing of messages between the management interfaces is handled by OSPF. To take full advantage of this system mode it is required a network topology built up of just NE's supporting IP un-numbered feature.

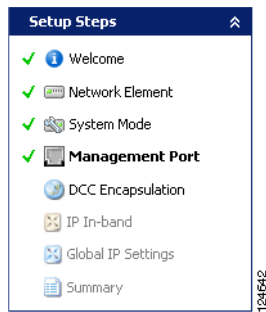
See the table below and the [“4.2.13.1 DCC Usage Limitations” section on page 4-13](#) for network element variant available choices and limitations.

Table 4-1 System mode vs. network element

	ONS 15302	ONS 15305
IP Broadcast	x	--
IP Numbered	x	x
IP Un-numbered	x (rel 2.0 or newer)	x (rel 2.0 or newer)

4.2.7 Management Port - System Mode IP Numbered

Choose the port for management traffic



Step 1 Select which of the available protocol stacks you want to use for the Management port.

Disable

Disables the management port.



Note

Disabling the management port should only be performed when connected via other interfaces than the management port.

IP

Select this item if you want to activate the IP protocol for the management port.

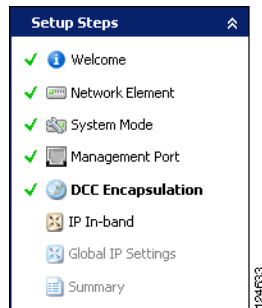
The system presents the current set-up of the management port, and the available choices. You select between the following choices:

Table 4-2 Management port modes

Management port mode	Purpose	Comment
Disabled	To turn of local access via MNGT-port.	"Disabled" prohibits access to the MCN through the management port.
IP	Enable IP for MNGT-port.	Default mode.

If IP is selected, the operator is required to set up the IP global attributes. See the [“4.2.10 Global Ip Settings - System Mode Ip Numbered”](#) section on page 4-10 for details.

4.2.8 DCC Encapsulation - System Mode IP Numbered



This step allows you to set up the DCC configuration. If you don't want management over DCC, select all items and press the “Disable Selected” button.

You select the encapsulation mode of the selected DCC channel, or remove the channel from the MCN. The alternatives are:

- Not used
- IOverDcc encapsulated IP (proprietary).
- PPP encapsulated IP (IP over PPP).

The following two sections details the setup of IP over DCC and IP over PPP:

For network element type support of the different selections see [Table 4-4 on page 4-15](#)

4.2.8.1 IP over DCC Encapsulation

Sets up the DCC channel in a proprietary mode where the management MAC packages are encapsulated in HDLC frames and sent across the MCN.

-
- Step 1** Set the mode as “**ipOverDcc**” and then set up the IP address and subnet mask of the interface and set up the following DCC channel attributes:
- IP address of the DCC port
 - IP subnet mask of the DCC port
- Step 2** Press **Next** when you are satisfied with the DCC setup.
-

4.2.8.2 Ip Over Ppp Encapsulation

Sets up the DCC channel in **ppp** mode where the management IP packages are encapsulated in PPP frames and sent across the MCN.

-
- Step 1** Select the DCC channels the list of available DCC channels, and set the following DCC channel attributes:
- mode = ppp
 - IP address of the DCC port
 - IP subnet mask of the DCC port

Step 2 Press **Next** when you are satisfied with the DCC setup.

4.2.9 IP in-band - System Mode IP Numbered

This step allows you to configure IP addresses on In-band interfaces, that is a LAN port, a WAN port or a VLAN, which enables you to run management IP traffic (SNMP) over the in-band interfaces.



Note

Only LAN and WAN ports have Slot/Port configuration (not VLANs)



Note

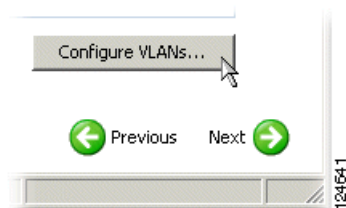
The table may contain ifIndex that are not associated with IP-In-band configuration.



Note

If VLAN is used for management traffic, it is required that the VLAN is configured in advance.

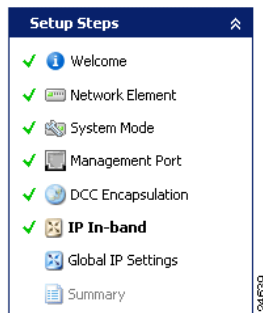
Figure 4-4 *Configure VLAN*



If VLANs are not already configured, this can be done by clicking the Configure VLANs button found in lower right corner.

The system presents the current IP in-band setup (if any).

Figure 4-5 *IP In-band*



Step 1 Select what (LAN/WAN) interface to use for management purposes. The choices are:

- No change

Continue to sub-flow [“4.2.10 Global Ip Settings - System Mode Ip Numbered”](#) section on page 4-10.

- Set up In-band channel


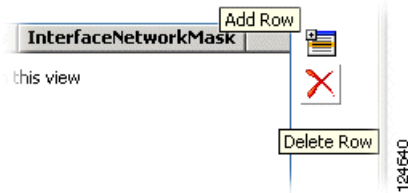
Step 2 Click the **Add** button .

Figure 4-6 Add Row



Step 3 Enter **InterfaceNumber**. (iFindex)

Step 4 Enter **IP address**. (xxx.xxx.xxx.xxx)

Step 5 Enter **InterfaceNetworkMask** (xxx.xxx.xxx.xxx) (subnet mask)

4.2.10 Global Ip Settings - System Mode Ip Numbered

This flow sets up the global IP for the MCN.

Step 1 Click the **Add** button in the **Routing Table** and define:

Figure 4-7 Routing Table

Routing Table

Step 2 Enable the **OSPF** routing protocol, **if used** in the MCN.

☒ **Open Shortest Path First (OSPF)**

Id	AreaId	ImportAsExternal	Metric
0.0.0.0		importNoExternal	0
		importExternal	
		importNoExternal	

Router Id

124635

Step 3 Click **Add** and enter/select values for these attributes:

AreaId

ImportAsExternal; importExternal or importNoExternal

Metric

Step 4 Enter **Router Id**.

Step 5 Enable the **RIP** if used in the MCN.

Routing Information Protocol (RIP)

☒ Use RIP

Previous Next

124635

Step 6 Click **Next** to continue.



Note

Global and interface specific OSPF and RIP parameters can be tuned under the IP attribute view (management tree).

4.2.11 System Mode - IP Broadcast

This procedure describe configuration tasks when System Mode is set to IP Broadcast.

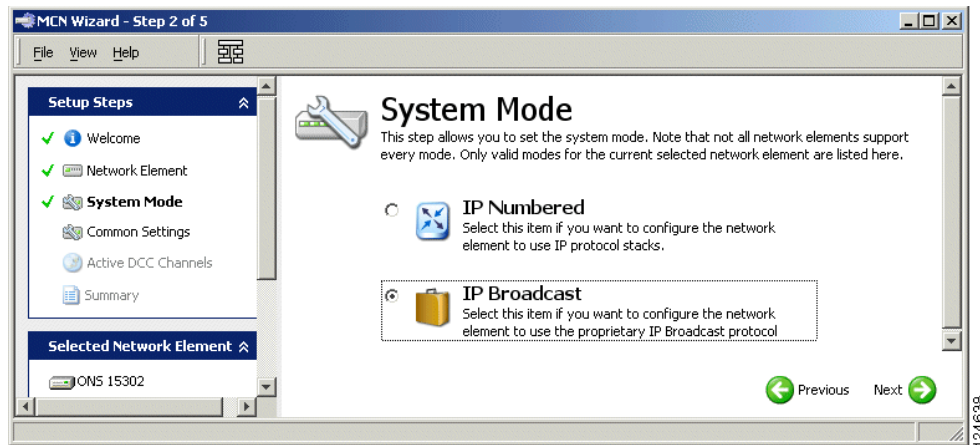


Note

This system mode is only supported by ONS 15302

4.2.11.1 System Mode

Figure 4-8 System Mode - IP Broadcast



-
- Step 1** Check **IP Broadcast** as System Mode.
- Step 2** Click **Next** to proceed.
-

4.2.11.2 Common Settings

This step allows you to configure the default gateway, the management port settings and the MAC filter on the selected network element

4.2.11.3 Gateway

Default gateway address.

4.2.11.4 Management port

Enables/Disables the management port. A disabled management port can be enabled again from ONSCLI.

4.2.11.5 Media Access Control (MAC) Filter

Enables/Disables the MAC-filter. When enabled, the management port will reject ethernet traffic with MAC addresses outside the address range assigned to Cisco products.

4.2.11.6 Active DCC Channels

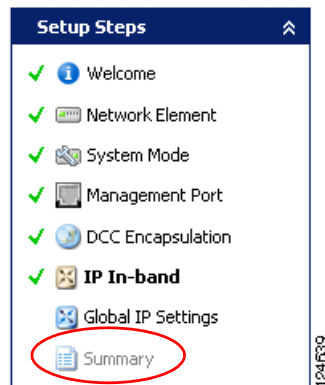
See [“4.2.8 DCC Encapsulation - System Mode IP Numbered”](#) section on page 4-8.

4.2.11.7 Summary

See [“4.2.12 Summary” section on page 4-13](#).

4.2.12 Summary

Figure 4-9 Summary



When the MCN wizard sequence is completed you should review the configuration before committing the changes to the network element. The system presents an overview of the configuration prepared.

Step 1 If the configuration is satisfactory, click **Save** to commit the configuration into the network element.

When committed, the system sends out a sequence of configuration commands. The commands are sequenced in a way that does not cause deadlocks or loss of communication with the managed element through the implementation of the MCN configuration for the network element.

4.2.13 Special Requirements

Requirements for ONS 15305 and ONS 15302

4.2.13.1 DCC Usage Limitations

4.2.13.2 ONS 15305

- 8*DCC-R and 4*DCC-M per slot
- An MSP 1+1 link with DCC management traffic consumes 2 or 4 DCC's, as both working and protecting DCC channels must be configured

4.2.13.3 ONS 15302

- Max. 2 DCC channels per (logical) STM-1 port is allowed, 1*DCC-R and/or 1*DCC-M(1 logical DCC channel = 2*DCC-R or 2*DCC-M, 2 logical DCC channels = 2*DCC-R and 2*DCC-M)
- If IP/DCC (proprietary) or IP encapsulation, both working and protecting DCC channels must be configured manually
- If IP/PPP, only the working channel needs to be configured - the system automatically configures the protecting channel.
- IP/PPP is only supported on DCC-R (IP/PPP supported on DCC-M from ONS 15302 version 2.0)

For ONS 15302 MSP 1+1 configuration requires special attention. There are up to four physically available DCC channels (2*DCC-R plus 2*DCC-M), but logically they operate as up to 2 channels (1*DCC-R and/or 1*DCC-M) in a protection scheme.

4.2.14 Features Vs. Network Element Types

The features supported by the network elements are shown in [Table 4-3](#).

Table 4-3 **Features Supported by ONS 15302 and ONS 15305**

Feature		ONS 15302	ONS 15305
Communication	IP Broadcast DCC-R/M	X	-
	IP HDLC DCC-R/M	X	X
	IP/PPP DCCR	X	X
	IP/PPP DCCM	X	X
	IP Un-numbered	X	X
	IP-Routing	X	X ¹
	In-band	X	X ²
Security & Traffic Control	Management Port on/off	X	X
	SNMPv1 Community	X	X
	SNMP Manager Identity	X	X
	SNMP read/write control	X	X
	VLAN (802.1Q)	X	X

1. See above.

2. Dependent of equipped module(s)

4.3 Management Modes and Configuration


Note

The following sections describe how to configure the Management Port and the DCCs by using the Management Interfaces managed object present in the Management Tree.

The management traffic is IP based (SNMP and TFTP messages), and therefore configuring a management path comes to deciding which encapsulation shall be used to send the IP datagrams carrying the management traffic over the network. For the management interfaces the following encapsulation type is supported

- IP directly carried over a layer 2 protocol (Ethernet, PPP, or proprietary).

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


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 4-4 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

A DCC can run only one mode at a time. In addition, a maximum of eight DCCs can be used for management purposes, that means only up to eight DCCs can be assigned to a management mode.

The following sections describe how to configure the management port and the DCCs by using the management interfaces managed object present in the management tree.

4.3.1 Management Port Configuration

The management port can run two types of encapsulation, referred to as modes. A particular mode is selected by setting the variable mode (management interfaces >management port > mode). Required configuration for possible modes:

- not used
- IP

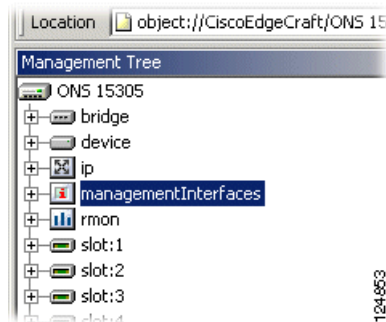
These are further detailed in the next sections.

4.3.1.1 Mode: Not Used

To configure the management port with mode set to not used:

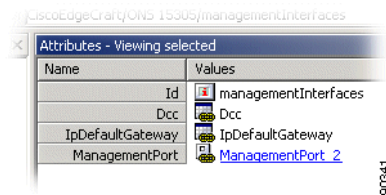
- Step 1** Click on the ONS 15305 managed object, then on the **management Interfaces** managed object in the Management tree, [Figure 4-10](#).

Figure 4-10 Management Interfaces - Managed Object



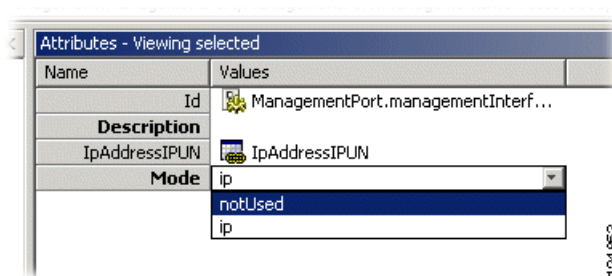
- Step 2** Click on **managementPort** in the attributes window, [Figure 4-11](#).

Figure 4-11 ManagementPort - Attributes



- Step 3** In the attributes window, set mode to **Not Used**, [Figure 4-12](#).

Figure 4-12 ManagementPort - Mode Selector



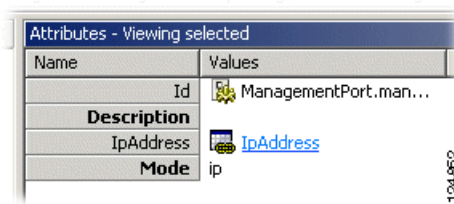
- Step 4** Click **Save** on the toolbar.

4.3.1.2 Mode: IP

To configure the management port with mode set to IP:

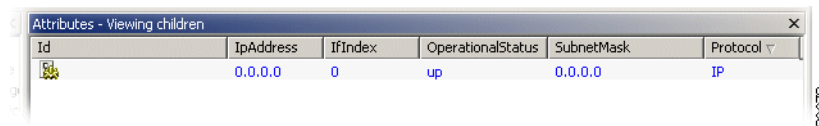
- Step 1** Click on the ONS 15305 managed object, then on the **management Interfaces** managed object in the management tree.
- Step 2** Click on **managementPort** in the attributes window.
- Step 3** In the attributes window, set **mode** to **IP**.
- Step 4** Click **Save** on the toolbar.
- Step 5** Click on **ipAddress** in the attributes window, [Figure 4-13](#).

Figure 4-13 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 4-14](#).

Figure 4-14 ManagementPort - Add IP Address



- Step 7** Click **Save** on the toolbar.
- Depending on your topology, additional routing information might have to be configured. You can define static routes, and or control dynamic protocols (RIP, OSPF) by using the IP managed object in the management tree. Defining a default gateway can be done directly from the management interfaces managed object as explained in the [“4.3.3 IP Default Gateway Configuration”](#) section on page 4-19.

4.3.2 DCC Configuration

A DCC can run three types of encapsulation, referred to as mode. A particular mode is selected by setting the variable mode (management interfaces >DCC >mode). Required configuration for one of the three possible modes (not used or IP) is further detailed in the next sections.

4.3.2.1 Mode: Not Used

To configure a DCC with mode set to Not Used

- Step 1** Click on the ONS 15305 managed object and then on the **management Interfaces** managed object in the management tree.
- Step 2** Click on **dcc** in the attributes window.

4.3.2 DCC Configuration

- Step 3** In the attributes window, each row represents a DCC interface. Set **mode** to **Not Used** for the desired DCC interface.
- Step 4** Click **Save** on the toolbar.

4.3.2.2 Mode: IP

To configure a DCC with mode set to IP:

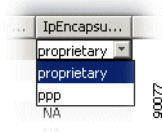
- Step 1** Click on the ONS 15305 managed object and then on the **management Interfaces** managed object in the management tree, [Figure 4-15](#).
- Step 2** Click on **dcc** in the attributes window.
- Step 3** In the attributes window, each row represents a DCC interface. Set **mode** to **IP over DCC** for the desired DCC interface.

Figure 4-15 Management Interfaces - Dcc Attribute

Id	DccType	Mode	IpEncapsulation	PppEncapsulation	Description
...	dccR	notUsed	proprietary	Not applicable	
...	dccM	notUsed	proprietary	Not applicable	
...	dccR	notUsed	proprietary	Not applicable	
...	dccM	ipOverDcc	proprietary	Not applicable	
...	dccR	notUsed	proprietary	Not applicable	
...	dccM	ipOverDcc	proprietary	Not applicable	
...	dccR	notUsed	proprietary	Not applicable	
...	dccM	notUsed	proprietary	Not applicable	

- 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 4-16](#).

Figure 4-16 IPEncapsulation - Encapsulation Selector



- Step 5** Click **Save** on the toolbar.
- Step 6** Click on **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 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 have to be configured. You can define static routes, and or control dynamic protocols (RIP, OSPF) by using the IP managed object in the management tree. Defining a default gateway can be done directly from the management interfaces managed object as explained in the “[4.3.3 IP Default Gateway Configuration](#)” section on page 4-19.

4.3.3 IP Default Gateway Configuration

To configure an IP default gateway on the network element:

- Step 1** Click on the ONS 15305 managed object, then on the **management Interfaces** managed object in the management tree.
- Step 2** Click on **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, that means 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 removal of default gateway.

4.4 ONS 15305 Scenarios

This section presents four typical network topologies, and describes how the management interfaces can be configured through the management interfaces managed object in Cisco Edge Craft in order to carry management traffic, [Figure 4-17](#) to [Figure 4-20](#) and [Table 4-5](#) to [Table 4-8](#).

4.4.1 Important Note

In the following scenarios, it is assumed that both RIP and OSPF are disabled. RIP has been manually disabled over the Management Interfaces.

Although each IP network is unique, the topologies and configurations presented in this chapter can be thought of basic building blocks, which can be combined together in order to apply them 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, activation and configuration of dynamic routing protocols (RIP, OSPF) 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 run a dynamic routing protocol. As the number of static routes grows with the number of interfaces configured to run IP over DCC, running a dynamic routing protocol can be advantageous. Note that 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 only the management traffic).

Each of the next sections ([4.4.3 Scenario 1: CEC and ONS 15305 on the Same Subnet](#), [page 4-20](#) to [4.4.6 Scenario 4: IP over PPP](#), [page 4-24](#)) present a figure of a typical IP topology, together with the required parameters to be configured in the Management interfaces M.O.

4.4.2 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, that means the value of the attribute will not influence the configuration.

The notation Interface: (XXX) used for defining the interface of the default gateway ([Figure 4-18](#) to [Figure 4-20](#)) indicates that the ifIndex of the XXX interface should be used. Possible values for XXX are, (MGMT Port), or (DCC #n) to the ifIndex of the management port, or the ifIndex of DCC channel n respectively. The values of the ifIndex can be found under the respective M.O.s, that means management port, and DCCs.

4.4.3 Scenario 1: CEC and ONS 15305 on the Same Subnet

Figure 4-17 Cisco Edge Craft and ONS 15305 on the Same Subnet

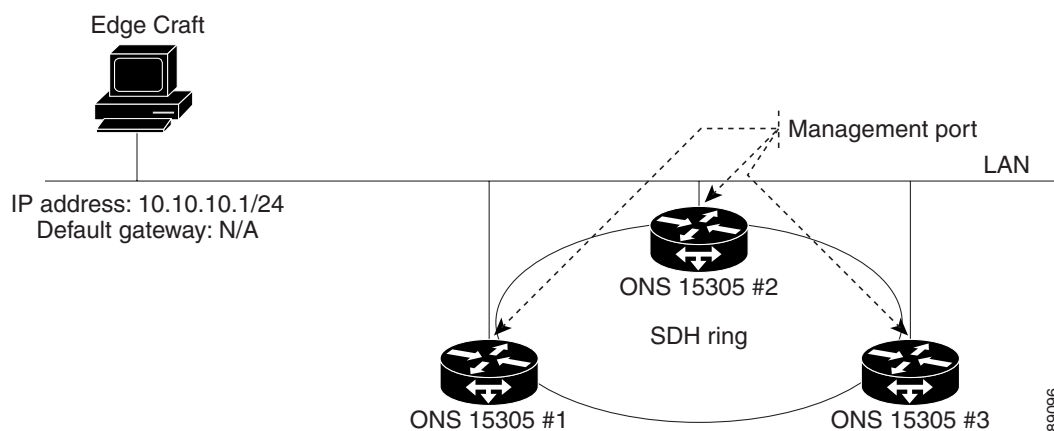


Table 4-5 *Cisco Edge Craft and ONS 15305 on the Same Subnet - Settings*

	ONS 15305 #1	ONS 15305 #2	ONS 15305 #3
Management 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
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
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 Default Gateway			
ipAddress	N/A	N/A	N/A
interface	N/A	N/A	N/A

4.4.4 Scenario 2: CEC and ONS 15305 on Different Subnets

Figure 4-18 Cisco Edge Craft and ONS 15305 on Different Subnets

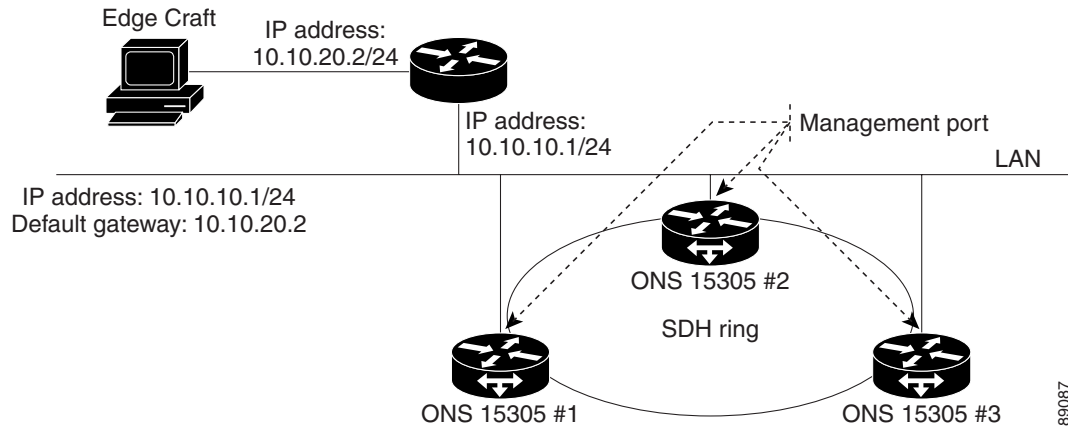


Table 4-6 Cisco Edge Craft and ONS 15305 on Different Subnet - Settings

	ONS 15305 #1	ONS 15305 #2	ONS 15305 #3
Management 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
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
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 Default Gateway			
ipAddress	10.10.10.1	10.10.10.1	10.10.10.1
interface	mgmt port	mgmt port	mgmt port

4.4.6 Scenario 4: IP over PPP

Figure 4-20 IP over PPP

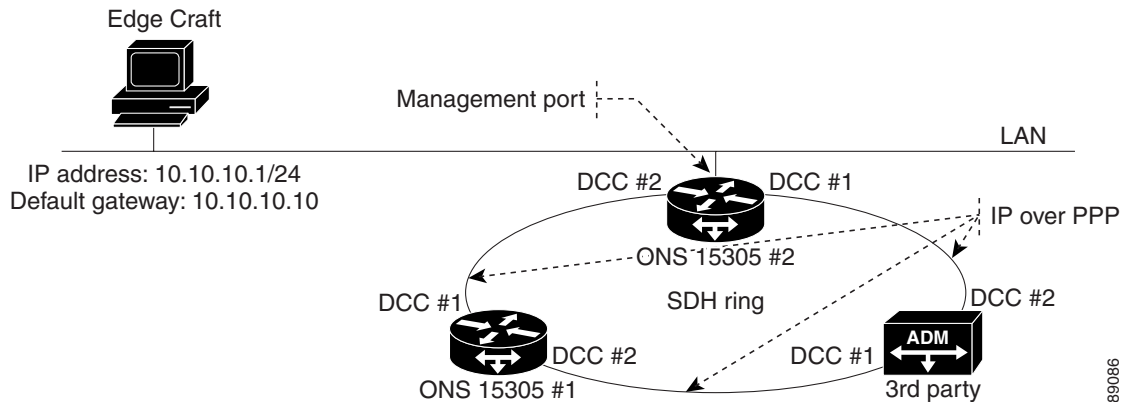


Table 4-8 IP over PPP- Settings

	ONS 15305 #1	ONS 15305 #2	ONS 15305 #3
Management Port			—
mode	notUsed	IP	—
iPAddress	N/A	IP, 10.10.10.10 / 24	—
DCC#1			
mode	IP	notUsed	—
ipEncapsulation	PPP	PPP	—
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	—
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 Default Gateway			

Table 4-8 *IP over PPP- Settings (continued)*

	ONS 15305 #1	ONS 15305 #2	ONS 15305 #3
ipAddress	192.168.10.2	N/A	192.168.20.1
interface	DCC #1	N/A	DCC #2

The 3rd party equipment supports:

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

4.5 Manage Common Parameters

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

The section involves presentation and modification of the NE identification, time settings, users, available features, 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.

4.5.1 View Common Parameters

Select the **device** in the management tree.

The common attributes (parameters) as defined in the information model, are presented for you.

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

4.5.2 Modify Common Parameters

How to change and update parameters for a Network Element.

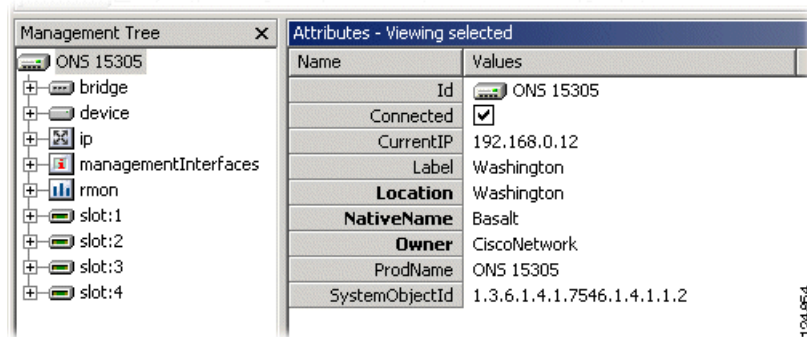
4.5.2.1 Identification of the Network Element

-
- Step 1** Select the network element in the management tree, [Figure 4-21](#).

Step 2 The following attributes can be modified:

- Location
- NativeName
- Owner

Figure 4-21 Identification of Network Element



4.5.2.2 Label

The attribute Label is based on the Location attribute and generated, based on the following rules:

Rule 1: Label = Location

Rule 2: Label = Ip address, if no contact with NE first time in management

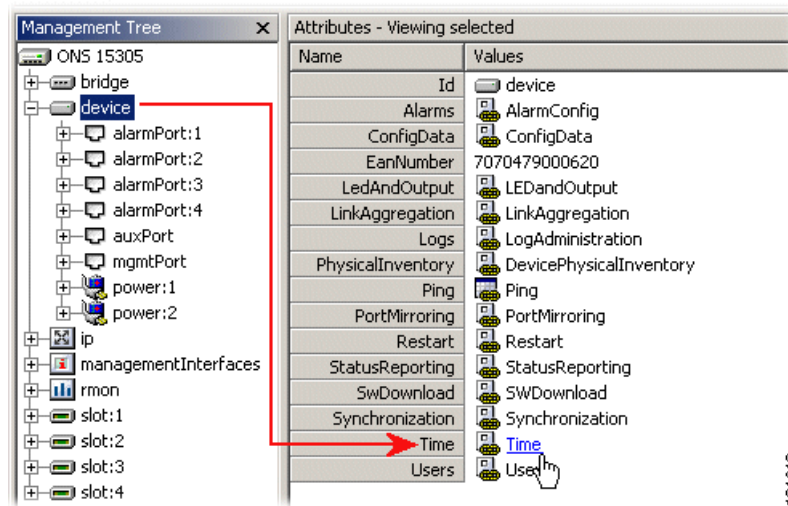
Rule 3: If Location is blank, Label = Ip address

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

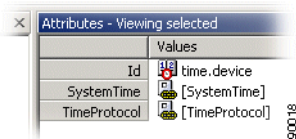
4.5.2.3 Time Settings

The example below shows ONS 15305.

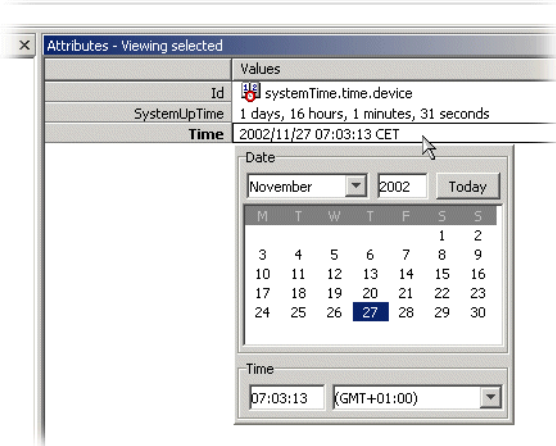
Step 1 Select **ONS 15305** and then the **device** managed object, [Figure 4-22](#).

Figure 4-22 Time Settings - Time Attribute

Step 2 Click **Time**, [Figure 4-23](#).

Figure 4-23 Time Attribute - Values

Step 3 Click **SystemTime>Time** to view or modify, [Figure 4-24](#).

Figure 4-24 Time Attributes - System Time

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

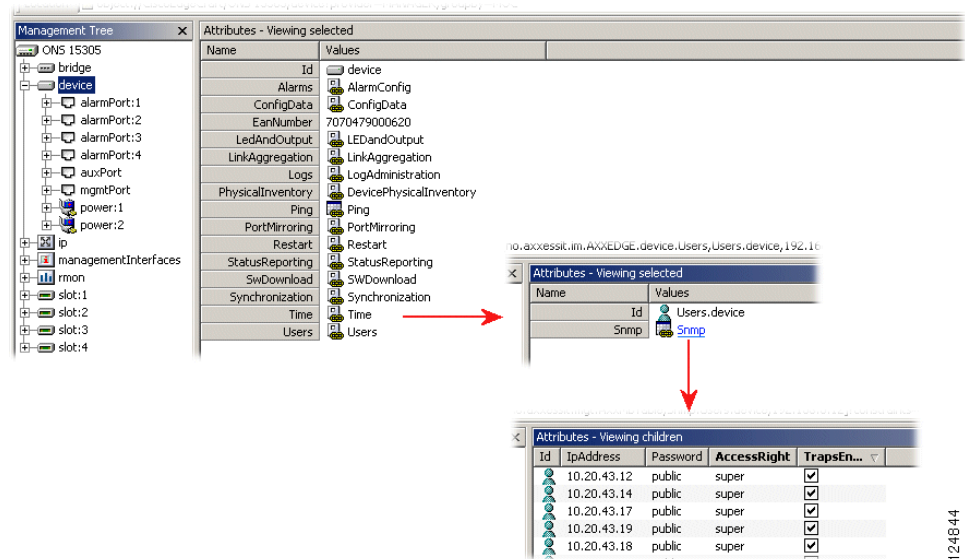
- TimeServerIpAddress
- TimeSyncInterval

- Itemizing

4.5.2.4 Users

This section describes how to add a new user, [Figure 4-25](#).

Figure 4-25 Add a New User - Overview



124844

Add a New User

To add a new user, follow these steps:

- Step 1** Navigate as described in, [Figure 4-25](#).
- Step 2** Click **Add**.
- Step 3** **Enter**
 - password
 - IpAddress
- Step 4** **Select** desired **AccessRight** from pull-down menu.
- Step 5** **Select** desired **TrapsEnable** state from pull-down menu.
- Step 6** Click **Save**.

VT 100 Password (ONS 15302 only)

To edit the VT 100 password, follow these steps:

- Step 1** Select **device>time>VT100**.

Step 2 Edit **Vt100Password** to desired value.

Step 3 Click **Save**.

4.5.2.5 Physical Inventory - ONS 15305

Step 1 Select device > **DevicePhysicalInventory**, [Figure 4-26](#).

The screenshot displays the ONT configuration interface for ONS 15305. The Management Tree on the left shows the hierarchy: bridge > device. The 'Attributes - Viewing selected' window shows the 'PhysicalInventory.device' attribute selected. A red arrow points from this attribute to the 'MAIN CARD (FW)' entry in the 'Attributes - Viewing children' window. The 'Attributes - Viewing children' window shows a list of components including SYSTEM SW, MAIN CARD (FW), and various hardware modules like 4XFAN-ALARM-DESUB9, 48DCDC-5-100W-MINI4, 230VAC-0,5A-50/60Hz, SYSCONT-SD128-4xRJ45, MAIN BOARD, ONS15305 64x64/20G BaseModule, and BOOTSTRAP SW.

Name	Values
Id	device
Alarms	AlarmConfig
ConfigData	ConfigData
EanNumber	7070479000620
LedAndOutput	LEDandOutput
LinkAggregation	LinkAggregation
Logs	LogAdministration
PhysicalInventory	DevicePhysicalInventory
Ping	Ping
PortMirroring	PortMirroring

Name	Values
Id	PhysicalInventory.device
Hardware	Hardware
LicenseName	-
LicenseVersion	0
Software	Software

Id	Name	SwType	SwVersion	Bank1productNum
07	SYSTEM SW	software	07	45004-77AB
05	MAIN CARD (FW)	firmware	05	45004-70AA

Bank1Ics	Bank2productNum...	Bank2Ics	OperBank	Adminbank
07	45004-77BA	00Z	bank1	bank1
05	45004-70AA	05A	bank1	bank1

Id	Name	HwType	SerialNumber	ProductNumber	Ics
01	4XFAN-ALARM-DESUB9	fanAndAlarm	0310001231	50004-24AA	01
02	-48DCDC-5-100W-MINI4	power1	0310001213	50004-06AA	02
01	230VAC-0,5A-50/60Hz	power2	0335002704	50004-25AA	01
01	SYSCONT-SD128-4xRJ45	sysCont	0299000004	40004-23AA	01
01	MAIN BOARD	mainBoard	0303005419	40004-01AA	01
02	ONS15305 64x64/20G BaseModule	device	0311001966	74-3103-01	02
02	BOOTSTRAP SW	bootSw		45004-86AA	02

Step 3 Select **Software** hyper link to list software inventory.

4.5.2.6 Physical Inventory - ONS 15302

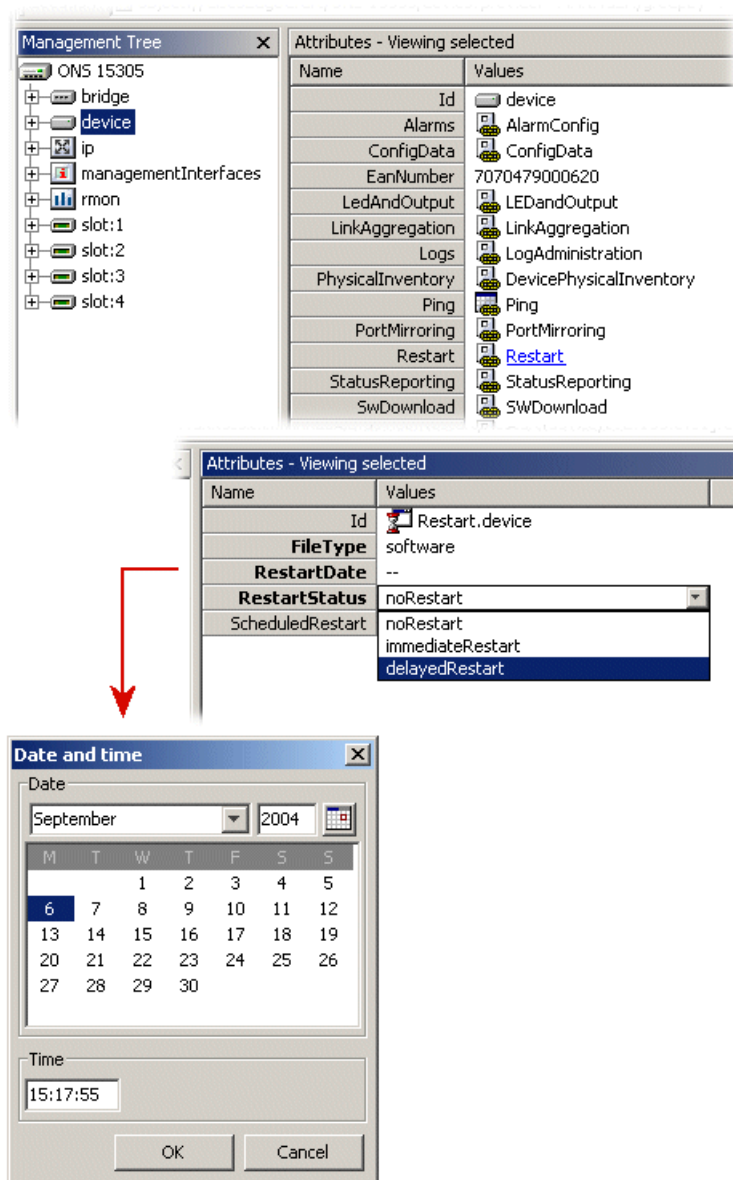
Select device>inventory.

4.5.2.7 Restart of ONS 15305

How to perform a restart or a scheduled restart of the Network Element.

Step 1 Click device>**Restart**, [Figure 4-27](#).

Figure 4-27 Restart of Network Element - Overview



Step 2 Select desired **RestartStatus**.

124812

- Step 3** If selecting **delayedRestart**, set **time** and **date**.
- Step 4** Click **Save**.
-

4.5.2.8 Restart of ONS 15302

How to restart ONS 15302:

-
- Step 1** Click device>**Restart**.
- Step 2** Select **restart**.
- Step 3** Click **Save**.
-

4.5.2.9 Logs (Alarm Logs, Performance Data Logs)

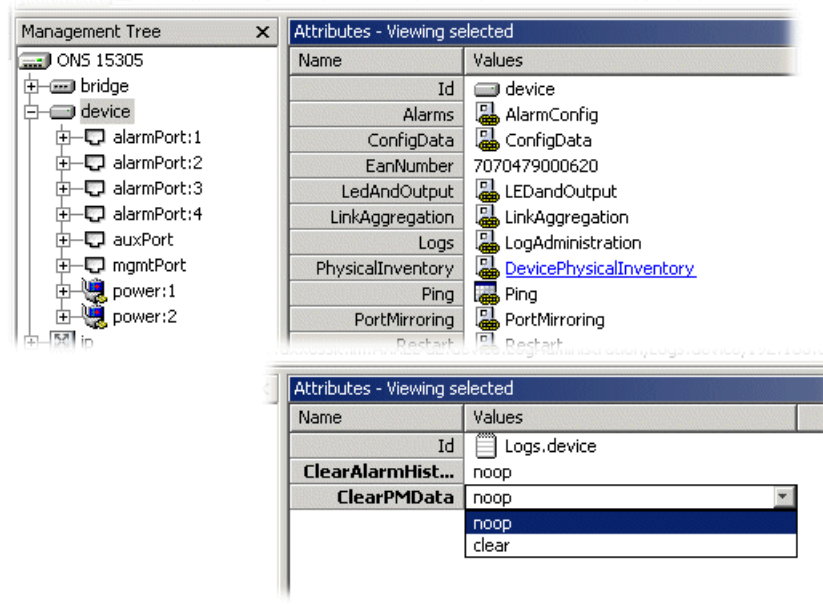
How to work with logs

Clear Alarm History:

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

Clear PM Data:

-
- Step 1** Select device > **LogAdministration**
- Step 2** Set **ClearPMData** to **clear**, [Figure 4-28](#).
- Step 3** Click **Save**.

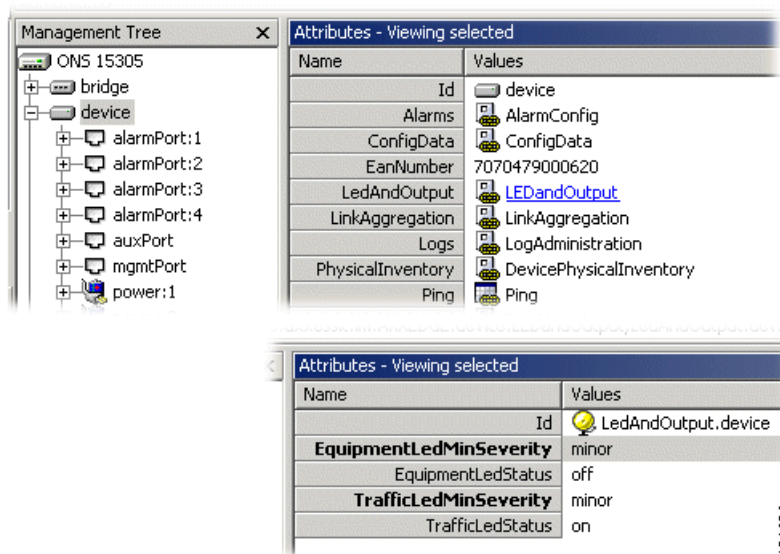
Figure 4-28 Clear Alarm- and Performance Data Log

124639

LEDs and Alarm Output

How to select the severity output level.

- Step 1** Click device > **LEDandOutput**
- Step 2** Select **severity** to light the NE LEDs, [Figure 4-29](#).

Figure 4-29 LEDs - Severity Selector

124638

4.5.2.10 Status Reporting

Status reporting is a kind of “alive” reporting from the device to all trap-receivers defined in the community-table.

This function can be “enabled/disabled” and the status-trap-reporting frequency (time-out) can be specified/altered.

The system currently reports the following in this status-trap:

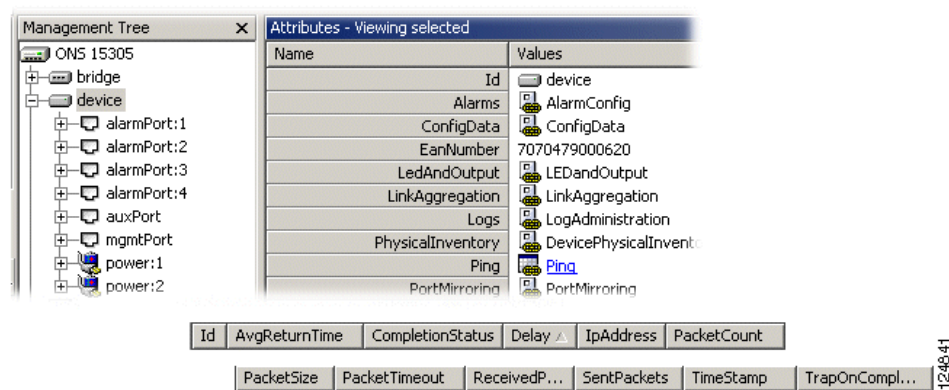
- EquipmentLedStatus,
- AlarmTrafficLedStatus,
- DeviceStatusReporting,
- DeviceStatusReportingFrequency,
- sysDescr,
- sysObjectID,
- sysUpTime,
- sysContact,
- sysName,
- **sysLocation**

One of the NE/ network discovery criteria in Cisco EdgeCraft is Trap Discovery. The status trap sent by NE default every 10 minutes completes this solution.

Ping Mechanism

Modify the ping mechanism:

Figure 4-30 Ping Mechanism



Step 1 Select device > **Ping** hyper link, [Figure 4-30](#).

Step 2 The following attributes are modifiable:

Delay

PacketCount

TrapOnCompletion (true/false)

PacketSize

PacketTimeout

Alarm Ports

Modify the Alarm ports:

Step 1 Select device > **alarmPort** in the management tree, [Figure 4-31](#).

Step 2 The following attributes are modifiable:

- Description

Free text description.

- Mode

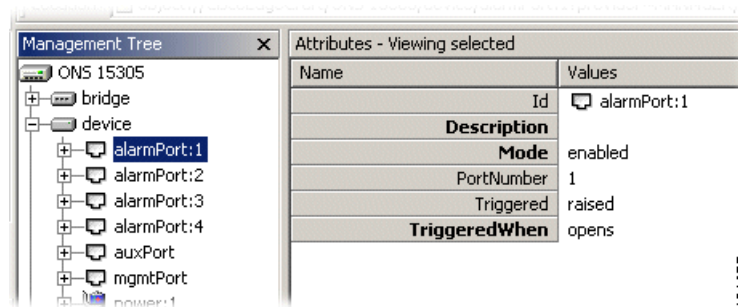
enabled or disabled

- TriggeredWhen

opens or closes (when an alarm is to be triggered)

Step 3 Click **Save**.

Figure 4-31 Alarm Ports



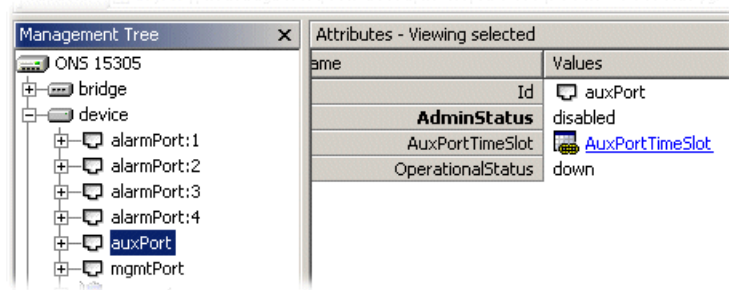
124.865

AUX Port - ONS 15305

Modify AUX Port on the ONS 15305:

- Step 1** Select device > **auxPort**, [Figure 4-32](#).

Figure 4-32 *AUX Port*



- Step 2** The following attributes are modifiable:
- AdminStatus enabled or disabled
 - AuxPortTimeSlot, refer to the [“Figure 4-33AUX port - Timeslots”](#) section on page 4-36.

Figure 4-33 *AUX port - Timeslots*

Id	Instance	RdiAlarms	AisAlarms
exx155ESdhMsAisAlarmReporting:1	ms:1	allow	allow
exx155ESdhMsAisAlarmReporting:2	ms:2	allow	allow
exx155ESdhAu4AisAlarmReporting:1	au4:1	NA	allow
exx155ESdhVc4RdiAlarmReporting:1	vc4:1	allow	NA
exx155ESdhVc12sRdiAlarmReporting	vc12	supress	NA
exx155ESdhTu12sAisAlarmReporting	tu12	NA	supress

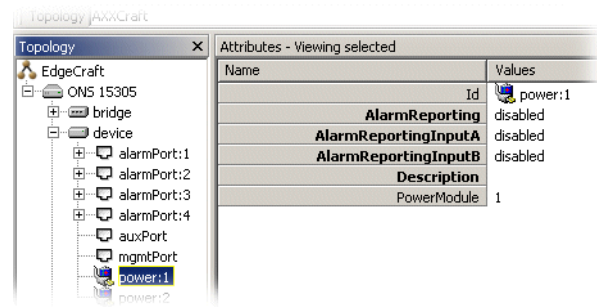
The following attributes can be modified for AuxPortTimeSlot:

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

Power Module - ONS 15305

Modify the Power Module attributes:

Figure 4-34 Power Module - Attributes



-
- Step 1** Select device > **power**, [Figure 4-34](#).
- Step 2** The following attributes are modifiable:
- AlarmReporting
disabled or enabled
 - AlarmReportingInputA
disabled or enabled
 - AlarmReportingInputB
disabled or enabled
 - Description
free text description
-

4.6 Manage Synchronization

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

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

You can override the automatic selection process by manual commands.

For further reading on SDH synchronization, please 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)")

4.6.1 SDH Synchronization

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.

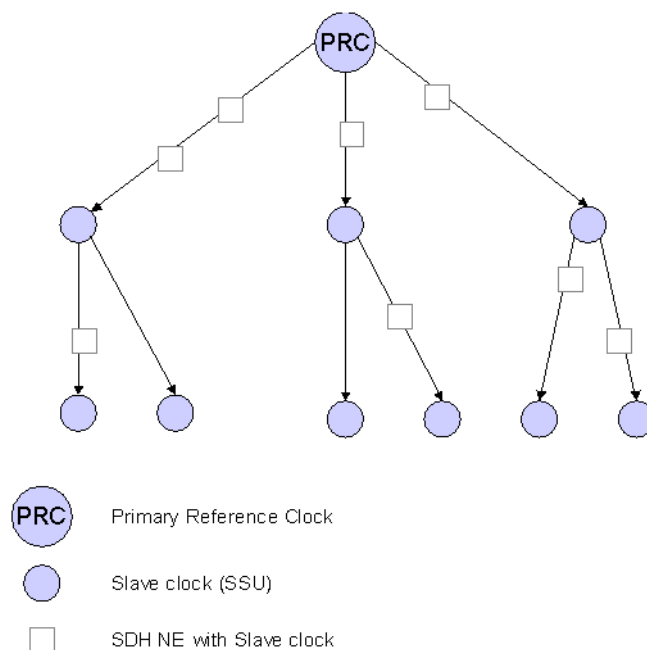
4.6.1.1 Synchronization Networks

A synchronization network is a set of clock nodes that are maintained in synchronization with one another. To achieve this it is necessary to accurately transfer synchronization reference information between nodes so that their relative synchronization may be monitored and maintained.

Since it is difficult to synchronize all international nodes from the same master clock, each network operator typically have 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 4-35](#).

Figure 4-35 Example Synchronization Network



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

Intermediate SDH NEs will also contain slave clocks, the SDH equipment Clock (SEC). Their quality are 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 can be seen from the figure, 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.

4.6.1.2 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 is sometimes necessary to indicate in SSM that this synchronization reference should not be used. This is done by sending the do not use (DNU) message.

4.6.1.3 Synchronizing the SDH Equipment

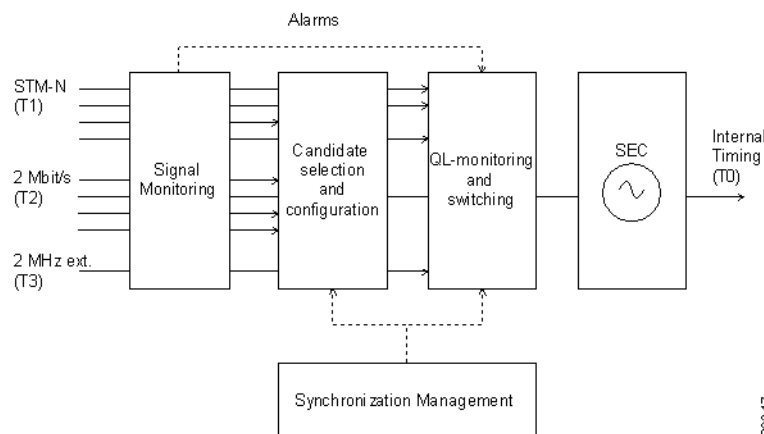
All SDH equipment contains a clock for the SDH pointer adjustments, cross connection matrix operations and the outgoing line signal (STM-N). It is normally operating as a slave clock and locked to a high quality incoming reference, but can run in holdover mode if the reference is lost.

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 Mbit/s PDH interfaces (T2) or the external 2 MHz synchronization input (T3) as indicated in Figure 4-36.

The figure shows that only one at the time of 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 4-36 T0 Selection



90347

4.6.2 ONS 15305

Configuration of synchronization for ONS 15305.

4.6.2.1 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.

4.6.2.2 Candidate Selection and Configuration

In 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 2Mbit/s 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 failed (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. (See the [“QL-monitoring and Switching:” section on page 4-42](#)).
- 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.

4.6.2.3 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.
- The following methods are available for the selection process:

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.

4.6.2.4 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 shall be free for faults for the wait to restore time before taken into consideration by the selection process.

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

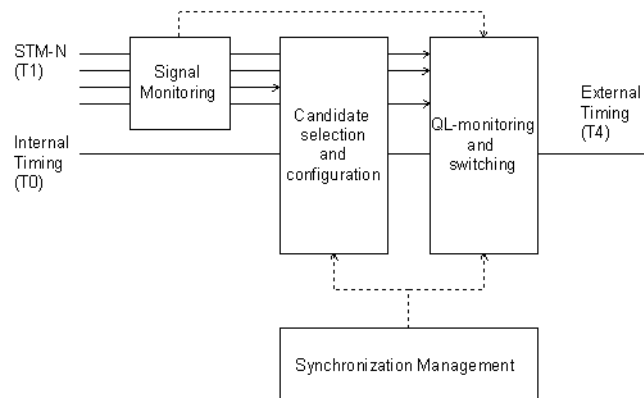
Synchronizing External Equipment

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 a separate stand alone synchronization equipment (SASE).

Synchronization reference information can be extracted from any of the incoming STM-N SDH interfaces (T1) or the internal timing (T0) as indicated in [Figure 4-37](#).

The figure shows that only one at the time of the available synchronization references will be used for External Timing (T4).

Figure 4-37 **T4 Selection**



Here is a short description of the functional blocks for T4 selection:

Signal Monitoring:

See the “4.6.1 SDH Synchronization” section on page 4-38.

Candidate Selection and Configuration:

See the “4.6.1 SDH Synchronization” section on page 4-38.

T0 can be one of the candidates.

QL-monitoring and Switching:

See the [“4.6.1 SDH Synchronization” section on page 4-38](#).

Additional parameter for T4:

- QL minimum level (QLM).

4.6.2.5 Rules

- 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 Mbit/s 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.
- You should receive a warning before deleting the active synchronization source. However, no further restrictions apply.
- The Automatic selection process will find the best source based on the current QL. If more than one source have the highest QL, the source with the highest QL and priority will be selected. If priority is also the same, ONS 15305 will choose the first source in the list with 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 failed or SEC.
- WTR clear does not exist as a method in the MIB. Must set WTR = 0 and then back to original value if method is implemented in 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 shall be squelched (muted) to let the slaved oscillator go into holdover or select another reference.
- T4 is only used for external synchronization output (not for output STM-N signals).

4.6.2.6 Synchronization Alarms

Synchronization alarms are treated as any other ONS 15305 alarms as described in a separate section.

The following table identifies the alarms related to SDH synchronization events.

Table 4-9 *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**

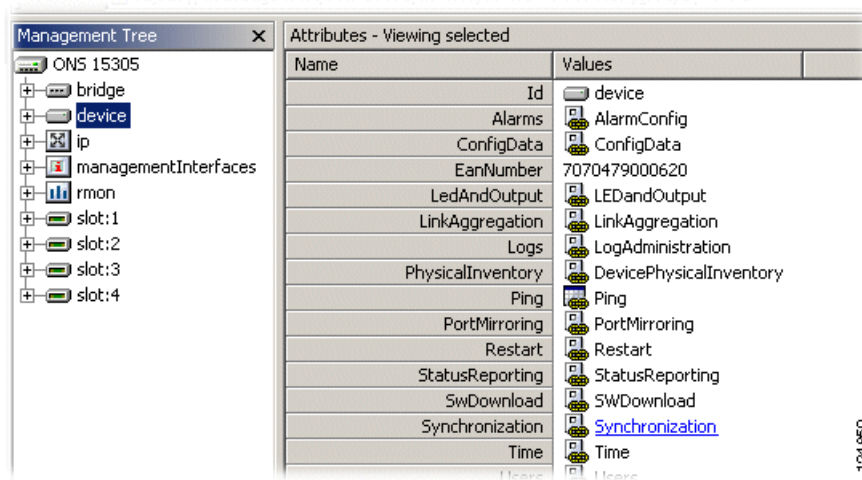
By a synchronization candidate is meant a synchronization source contained in either of the T0 or T4 sync. source tables (5 entries each).

4.6.3 View the Synchronization Data (T0 or T4)

T0 and T4 Synchronization are treated in common in the description of the flows due to their common behavior. The user is considered to be an experienced SDH user since synchronization management is not directly related to the services offered by ONS 15305.

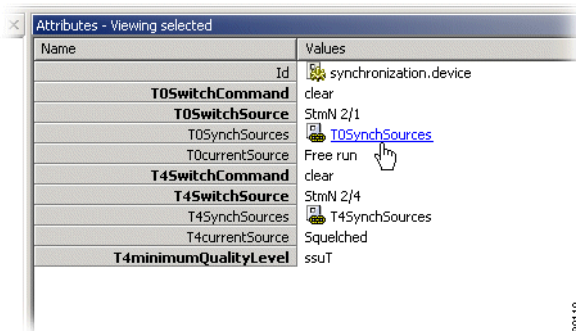
You access the synchronization attributes from the management tree, [Figure 4-38](#).

4.6.4 Add Synchronization Source Candidate (T0 or T4)

Figure 4-38 Synchronization - Selecting Managed Object

The system presents a list of all Synchronization Source candidates.

All attributes of the Synchronization Source candidate are presented as defined in the information mode, [Figure 4-39](#).

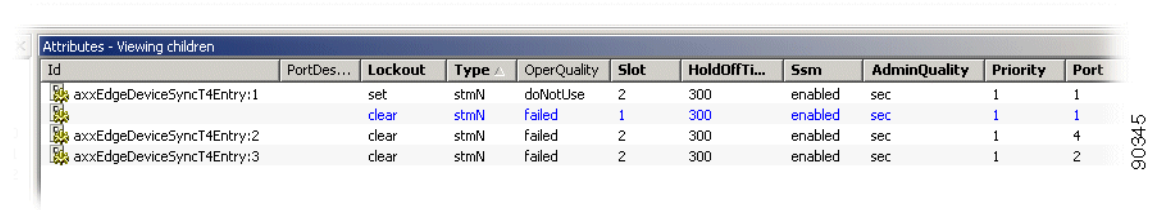
Figure 4-39 Synchronization - T0 SynchSources attribute

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.

4.6.4 Add Synchronization Source Candidate (T0 or T4)

- Step 1** Select T0 SynchSources or T4 SynchSources, [Figure 4-39](#).
- Step 2** Click **Add** in toolbar, [Figure 4-40](#).

Figure 4-40 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	1	300	enabled	sec	1	1
axxEdeDeviceSyncT4Entry:3		clear	stmN	failed	2	300	enabled	sec	1	4
										2

Step 3 Enter the **synchronization parameters** in the management tree 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, ssuL¹, ssuT, prc
- **Priority:** 1 to 5 (where 1 is highest priority)
- **Lockout:** clear/set
- **Hold-Off Time:** 300 to 1800 ms
- **Wait To Restore Time:** 0 to 12 min.

Step 4 Click **Save** to commit the new synchronization source candidate.

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.

The system verifies that the candidate is legal before performing the actual add. If any errors are found, the candidate is not added and you is informed and 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.

4.6.5 Modify Synchronization Source Candidate (T0 or T4)

Step 1 Access the synchronization attributes from the management tree, [Figure 4-39](#).

Step 2 Modify the modifiable synchronization source candidate attributes. 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.

1. Synchronization Supply Unit (SSU):

- High quality
- Two types: SSU Transit (ssuT) better quality than SSU Local (ssuL)
- Between PRC and SEC
- Can sync. a part of a network if connection to PRC is lost

4.6.6 Delete Synchronization Source Candidate (T0 or T4)

You have two possible choices for deleting a synchronization source candidate:

Alternative 1

-
- Step 1** Access the synchronization attributes from the management tree.
 - Step 2** Select the **synchronization source candidate(s)** to delete and click **Delete** in the toolbar menu.
 - Step 3** Click **Save** to commit.
-

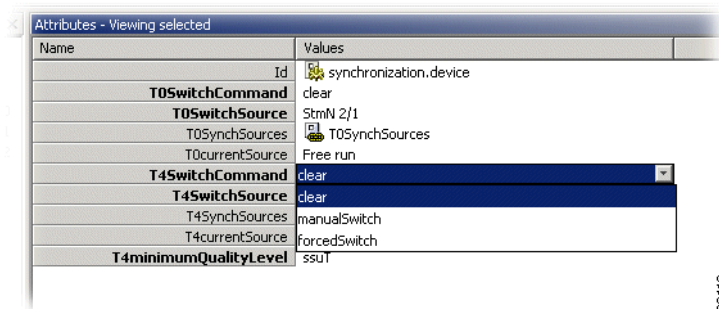
Alternative 2

-
- Step 1** Select the Port (synchronization source) in the management tree
 - Step 2** Select **Do not use for T0 Synchronization** from the drop down menu.
 - Step 3** Select **Delete**. If you selected synchronization source candidate is the active synchronization source, you receives a warning from the system.
 - Step 4** Click **Save** to commit the final delete.
-

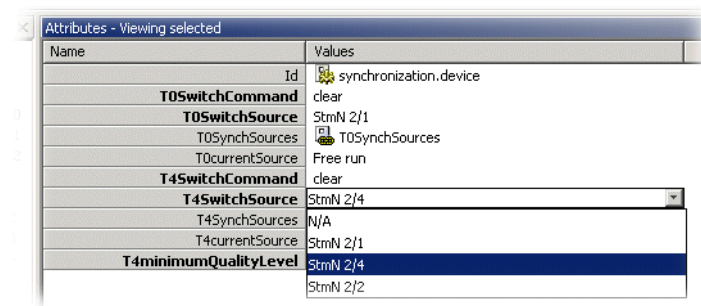
4.6.7 Operate Synchronization Switch (T0 or T4)

Select **T0** or **T4SwitchCommand** and set to desired value, [Figure 4-41](#).

Figure 4-41 Operate Synchronization Switch 1



Click **T0** or **T4SwitchSource** and select **new** synchronization source. (One of the synchronization source candidates), [Figure 4-42](#).

Figure 4-42 Operate Synchronization Switch 2

Click **Save** to commit the changes.

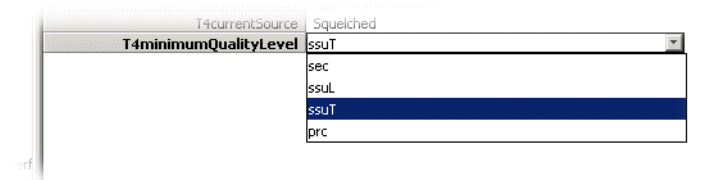
If the switch parameters are valid, the switch is performed. If a manual or forced switch is performed, the selected source will remain selected until a new forced, manual or clear command is sent.

4.6.8 View Synchronization Switch (T0 or T4)

Access the synchronization attributes from the management tree, [Figure 4-43](#).

The attributes for the synchronization switch are presented:

- QLM (T4 Only)

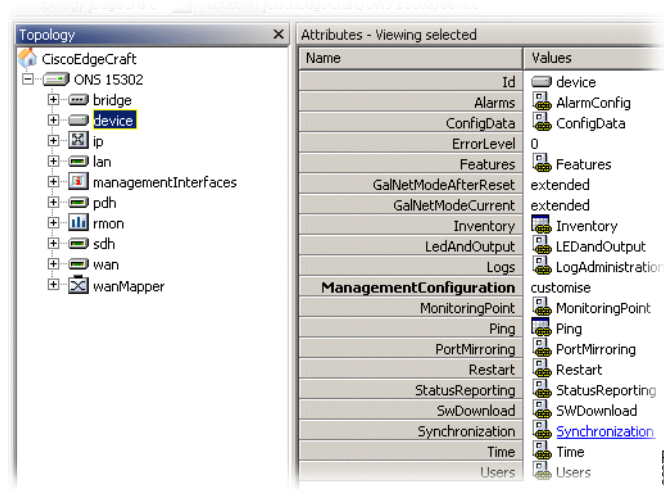
Figure 4-43 View Synchronization Switch

Manual, forced or automatic selection mode.

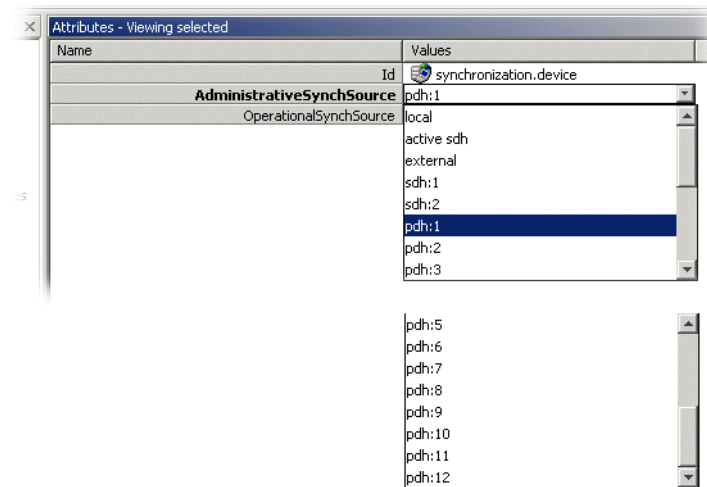
4.6.9 Operate Synchronization on ONS 15302

Below you find guidelines for management of ONS 15302 synchronization.

- Step 1** Select device > **Synchronization**, [Figure 4-44](#),

Figure 4-44 Select Synchronization

Step 2 Select **AdministrativeSynchSource** from pulldown menu, [Figure 4-45](#).

Figure 4-45 Select AdministravtiveSynchSource

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

4.7 Software download and Configuration- Custom GUI

This section describes how to upgrade a network element with download files through the Software Download GUI. Configuration backup and restore is also described.



Note

ONS 15305 is used as an example in the presented procedures.

The features presented is also available from the Management Tree, see [“4.8 Download Software to Network Element” section on page 4-67](#).

See the [“1.2 Commissioning Wizard” section on page 1-17](#) for first time installation.

4.7.1 Introduction

The network element contains device software and firmware, module software and firmware, and configuration data. See the [“4.7.3.4 Network Element Support” section on page 4-50](#).

Contact your assigned distribution channel to obtain software release available for updates and upgrades of the network element.

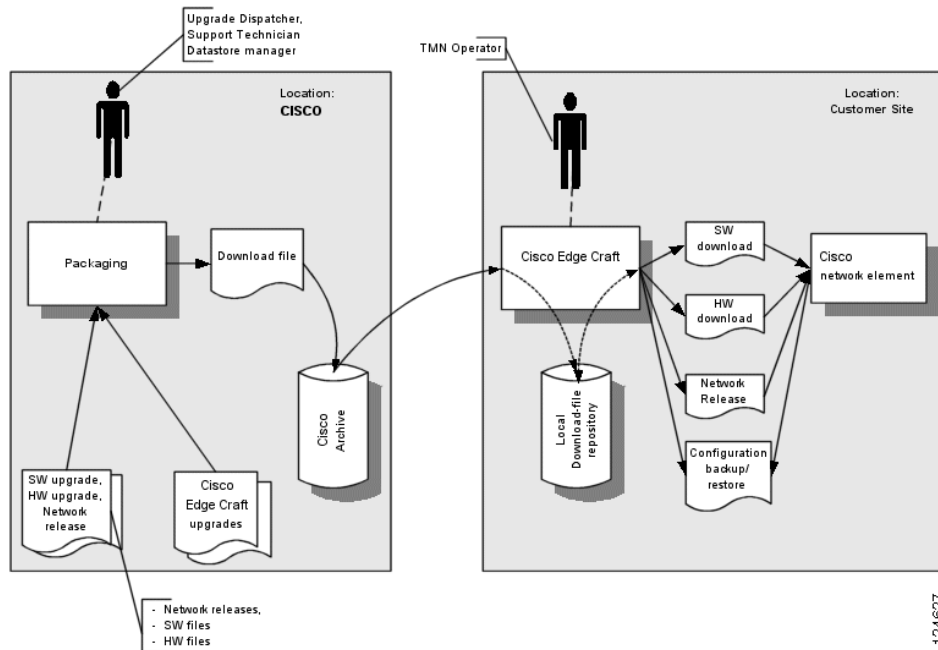
4.7.2 Overview

The presentation is split into 5 sub sections:

- “Software Download Process” on page -49
- “Presentation of the Software Download GUI” on page -53
- “How To Install A Downloaded File Into The Management System” on page -59
- “How to Install Download File to the Network Element” on page -61
 - “How To Upgrade A Network Element With A New Network Release” on page -61
- “How to Backup and Restore Configuration Data” on page -64

4.7.3 Software Download Process

The management system supplies the selected network element with the necessary information to start downloading new files. The download process is controlled by the element itself.

Figure 4-46 Software download process overview¹**Note**

A download file can contain CEC upgrades and patches for the management system itself. Handling of such tasks is not a part of this presentation.

A network element or network element plug-in module can be upgraded the following ways:

4.7.3.1 Software Upgrade

Software upgrade is performed as file downloads to the network element device or to selected modules.

4.7.3.2 Firmware Upgrade

Some network element types have programmable hardware functionality through the use of Field Programmable Gate Arrays (FPGA). The hardware is upgraded by downloading files with new FPGA code.

4.7.3.3 Configuration Backup and Restore

Enables efficient backup and restore of the configuration of network elements. Configuration files are stored on local or remote file systems.

4.7.3.4 Network Element Support

The Software Download GUI support network elements as follows:

1. Firmware is mentioned as hardware (HW) in figure above

ONS 15305:

- Network release and embedded software control file
- Plug-in module upgrade
- Software upgrade
- Configuration backup and restore
- Firmware (FPGA's) upgrade.
- Scheduled and automatic restart of equipment after download completion.

**Note**

One part of the upgrade is controlled by the embedded software on the network element which checks which components are included in the release and ask for upgrade of those components that are newer.

ONS 15302:

- Software upgrade
- Configuration backup and restore
- Manual restart of equipment after download completion

**Note**

A network release supports a given set of traffic modules. If a new module is introduced, the network element needs a new network release.

4.7.3.5 Download Files

There are two classes of download files: “Single Download File” and “Network Release Download File”. Download files have administrative information to tell the network element whether it is a Software or Hardware configuration file. The files appear as *.package.zip.

4.7.3.5.1 Single Download File

It consists of one file per download: Software file, firmware file, and configuration file.

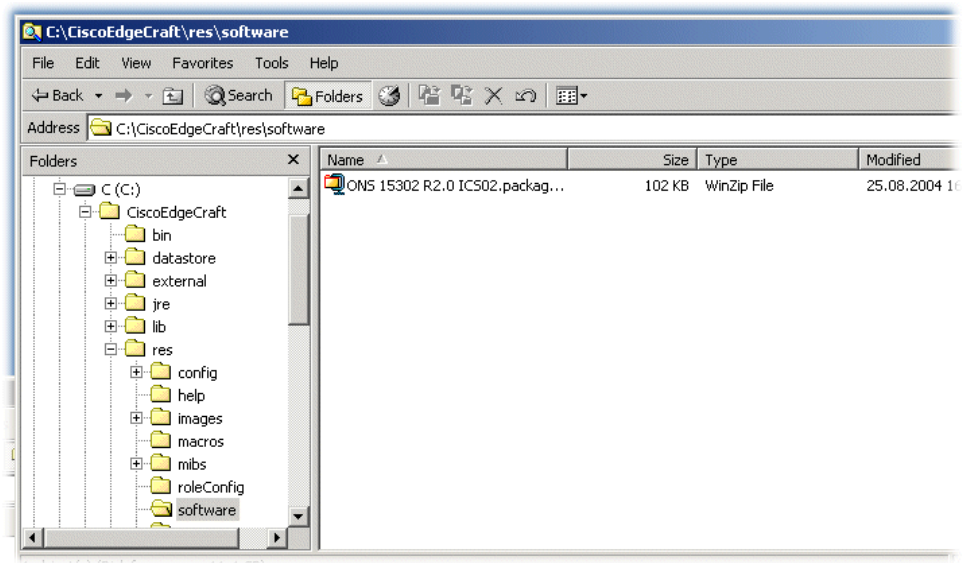
4.7.3.5.2 Network Release Download File

It is a collection of upgrade files which are combined and packed into one file. This download file contains one or more independent upgrade components:

- Device software
- Device firmware
- Plug-in module software and firmware

4.7.3.5.3 Location Of Download Files

A prerequisite for software download is that the files are located in a directory where the TFTP download server can locate them. This is the “. /res/software” directory to the installed Cisco EdgeCraft. The files may be placed in the download directory manually, or by use of a Package Installer, see the [“4.7.5 How To Install A Downloaded File Into The Management System”](#) section on page 4-59. See “Location of backup file”.

Figure 4-47 Software directory - location of download files

4.7.3.6 TFTP Server Settings

The embedded TFTP host of the management system has a default interface setup. This is the first network host located on the computer.



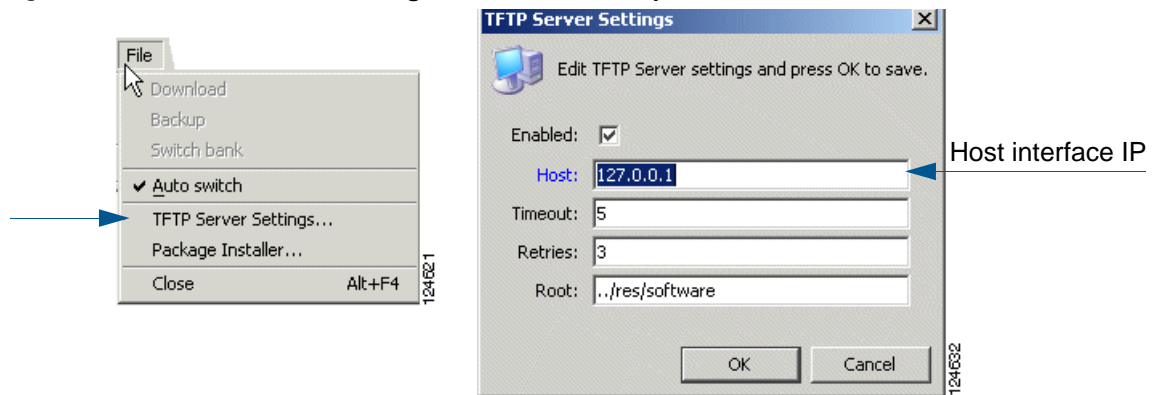
Note

External TFTP host is not supported by the custom GUI. See the [“4.8 Download Software to Network Element”](#) section on page 4-67 for details.

4.7.3.6.1 Edit TFTP Server Settings

This procedure is for advanced users only, and apply to those environment with several IP interfaces.

- Step 1** Open **TFTP server settings** from File menu.
- Step 2** Edit the address to the desired host interface IP.

Figure 4-48 TFTP server settings - Interface IP example

Host: Host interface IP number to run the embedded TFTP server

Timeout: Number on TFTP server time-out in seconds

Retries: Number on package transmission in seconds

Root: Location of the TFTP data repository

**Note**

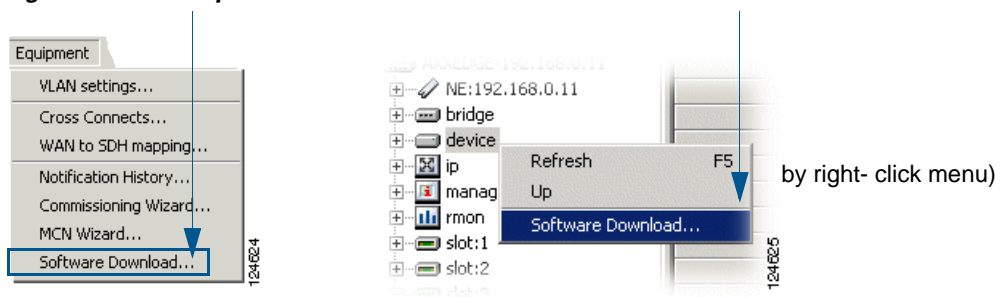
If the TFTP port is occupied by an other program this will be reported in the Error log, see the [“3.1.2.7 Log Viewer” section on page 3-8](#).

4.7.4 Presentation of the Software Download GUI

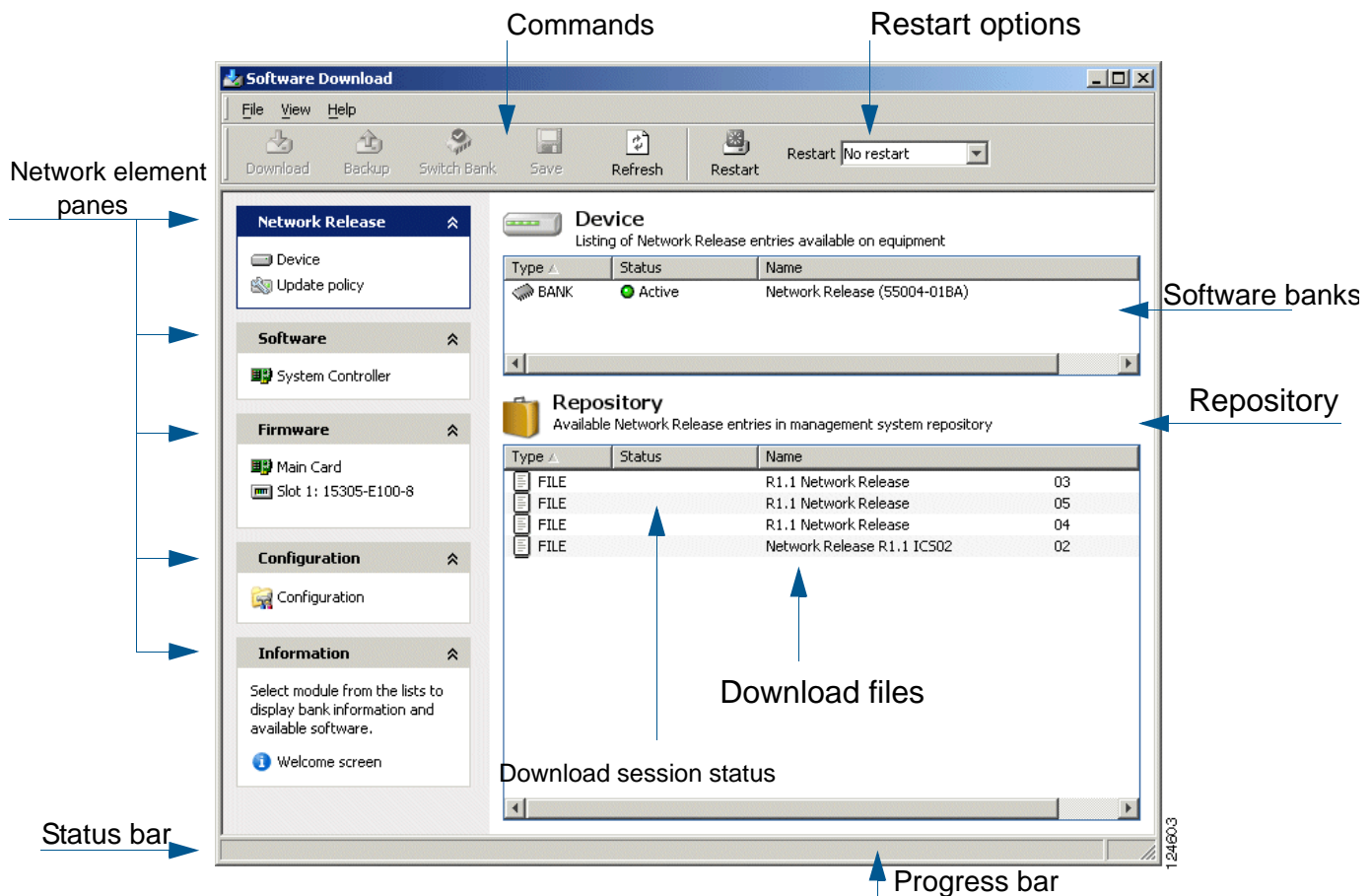
The Software GUI lets you download and manage software downloads.

4.7.4.1 Open the Software Download GUI

The Software Download GUI is available from Management Tree and Equipment menu.

Figure 4-49 Open the Software Download GUI

The network element is presented with panes to the left. Data available on the equipment sw banks and data available in the management system repository are listed in the window to the right

Figure 4-50 Software Download GUI - overview

The Figure 4-50 presents an ONS 15305 with two of four possible service modules available on the network element, listing the network release download files available for the equipment.

**Note**

In order to view, navigate and operate on the service modules, they must have the following settings (With reference to the Management Tree and Attributes Viewer):

ServiceState: 'inservice'

InstallState: 'InstalledAndExpected'

Please see the [“4.11.2 Modify Slot”](#) section on page 4-87 for further details.

You can navigate in the Software Download GUI when an activated session runs in the background.

**Note**

It is not possible to run several sessions at the same time.

4.7.4.2 Operational and Administrative Software Bank of Network Elements

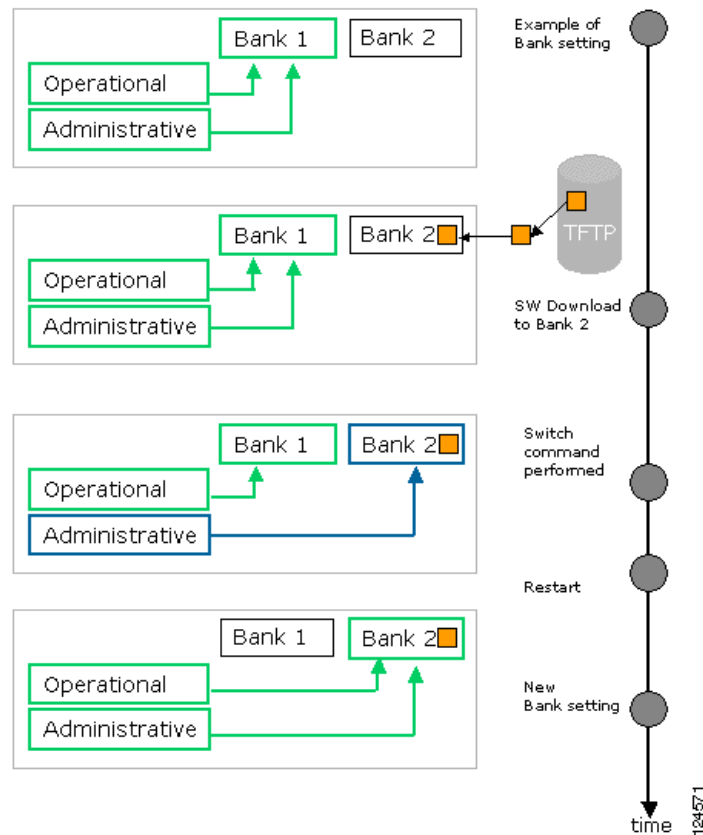
The network element store its software and firmware in banks. Some network elements have two banks, numbered as bank 1 and bank 2. At any time, only one bank is operational.

**Note**

Both firmware and software downloads are located in two banks, where one is active and the other is passive.

In the example below, bank 1 initially is both the administrative and the operational. 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 4-51 General illustration of switching Software banks

**Note**

ONS 15305: You modify the parameters related to the administrative bank. This is the bank that becomes active after restart.

You can switch between the software banks, displayed as active or inactive. Bank switch is supported with progress status such as switching, restarting, and finished.

The inactive bank will be replaced in case of a network release upgrade. However, you can select which bank to be active after a restart of the network element: The current installation state or the downloaded firmware/ software.

4.7.4.3 Manual Switching of Banks

Step 1 Select **Inactive bank**

Figure 4-52 .Select inactive bank- example

Type	Status	Name	Version	Date
BANK1	Active	8xE1-RJ45 (FW) (45004-74AA)	03	
BANK2	Inactive	(45004-74AA)	04	

- Step 2** Press **Switch bank** from toolbar or from right- click menu
The system switches bank and restarts the network element

Figure 4-53 Bank switch- example

...switching

Type	Status	Name	Version
BANK1	Active	8xE1-RJ45 (FW) (45004-74AA)	03
BANK2	Switching	(45004-74AA)	04

...restarting

Type	Status	Name	Version
BANK1	Active	8xE1-RJ45 (FW) (45004-74AA)	03
BANK2	Restarting	(45004-74AA)	04

...completed

Type	Status	Name	Version
BANK1	Active	8xE1-RJ45 (FW) (45004-74AA)	03
BANK2	Finished	(45004-74AA)	04

...after "Refresh"

Type	Status	Name	Version
BANK1	Inactive	(45004-74AA)	03
BANK2	Active	8xE1-RJ45 (FW) (45004-74AA)	04

- Step 3** Press **Refresh**.

The system is updated and presents the equipment with new software bank.

4.7.4.4 Auto Switch

By default, the switch bank is on but this default setting can be changed. Auto switch bank is the recommended setting after a download completion.

- Step 1** Select **File menu**.
- Step 2** Uncheck **Auto switch bank**.

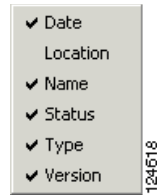
4.7.4.5 Repository

The repository lists the available download files in the management system and firmware, and software, configuration on the equipment.

Download sessions is supported with progress status such as switching, downloading, flashing, finished, and error. The system displays the a progress and status bar, if the network element supports it.

You choose visible columns in the Repository list from the right- click menu:

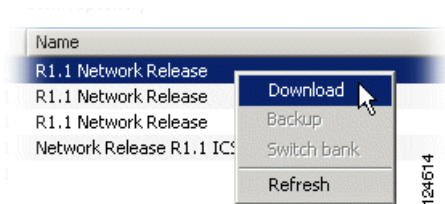
Figure 4-54 Visible Repository columns



4.7.4.6 Commands

The commands for download sessions are available from toolbar, file menu and a right- click menu. Only the relevant command will be available.

Figure 4-55 Download Command



4.7.4.7 Confirmation Dialog

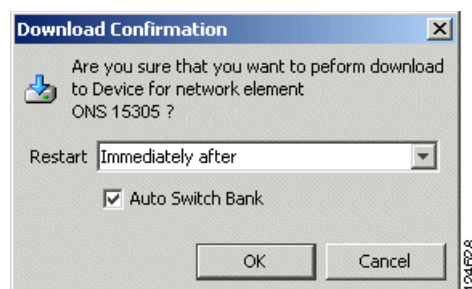
A confirmation dialog box will appear according to the command you have chosen, prior to the session starts. Only the relevant options will be available.



Note

It is not possible to reselect switch bank for sessions concerning configuration.

Figure 4-56 Download Confirmation dialog box - Example Device



Step 1 Press **OK** to confirm download session.

You may change the restart option and switch bank setting.

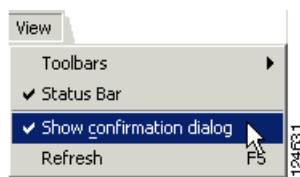
4.7.4.7.1 Deactivate Confirmation Dialog

You can turn off this function from View menu.

Step 1 Select **View** menu from toolbar.

Step 2 Uncheck 'Show confirmation dialog'

Figure 4-57 *Show Confirmation Dialog.*



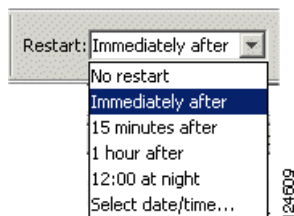
4.7.4.8 Restart Options

A network element must be restarted after a download session in order to be upgraded with the selected download file.

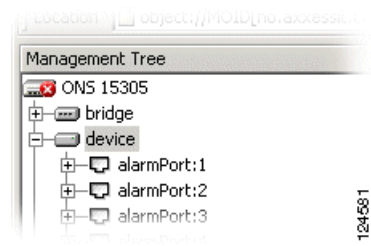
To restart automatically after download:

Step 1 Choose "Immediately after".

Figure 4-58 *Restart options*



In case of an immediate restart, the network element will be without contact for a while, presented as **connection lost** in the Management Tree.

Figure 4-59 Connection Lost During Restart

To see the new installation state of a restarted equipment:

Step 2 Press **Refresh** in the Software Download GUI.

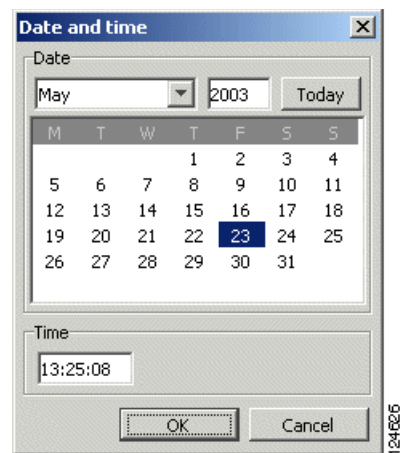
**Note**

Automatic restart is recommended. Some network elements need a manual restart, please see the [“4.5.2.8 Restart of ONS 15302”](#) section on page 4-32.

To schedule restart after download:

Step 1 Choose ‘**Select date/ time...**’ from Restart pull- down menu.

Step 2 Set **date/ time** in calendar.

Figure 4-60 Restart Calendar

Step 3 Press **OK**

4.7.5 How To Install A Downloaded File Into The Management System

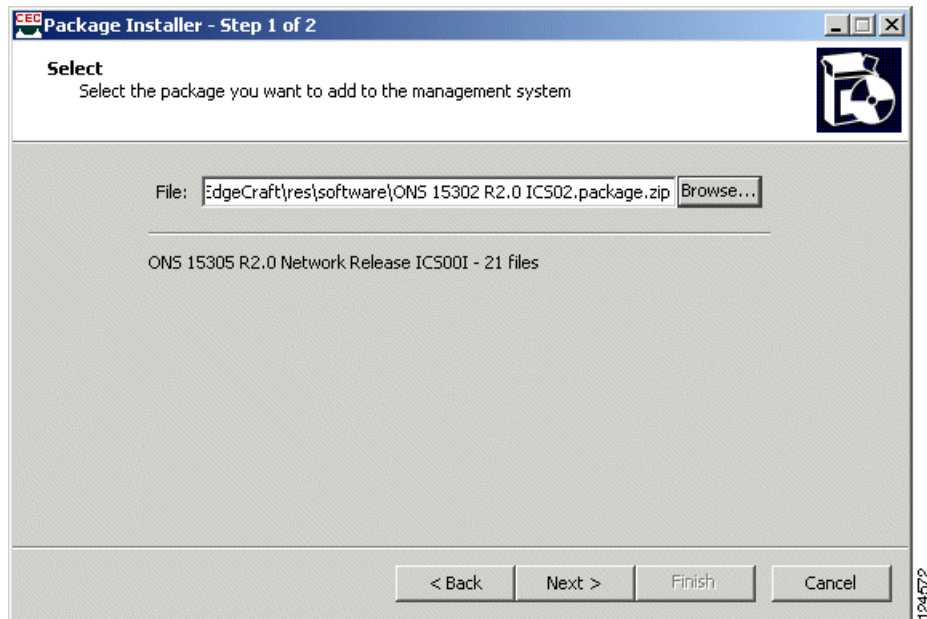
The Packet Installer will help you install software into the management system. You will select a downloaded file and add this to the central software repository. New software for the equipment will then be available from the Software Download application.

For overview see the [“4.7.3 Software Download Process”](#) section on page 4-49 and the [“4.7.3.5.3 Location Of Download Files”](#) section on page 4-51.

4.7.5 How To Install A Downloaded File Into The Management System

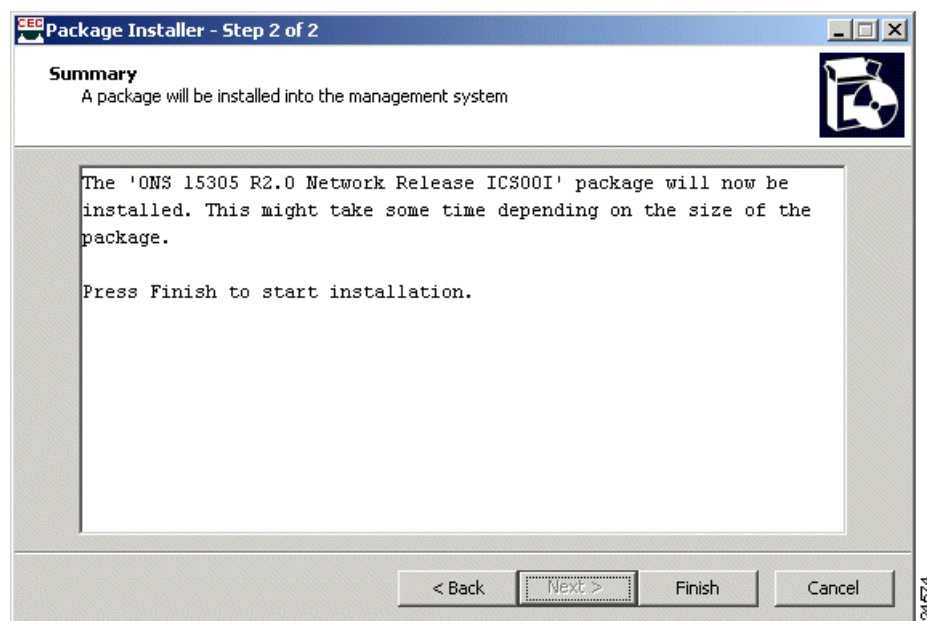
- Step 1** Select **Package Installer** from **File** menu.
- Step 2** Read the information in the introduction window, and press **Next**.
- Step 3** **Browse** and **select** download file from your software- folder, and press **open**.

Figure 4-61 Packet Installer- browser example



- Step 4** Press **Next** for summary.

Figure 4-62 Summary of file transfer

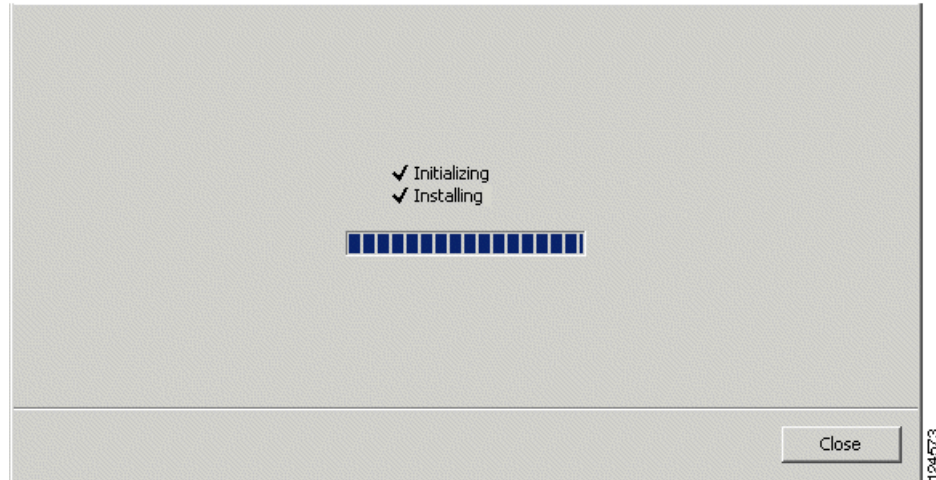


- Step 5** Verify the compatibility of the selected download file for the network element, and compare the version and ICS numbers of the download file to what is already installed on the equipment.



Note Press **Back** to reject the current download file and reselect in step 1. Press **Cancel** to exit the wizard.

- Step 6** Press **Finish** to activate file transfer.
The selected file is unpacked and transferred to the management system software repository.



- Step 7** Press **Close** to exit wizard.

The download file (network release or single file) is available in the repository list(s) in the Software Download GUI, and saved to the “.res/ software” directory. of the installed management system.

4.7.6 How to Install Download File to the Network Element

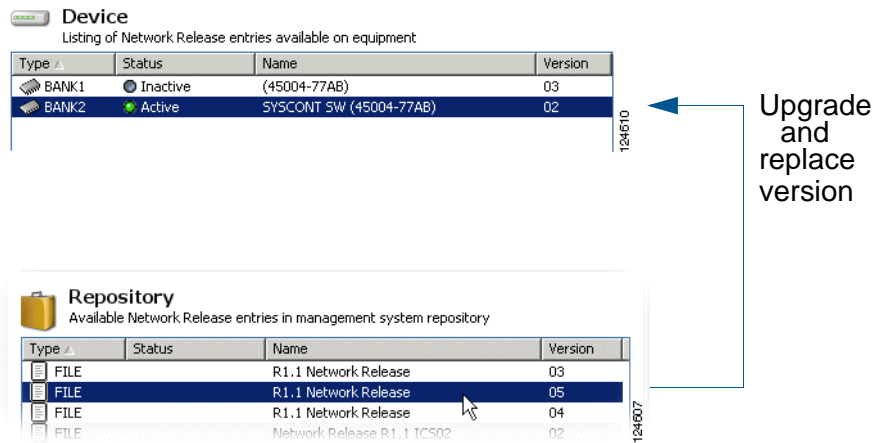


Note If a scheduled restart is set before a **new** download session is started; the scheduling parameters will be overwritten.

4.7.6.1 How To Upgrade A Network Element With A New Network Release

This procedure illustrates a network release upgrade to ONS 15305 with automatic restart of the network element and automatically switch of banks. It also apply to firmware and software download sessions.

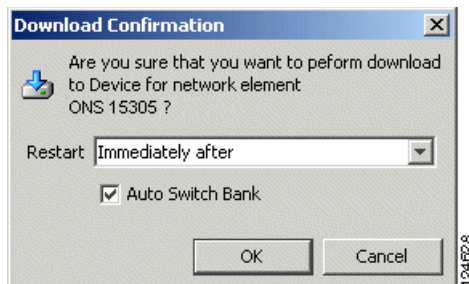
- Step 1** Open the **Network Release** pane and press **Device**.
Step 2 Select desired **Network Release** from the repository list.

Figure 4-63 Select Download File- Example R1.1 Network Release Ics05

Step 3 Choose **Immediately after** (optional), see [4.7.4.8 Restart Options, page 4-58](#) for other options.

Step 4 Press **Download**.

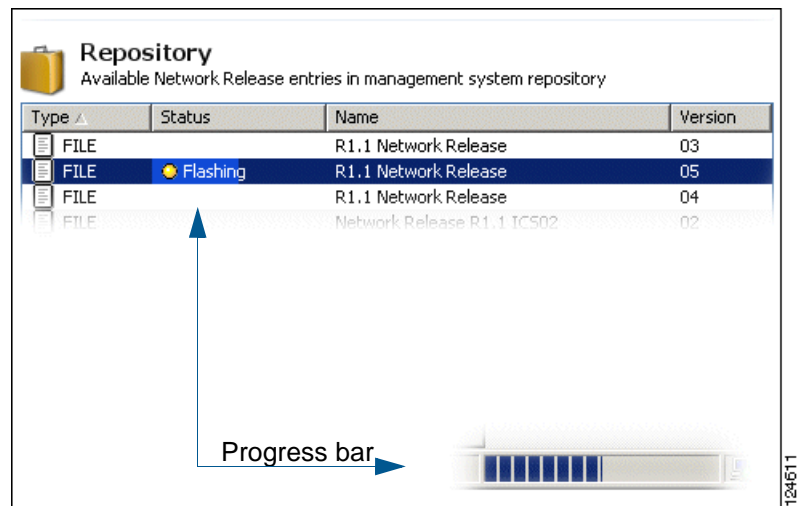
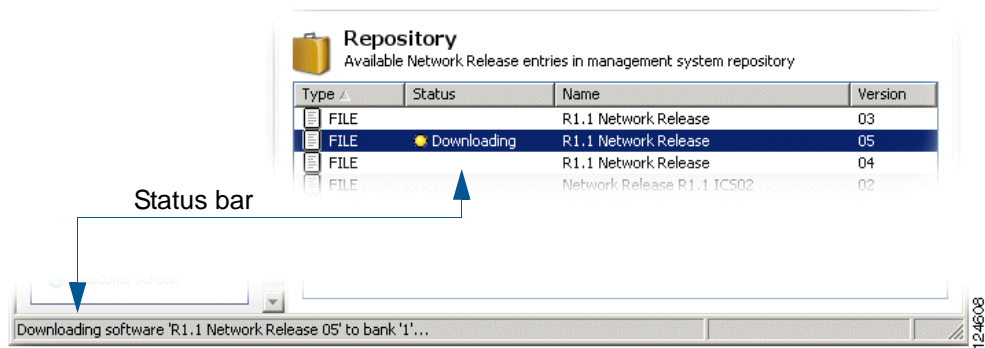
The **Download Confirmation** dialog box appears

Figure 4-64 Download Confirmation Dialog Box

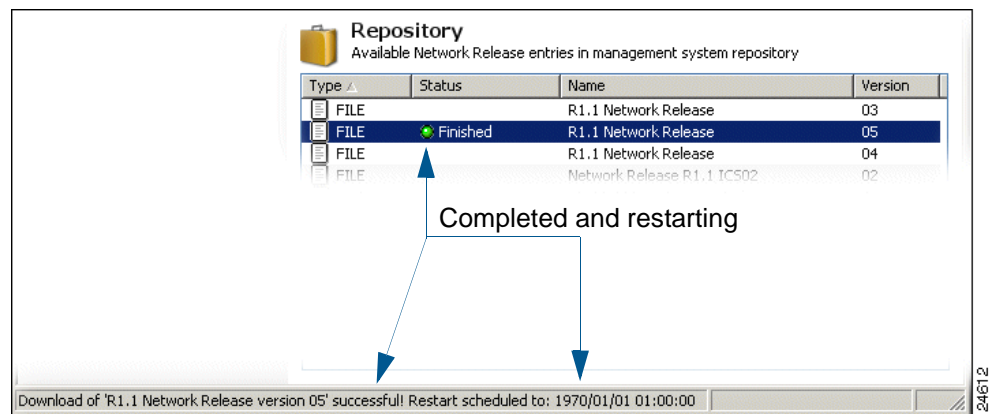
Step 5 **Confirm and / or reselect options** for restart of the equipment after the download completion, see [4.7.5 How To Install A Downloaded File Into The Management System, page 4-59](#).

Step 6 Press **OK** to confirm.

The system starts the download session.

Figure 4-65 Download session and progress- example device

Step 7 View the download progress and status bar

Figure 4-66 Restart- example device

When the download session has finished, the status bar displays restart time. This information is kept until the restart of the network element is completed.



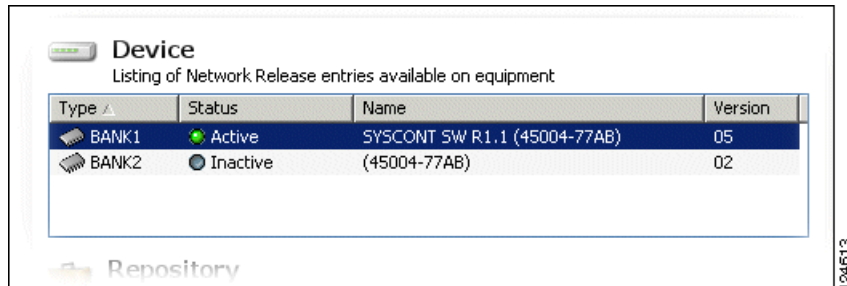
Note

For manual restart of a network element, please see page -32.

Step 8 Press **Refresh**.

The installation state of the restarted equipment is updated.

Figure 4-67 New Software installed on network element- example network release



4.7.7 How to Backup and Restore Configuration Data

Configuration data can be backed up on files and restored.

4.7.7.1 Create Backup File of Data Configuration

Follow these steps to create a backup file of your configuration.

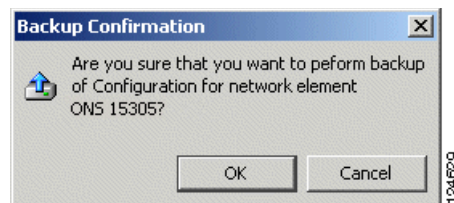
Step 1 Open the **Configuration** pane and press **Configuration**.

Step 2 Select **Active** configuration on the network element, see Figure 4-69

Step 3 Press **Backup**.

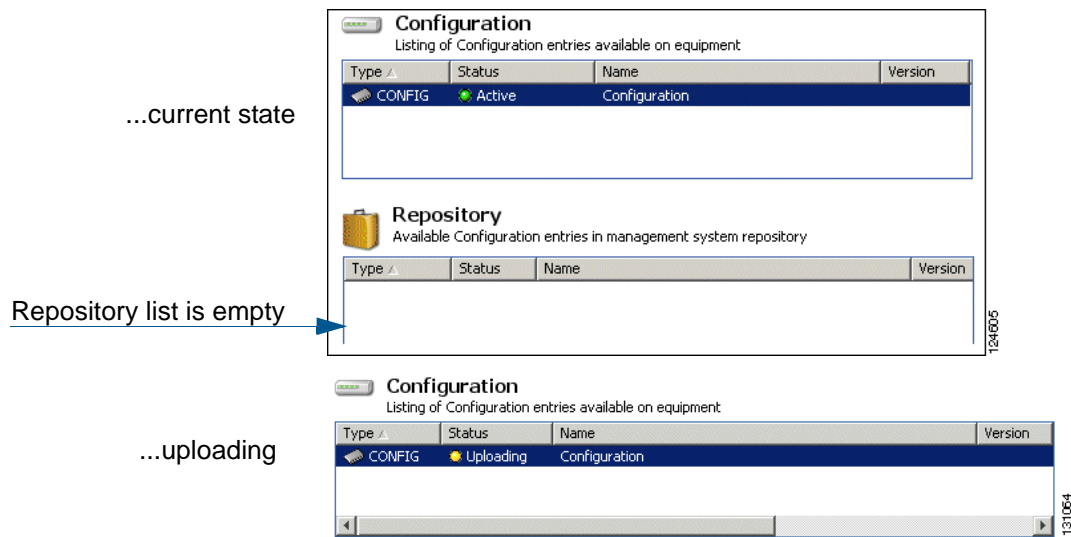
The **Backup Confirmation** dialog box appears.

Figure 4-68 Backup Confirmation dialog box



Step 4 Press **OK** to confirm.

The system creates a configuration file and saves the active configuration data from the network element.

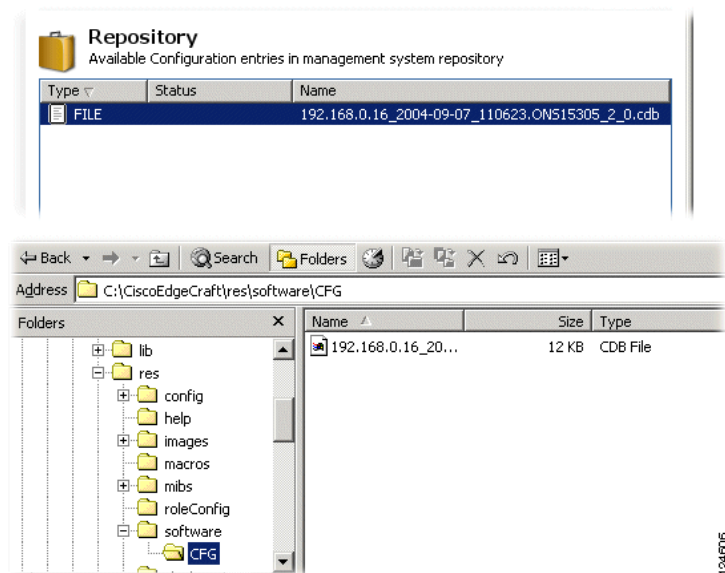
Figure 4-69 Upload session- example configuration back- up

Step 5 When the status says **Finished**, press **Refresh**.

The configuration file is available in the Repository list, as shown in Figure 4-70

Location of backup file

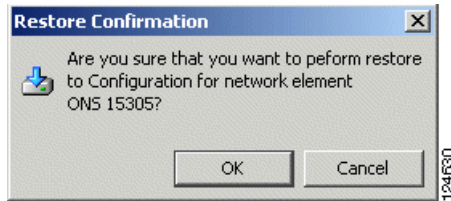
For initial backup, the management system will create a CFG- folder under “.res/ software” directory and save the backup file(s) to this folder, as shown in Figure 4-70.

Figure 4-70 Configuration folder and file- locations

4.7.7.2 Restore Data Configuration From Backup File

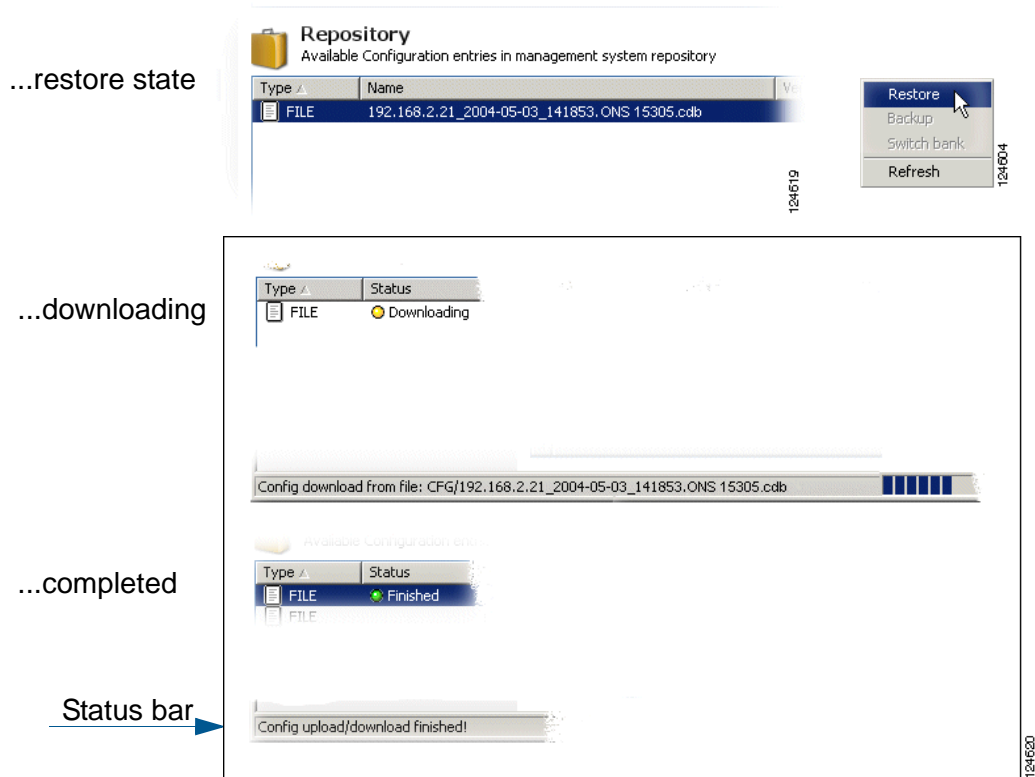
- Step 1** Open the **Configuration** pane and press **Configuration**.
- Step 2** Select desired **configuration backup file** from the Repository list.
- Step 3** Click **Restore**.
- The **Restore Confirmation** dialog box appears.

Figure 4-71 Restore Confirmation Dialog Box



- Step 4** Press **OK** to confirm.

Figure 4-72 Restore data configuration- example



- Step 5** Click **Refresh** after session completion.
- The configuration data of the network element is restored.

4.8 Download Software to 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 be able to start download of 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.

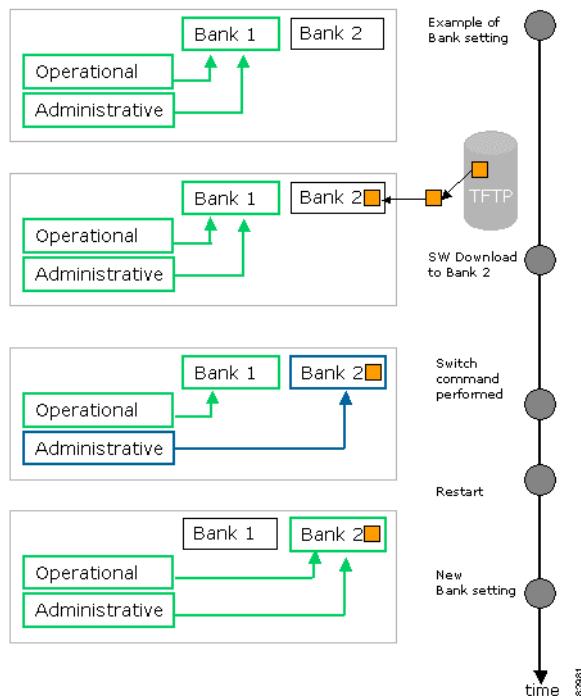
4.8.1 Network Release

The network element contains device software and firmware, and module firmware. Updates of the software and firmware is 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, that means check which files are included in the release and download those files that are missing or are too old in the network element.

4.8.2 Operational and Administrative Software Bank

ONS 15305 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 4-73](#). 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 4-73 Example of Switching Software Banks

4.8.3 How do Software Upgrades Affect Traffic?

A software update/upgrade including FPGA fix will affect all traffic. Traffic affected depends on module configuration, hence a Network Release download will affect the modules that are 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 STP mode is changed e.g. from per. Device to per VLAN (Ethernet/IP traffic affecting)
- when decreasing/increasing entries in tunable tables e.g. maxARP, maxVLAN's, maxBridge, etc.
- software upgrade without FPGA fix (Ethernet/IP traffic affecting)
- software upgrade with FPGA fix (All traffic affected)

The period of time from the moment you have triggered a restart to the device is up and running is dependent of modules and Software configuration of the device. The down period is dependent of inserted modules and configuration.

4.8.4 Download ONS 15305 Network Release

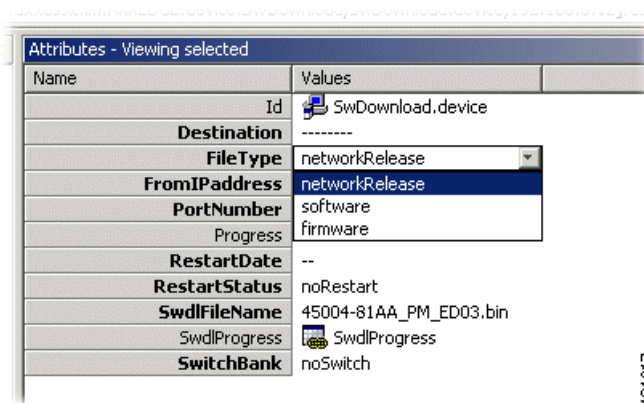
A Network Release is delivered as a zip-file together with a network release control file, [Figure 4-74](#).

**Note**

Please see Release Notes for an example of a TFTP server that has been verified to work in co- operation with Cisco EdgeCraft.

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

Figure 4-74 Download of Release Files



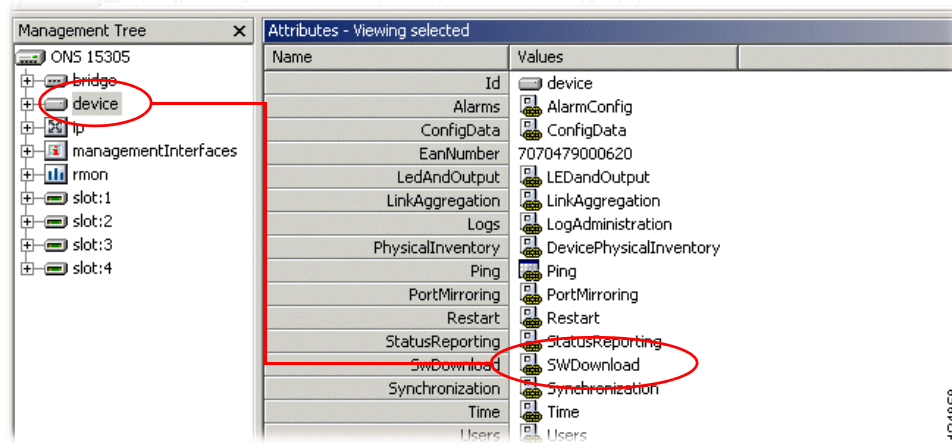
- Step 6** Enter **FromIPAddress** (TFTP server Ip address).
- Step 7** Set **restartstatus** to **immediateRestart**.
- Step 8** Enter **SwdlFileName** attribute values (File path and name).
- Step 9** Click **Save**.

**Note**

The status of the SwitchBank attribute (switch/noSwitch) is overruled when Filetype is set to networkRelease, thus a switch will be performed.

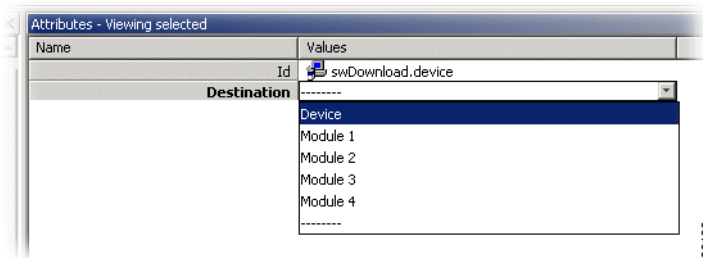
4.8.5 Software Download to ONS 15305

- Step 1** Select device and then **SWDownload**, [Figure 4-75](#).

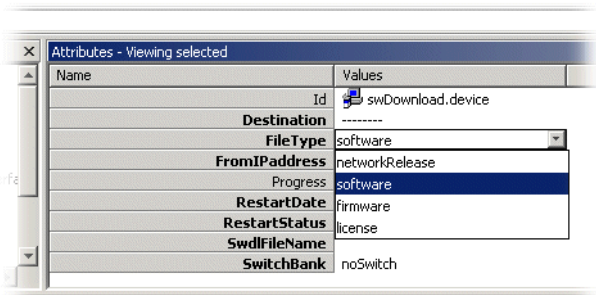
Figure 4-75 Select Device

The following attributes are modifiable, see [Figure 4-76](#) to [Figure 4-82](#).

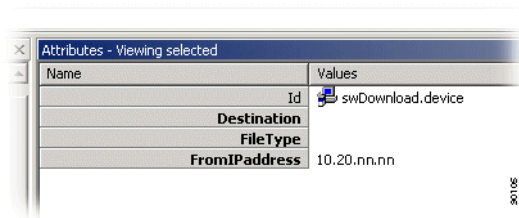
Step 2 Select desired **destination**.

Figure 4-76 Select Destination

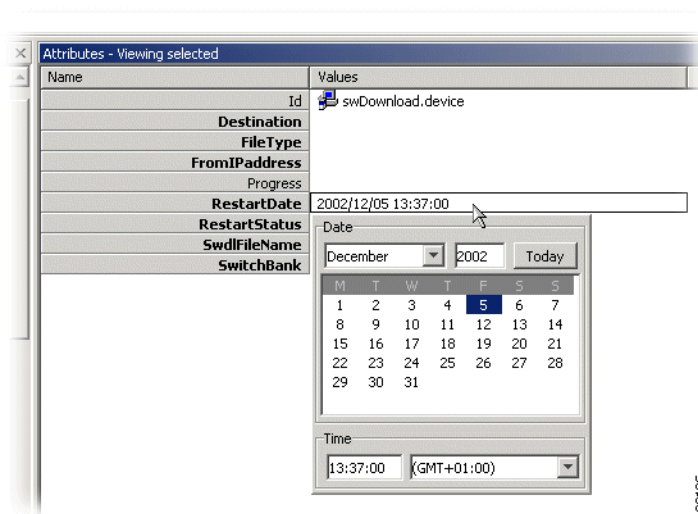
Step 3 Set **FileType** to software.

Figure 4-77 Select Filetype

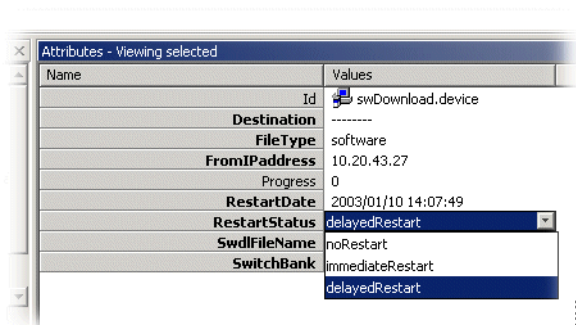
Step 4 Enter **FromIPAdress** (TFTP server Ip address).

Figure 4-78 Select IP Address

Step 5 Set **RestartDate** if you want **delayed restart** see [Step 6](#).

Figure 4-79 Set Restart Date

Step 6 Select **RestartStatus**.

Figure 4-80 Select Delayed Restart

Select whether network element should restart immediately or at a specific date/time after the download process.

Step 7 Enter **SwdIFFileName** attribute values (File path and name).

Figure 4-81 Set Software Download File Name

Name	Values
Id	swDownload.device
Destination	
FileType	
FromIPAddress	
Progress	
RestartDate	
RestartStatus	
SwdlFileName	
SwitchBank	

Step 8 Set **SwitchBank** attribute.

Figure 4-82 Select Switch Bank Attributes

Name	Values
Id	swDownload.device
Destination	
FileType	
FromIPAddress	
Progress	
RestartDate	
RestartStatus	
SwdlFileName	
SwitchBank	noSwitch switch noSwitch

- Switch

After the restart the operational bank will be switched and the new (downloaded) Software 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 the [“4.8.5.1 Manual Switch of Banks” section on page 4-72](#).

Step 9 Click **Save**.

4.8.5.1 Manual Switch of Banks

Follow these steps to manually switch banks

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

4.8.6 Software Download to ONS 15302

Follow these steps to download software to ONS 15302

-
- | | |
|---------------|--|
| Step 1 | Select device > SWdownload . |
| Step 2 | Enter FromIPAddress (TFTP server Ip address). |
| Step 3 | Enter SwdlFileName attribute values (File path and name). |
| Step 4 | Click Save . |
| Step 5 | Perform a restart. |
-

4.9 Backup and Restore NE Configuration Data

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

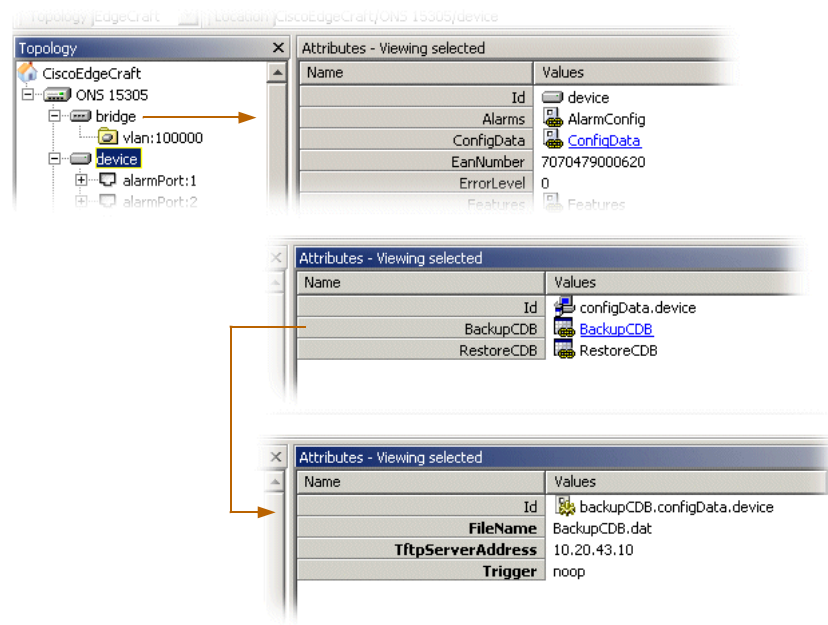
The section involves backup, presentation of an ongoing back-up process and starting a restore process configuration data between a host and a network element.

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

4.9.1 Backup Configuration Data

Backup CDB will perform a back-up of the configuration data of selected NE and place it on the TFTP-server.

-
- | | |
|---------------|--|
| Step 1 | Select device in the management tree. |
| Step 2 | Click on ConfigData . Here you select whether to upload or download the configuration from or to the network element, Figure 4-83 . |

Figure 4-83 Select ConfigData**Step 3** Select **BackupCDB**.

The following attributes values are modifiable:

- 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 4 Enter values for the parameters and set **trigger** to **backup**.**Step 5** Click **Save** to commit the changes.**Step 6** 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 It is recommended to monitor the TFTP console during the upload process.



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

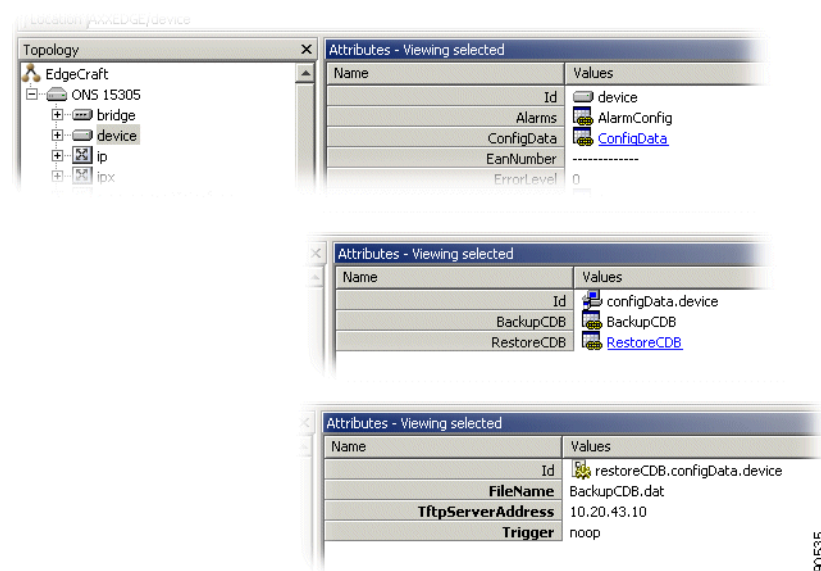
4.9.2 Restore Configuration Data

The previous configuration data restore session has finished. If a scheduled restart is set before a new configuration data download process is started, the scheduling parameters will be overwritten.

In order 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. This is the trigger needed by Cisco Edge Craft to restart the NE. For enabling trap-sending see [Chapter 1, “Configure Community-Handler.”](#)

- Step 1** Select device in the management tree.
- Step 2** Click on **ConfigData**. Here you select whether to upload or download the configuration from or to the network element, [Figure 4-84](#).

Figure 4-84 Select Device



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

The following attributes values are modifiable:

- 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 4** Set the parameters for the configuration data restore and set **trigger** to **restore**.
- Step 5** Click **Save** to commit the changes.

- Step 6** The TFTP upload process starts in the network element and the configuration data is stored in the network element. Cisco Edge Craft will after a restore is completed, restart the network element.



Note It is recommended to monitor the TFTP console during the download process.

4.10 Alarm and Event Configuration

The purpose of this section is to guide you through the configuration of alarm and event reporting, and to be able to 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. ONS 15305 let you suppress a number of different alarm types, for example AIS.

In some situation you might want to suppress alarms that are kind of oscillating between being active and not active. 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.

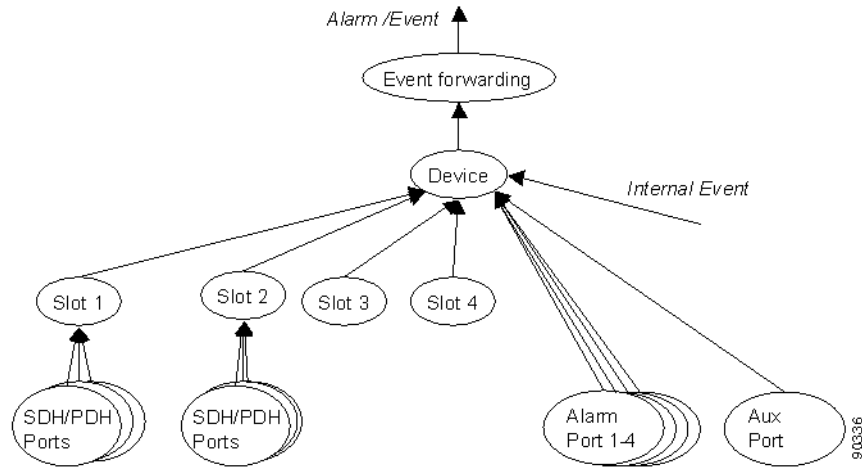
4.10.1 Event Forwarding

No alarms or events can 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 [“5.4.3 Setting a Loop in an ONS 15302 PDH port”](#) section on page 5-10.

4.10.2 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 4-85](#). In addition the event forwarding must be configured for the managers IP address as described in the [“4.10.1 Event Forwarding”](#) section on page 4-76.

Figure 4-85 General Alarm Reporting Filters.

Note that all alarms from objects [4.10.2.1 Device Alarm Enabling, page 4-77](#) to [4.10.2.5 Aux Port Alarm Enabling, page 4-78](#) including itself have to pass through the filter.

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

4.10.2.1 Device Alarm Enabling

It is possible to enable or disable alarm and event reporting from ONS 15305. In the disabled state, no alarms or events are reported (some generic events, like cold start, etc. are still reported).

-
- Step 1** Select device > **AlarmConfig** > **AlarmReporting**.
- Step 2** Set **AlarmReporting** to **enabled** or **disabled**.
-

4.10.2.2 Slot Alarm Enabling

Slot Alarm enabling:

-
- Step 1** Select the slot that should report alarms.
- Step 2** Set **AlarmReporting** to **enabled**.
-

4.10.2.3 Traffic Port Alarm Enabling

Traffic port alarm enabling:

-
- Step 1** Select the SDH or PDH port that should report alarms.

Step 2 Set **AdminStatus** to **enabled**

4.10.2.4 Alarm Port Alarm Enabling

Alarm port alarm enabling:

Step 1 Select the Alarm port that should report alarms.

Step 2 Set **AdminStatus** to **enabled** or **disabled**.

4.10.2.5 Aux Port Alarm Enabling

Aux port alarm enabling

Step 1 Select the Aux port that should report alarms.

Step 2 Set **AdminStatus** to **enabled**.



Note

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

4.10.3 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.

4.10.3.1 Suppress RDI, EXC, DEG, SSF Alarms

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

Step 1 Select device > **AlarmConfig** > **AlarmReportingVc**.

Step 2 Set **suppress** for the **attributes** corresponding to the **Alarms** that should be suppressed:

- RdiAlarms
 - ExcAlarms
 - DegAlarms
 - SsfAlarms
-

4.10.3.2 Suppress AIS Alarms from SDH Ports

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

-
- | | |
|---------------|--|
| Step 1 | Select device > AlarmConfig > AlarmReportingVc . |
| Step 2 | Set suppress for the AisAlarms attribute. |
-

4.10.3.3 Suppress AIS Alarms from E1 Ports

Suppress AIS Alarms from E1 ports

-
- | | |
|---------------|--|
| Step 1 | Select device > AlarmConfig > AlarmReportingE1 . |
| Step 2 | Set AisAlarms to suppress . |
-

4.10.3.4 Suppress AIS Alarms from AUX Port

Suppress AIS alarms from AUX port

-
- | | |
|---------------|---|
| Step 1 | Select device > AlarmConfig > AlarmReportingAux . |
| Step 2 | Set AisAlarms to suppress . |
-

4.10.4 Modify Alarm Severity and Description

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

-
- | | |
|---------------|--|
| Step 1 | Select device > AlarmConfig > AlarmPointConfig . |
| Step 2 | Set the severity level and description for the combination of alarm type and object type of your choice. 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. |
-

4.10.5 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 | Select device > AlarmConfig > SdThreshold . |
|---------------|---|
-

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

4.10.6 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 4-10](#) to [Table 4-12](#).

4.10.6.1 Persistency Group 1 (HighOrderLevel)

The table below shows associated alarm types grouped with associated object types:

Table 4-10 *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
CDF	rs, ms
AUX	auxPort

4.10.6.2 Persistency Group 2 (Unfiltered)

Persistency group 2:

Table 4-11 *Persistency Group 2 (Unfiltered)*

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

4.10.6.3 Persistency Group 3 (LowOrderLevel)

Persistency group 3:

Table 4-12 *Persistency 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** Select device > **AlarmConfig** > **AlarmPersistency**.
- Step 2** Set **onFilter** or **offFilter** to a value between 0 and 30 seconds.

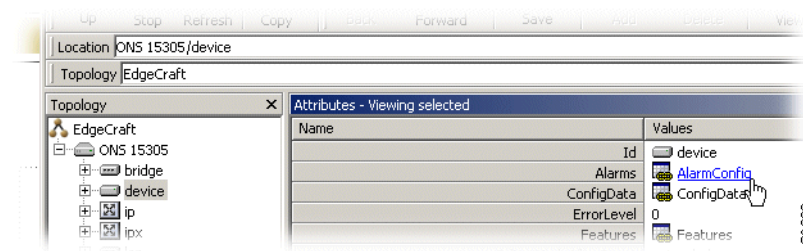
4.10.7 Modify ONS 15302 Alarm Configuration Attributes

This section explains how to modify alarm configuration attributes on the ONS 15302

4.10.7.1 Location of Alarm Configuration Attributes

Find alarm configuration attributes:

- Step 1** Select device > **AlarmConfig**, [Figure 4-85](#).

Figure 4-86 *Select Device*

4.10.7.2 Modify Alarm Severity and Description

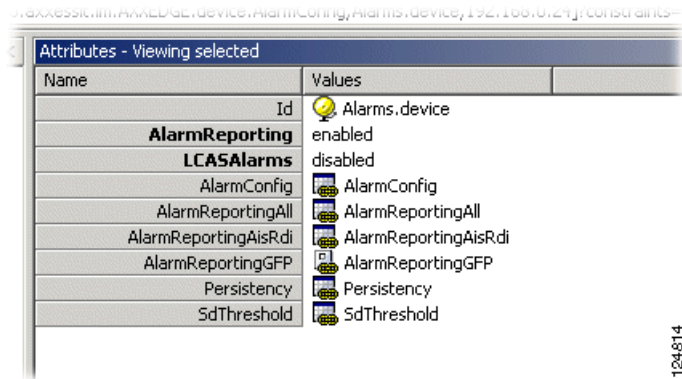
Modify Alarm severity and description like this:

4.10.7 Modify ONS 15302 Alarm Configuration Attributes

Step 1 Select device > **AlarmConfig** > **AlarmConfig**, [Figure 4-87](#).

Figure 4-87 Select Alarm Config

https://www.cisco.com/.../device/AlarmConfig/Alarms/device/192.168.0.21/constaints=...



Name	Values
Id	Alarms.device
AlarmReporting	enabled
LCASAlarms	disabled
AlarmConfig	AlarmConfig
AlarmReportingAll	AlarmReportingAll
AlarmReportingAisRdi	AlarmReportingAisRdi
AlarmReportingGFP	AlarmReportingGFP
Persistence	Persistence
SdThreshold	SdThreshold

124814

Step 2 Set the **Severity level** and **Description** for the combination of alarm type and object type of your choice.

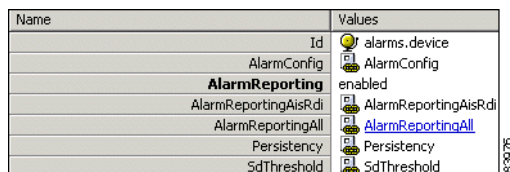
Step 3 Click **Save**. The next time the alarm is reported from this object type it will come up with the configured severity and description in the alarm list.

4.10.7.3 View all Alarm Reporting Instances

View alarm reporting instances:

Step 1 Select **AlarmReportingAll** to view all alarm reporting instances, [Figure 4-88](#).

Figure 4-88 Select AlarmReportingAll



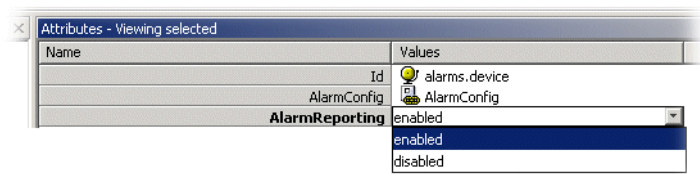
Name	Values
Id	alarms.device
AlarmConfig	AlarmConfig
AlarmReporting	enabled
AlarmReportingAisRdi	AlarmReportingAisRdi
AlarmReportingAll	<u>AlarmReportingAll</u>
Persistence	Persistence
SdThreshold	SdThreshold

83876

4.10.7.4 Enable Alarm Reporting

Enable Alarm reporting:

Step 1 Set **AlarmReporting** to **enable** using the available pull-down menu, [Figure 4-89](#).

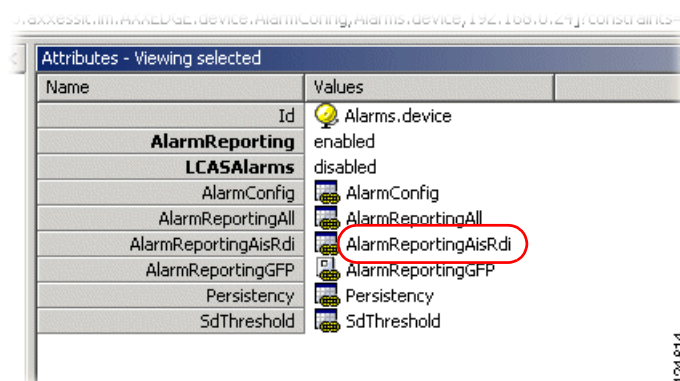
Figure 4-89 *Select AlarmReporting*

Step 2 Click Save.

4.10.7.5 Modify Ais Rdi Alarm Reporting

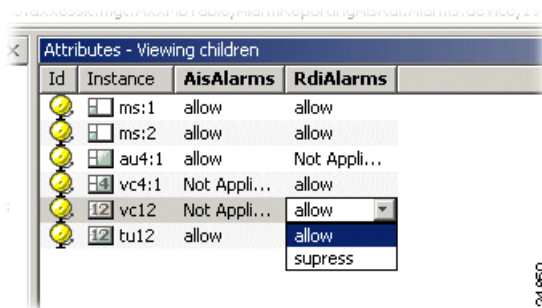
How to modify Ais Rdi alarm reporting.

Step 1 Select **AlarmreportingAisRdi**, [Figure 4-90](#).

Figure 4-90 *Select AlarmreportingAisRdi*

Step 2 Select desired instance.

Step 3 Select **allow** or **suppress** for Ais alarm, [Figure 4-91](#).

Figure 4-91 *Select AIS Attributes*

Step 4 Repeat for Rdi alarm.

4.10.7 Modify ONS 15302 Alarm Configuration Attributes

Step 5 Click **Save**.

4.10.7.6 Modify Alarm Persistency

Modify the alarm persistency:

Figure 4-92 Set Alarm Persistency Attributes

Name	Values
Id	alarms.device
AlarmConfig	AlarmConfig
AlarmReporting	enabled
AlarmReportingAisRdi	AlarmReportingAisRdi
AlarmReportingAll	AlarmReportingAll
Persistency	Persistency
SdThreshold	SdThreshold

Alarm reporting on and off can be delayed by setting the Alarm Persistency filters in ONS 15302.

- Step 1** Select device > **AlarmConfig** > **AlarmPersistency**, [Figure 4-92](#).
- Step 2** Set **onFilter** or **offFilter** to a value between 0 and 255 seconds.
- Step 3** Click **Save** when desired value settings are completed.

4.10.7.7 Modify Signal Degraded (Sd) Threshold

How to modify degraded Sd threshold:

- Step 1** Select **SdThreshold**, [Figure 4-93](#).

Figure 4-93 Select SDThreshold

Name	Values
Id	alarms.device
AlarmConfig	AlarmConfig
AlarmReporting	enabled
AlarmReportingAisRdi	AlarmReportingAisRdi
AlarmReportingAll	AlarmReportingAll
Persistency	Persistency
SdThreshold	SdThreshold

- Step 2** Select desired **MO** class
- Step 3** Set **SdThreshold** to a value between 6 and 9, [Figure 4-94](#).

Figure 4-94 Set SDThreshold

Id	MoClass	SdThreshold
axxc155ESdhMsSignalDegradedThreshold:1	Ms	9
axxc155ESdhMsSignalDegradedThreshold:2	Ms	7
axxc155ESdhRsSignalDegradedThreshold:1	Rs	7
axxc155ESdhRsSignalDegradedThreshold:2	Rs	6
axxc155ESdhVc4SignalDegradedThreshold:1	Vc4	8
axxc155ESdhVc12SignalDegradedThreshold	Vc12	7

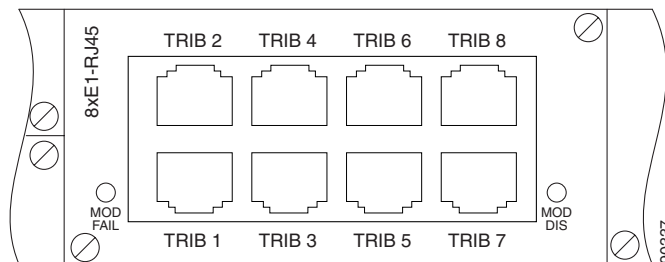
Step 4 Click **Save**.

4.11 Manage Slots on ONS 15305

A slot represents a physical position on the network element where different Hardware modules can be located, [Figure 4-95](#). The purpose of this section is to describe the tasks and dynamic involved in inserting modules into and removing modules from a slot.

This section also involves presentation and modification of slots. Slots are static and cannot be created or deleted.

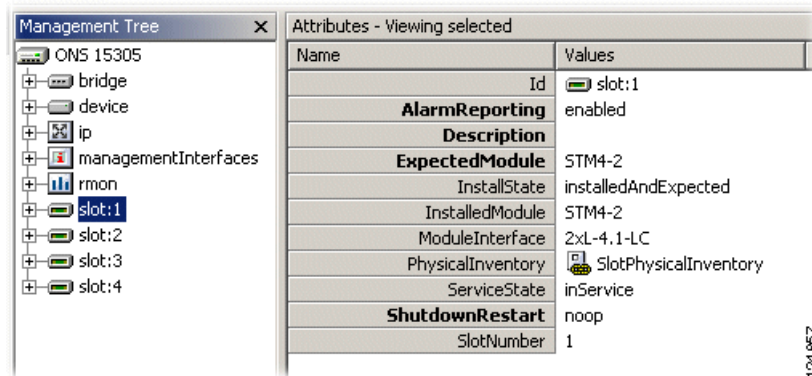
Figure 4-95 Slot on the Network Element



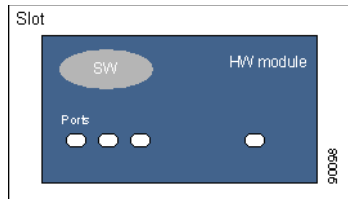
4.11.1 View Slot

- Step 1** The management tree 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 Hardware module. By default the slot is unequipped, [Figure 4-96](#).
- Step 2** Select a slot in the management tree.

Figure 4-96 Select Slot



1244857

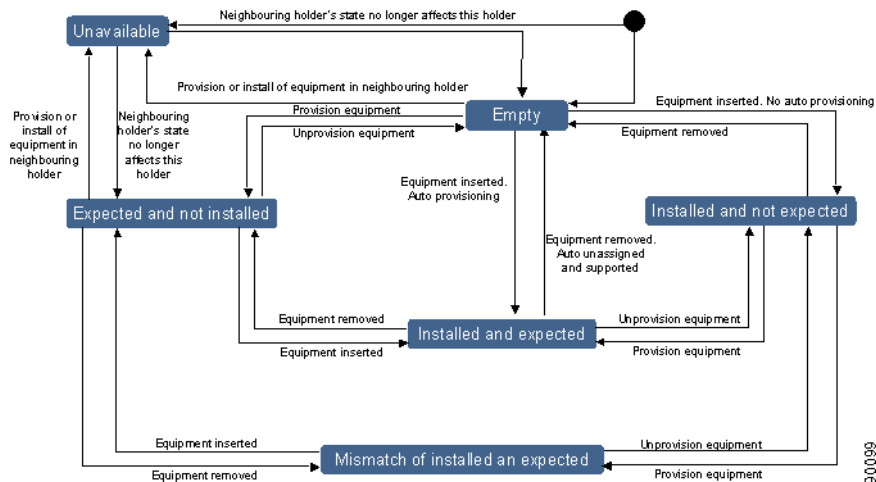
Figure 4-97 Slot Module - Port Concept

A slot can be empty or have a Hardware module with a given number of ports and Software version installed as illustrated in [Figure 4-97](#). The physical inventory data for the module, if module present in slot, is also presented in the attribute window.

You can configure the slot and set the expected module type for the slot. The module does not have to be physically inserted. The slot has therefore an attribute that reflects the relation between the expected module and the installed module, that means the slot state:

- 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 4-98](#). This is the suggested state machine from *TMF 814 supporting documentation*.

Figure 4-98 Relation between Installed and Expected Module in a Slot.

A state machine for the values of the attribute describing the relation between installed and expected module in a slot is shown in [Figure 4-98](#).

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, that means a match between expected and installed.

You can configure an expected module and assign it to a slot without any physical module present. The system populates the management tree according to the specified expected module. Before replacing a module, that means selecting a new expected module type, the expected module of the slot must be set to unequipped.

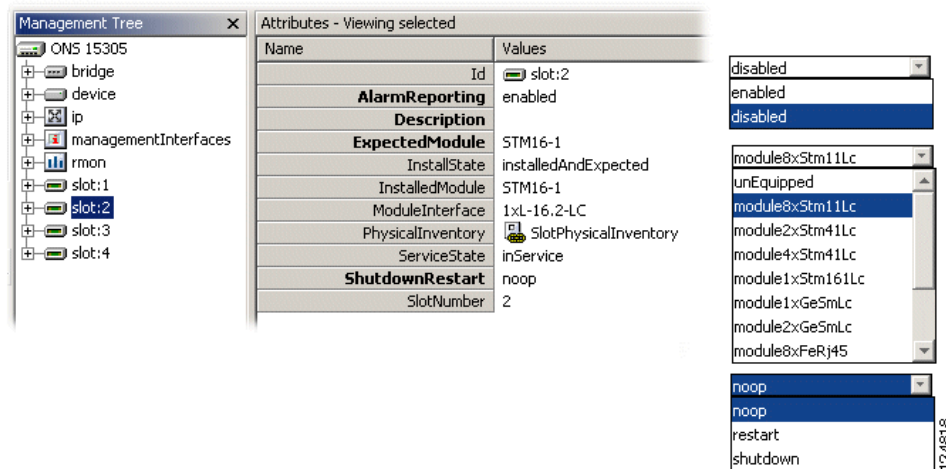
For management of different ports, see [Chapter 5, “Traffic Port Management”](#).

4.11.2 Modify Slot

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

Step 1 Select target slot, [Figure 4-99](#).

Figure 4-99 Select Target Slot



Step 2 The following attributes are modifiable:

- 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 physical interface on selected module. Thus this attribute value indicates LongHaul (ex. L-4.2-LC), ShortHaul (ex. S-4.1-LC) for STM modules. Connector is also indicated. See.

Step 3 Modify the modifiable slot attributes.

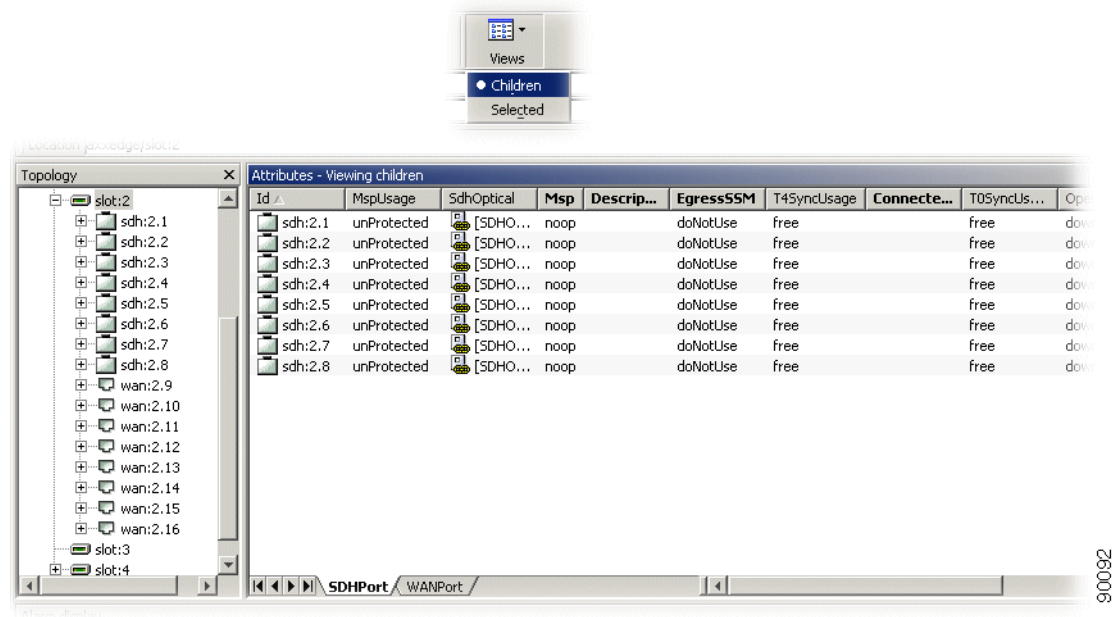
4.11.2 Modify Slot

Step 4 Click **Save** to activate the modifications.

For some of the changes to take effect a restart of the module is required. In these cases you are prompted to restart.

Step 5 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 4-100](#).

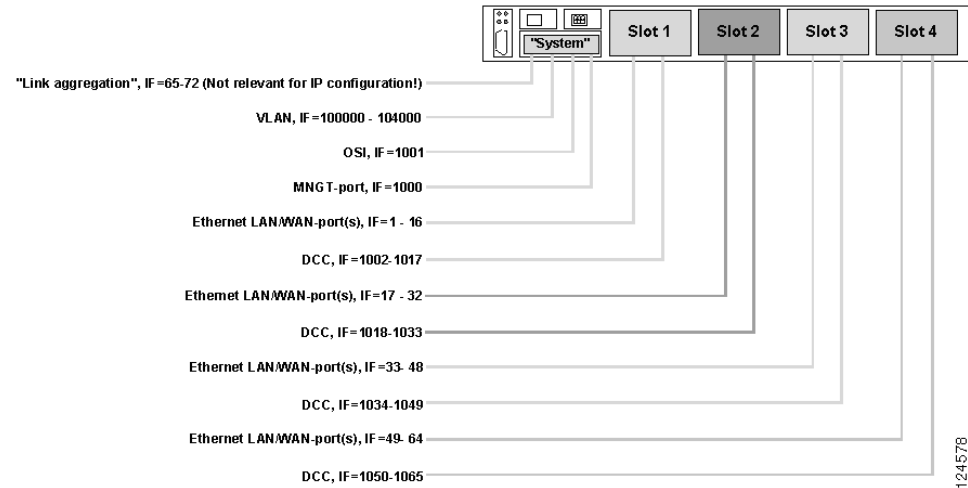
Figure 4-100 Set View Mode to Children



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

4.11.2.1 ONS 15305 Physical Interface Indices

Figure 4-101 IF-indices for physical/logical ports on the ONS 15305





Traffic Port Management

5.1 About Port Types

One of the advantages of the ONS 15305 compared to other products is the possibility to equip it 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.

See also the [“4.2.1 Manage the Management Interfaces of the Network Element” section on page 4-2](#), the [“Alarm Ports” section on page 4-35](#), and the [“AUX Port - ONS 15305” section on page 4-36](#).

Traffic ports are available on replaceable traffic modules. When a slot is configured to support a specific traffic module the ports of the traffic module is automatically created as described in the [“4.11 Manage Slots on ONS 15305” section on page 4-85](#).

In this chapter we concentrate on the configuration of the traffic ports. The chapter is organized according to the following structure:

- SDH ports
- PDH ports
- LAN ports
- WAN ports

5.2 Selecting a Traffic Port

Traffic ports are always located on a traffic module in slot 1 to 4. In ONS 15305 managed objects for modules and ports are available when the slot is configured for a specific module type. This section describes how to select a traffic port regardless of the traffic it carries.

-
- | | |
|---------------|---|
| Step 1 | Click on the ONS 15305 managed object, and then the slot managed object (where the port is) in the management tree. |
| Step 2 | When the slot is expanded, click on the port managed object with the desired port number. |
| Step 3 | The port is selected and the attributes related to the physical and electrical characteristics of the port is displayed in the attributes view.
The physical port usually carries a set of protocols (for example SDH) and the protocols are available from the management tree. |
-

5.3 SDH Ports



Note

Some procedures in this chapter apply for both ONS 15302 and ONS 15305. For procedures that only apply for ONS 15305, this is stated in the procedure heading.

5.3.1 Configuring ONS 15305 SDH Port Structure (Channelization)

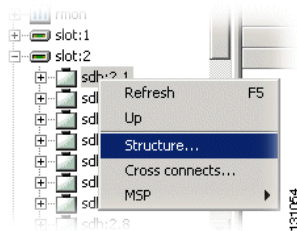
By default the SDH ports are unstructured (or not-channelized) when created. Only the SDH port, rs, ms and aug1 managed objects are available. In this state the paths inside the STM-N frame cannot be terminated nor cross-connected, but the port can be used as a protection port in an MSP protection scheme and as 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 management tree, showing termination points that are now available for cross-connection.

5.3.1.1 SDH Structuring Wizard

This wizard lets you to change the structure of an SDH object. The next steps let you set up the type of structure you want.

Figure 5-1 Open The Structuring Wizard



-
- Step 1** Select desired **SDH port**
- Step 2** Right-click and select **Structure**.

Figure 5-2 SDH Structuring Wizard

No changes will be performed until you press Finish and you can abort the wizard at any given time by pressing the Cancel button.

Structure Information displays the current SDH structure. The decisions you make in subsequent steps will affect this structure

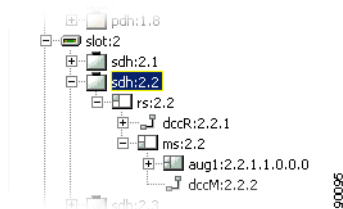
Structure Type; Select the type of SDH structure you want.

Completing the Structure SDH Structuring Wizard; This step lists all the changes that will be performed when you press Finish.

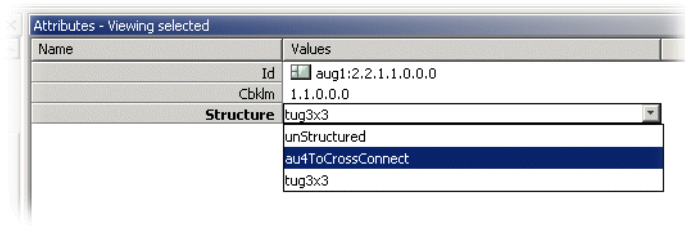
The following sections show how to perform structuring using the Management Tree.

5.3.1.2 AU4 Termination Points for Cross-connection

- Step 1** Select an SDH port, [Figure 5-3](#).
- 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 5-3 Select the Aug1 Managed Object

- Step 4** Set the **Structure** attribute to **au4ToCrossConnect**, [Figure 5-4](#).

Figure 5-4 Set the Structure Attribute

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

5.3.1.3 Tu3 Termination Points for XC

Tu3 termination points for XC.

- Step 1** Perform [Step 1](#) to [Step 3](#) in the “[5.3.1.2 AU4 Termination Points for Cross-connection](#)” section on [page 5-3](#).
- Step 2** Set the **Structure** attribute to **tug3x3**.
- Step 3** Select the **au4**, **vc4** and then the **tug3** managed object 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.

5.3.1.4 Tu12 Managed Objects for XC

Tu12 managed objects for XC.

- Step 1** Perform [Step 1](#) to [Step 3](#) in the “[5.3.1.2 AU4 Termination Points for Cross-connection](#)” section on [page 5-3](#).
- Step 2** Set the **Structure** attribute of the **tug3** managed object to **tu12x21**.
- Step 3** Click **Save** on the toolbar.
- Step 4** Repeat for the other tug3 objects on the port if you want to structure them as **x21tu12**.

5.3.2 Modifying or Removing 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.

5.3.2.1 Modify between Tu12 and Tu3 Objects

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 “5.3.1 Configuring 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. |
-

5.3.2.2 Modify between Au4 and Tu3 or Tu12 Objects

How to 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 unStructured for all tug3 objects contained by the aug1 object that should be modified, “5.3.2.1 Modify between Tu12 and Tu3 Objects” section on page 5-5 . |
| Step 3 | Follow the guidelines in “5.3.1 Configuring 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 Modification of the structure involves deletion of existing termination points and creation of new termination points (if new structure is not **unStructured**). To avoid unintentional traffic loss, 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 **unStructured** before the aug1 can be modified.

5.3.3 Setting and Reading Path Trace Identifiers

Path Trace are available at two levels in the SDH port:

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

5.3.3.1 Set or Read RS Path Trace Identifiers

How to set or read RS path trace identifiers:

-
- | | |
|---------------|--|
| Step 1 | Select an SDH port. |
| Step 2 | When the SDH port managed object is expanded, click on the rs . |
-

Step 3 Click on **PathTrace**.

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.

5.3.3.2 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, that means aug1 Structure is tug3x3, “[5.3.1 Configuring 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 on **PathTrace**.

The attributes are the same as for RS path trace [Step 4](#).

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.

5.3.4 Monitoring 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.

5.3.4.1 Read RS PM Counters

How to 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 on **PmG826NearEnd** to read near end PM data **or** **PmG826FarEnd** to read far end PM data.
- Step 5** The following attributes are available:
- Current15Min ES,SES, BBE and UAS
 - Current24Hour ES, SES, BBE and UAS
- Step 6** 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.
- Step 7** The following attributes are available:
- Interval15Min ES,SES, BBE and UAS
 - Interval24Hour ES, SES, BBE and UAS

5.3.4.2 Read MS PM Counters

How to 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 the **PMG826** link for PmG826NearEnd to read near end PM data or PmG826FarEnd to read far end PM data.
- Step 4** The attributes are the same as for RS PM.

5.3.4.3 Read VC-4 PM Counters

How to 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 the **PMG826** link for PmG826NearEnd to read near end PM data or PmG826FarEnd to read far end PM data.
- Step 6** The attributes are the same as for RS PM in [“5.3.4.1 Read RS PM Counters”](#) section on page 5-7.

5.3.5 Enabling 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 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.

5.3.6 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 that is output 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 **DoNotUse** automatically.

5.3.7 Use the SDH Port as a Synchronization Source Input

See the [“4.6.4 Add Synchronization Source Candidate \(T0 or T4\)”](#) section on page 4-44.

5.3.8 Carry Management Traffic DCC by SDH Port Channels

See the [“4.3.2 DCC Configuration”](#) section on page 4-17.

5.4 PDH Ports

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.

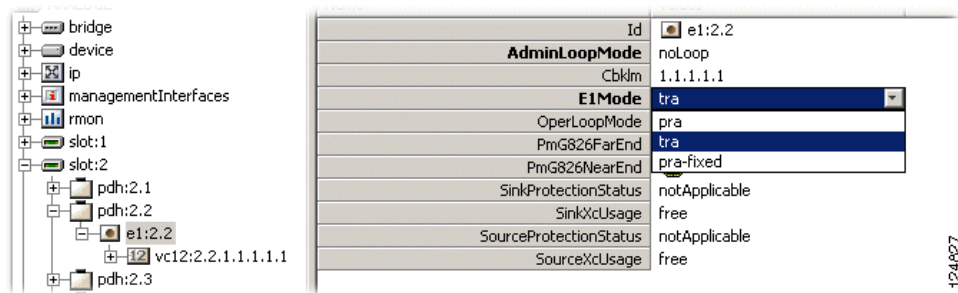
ONS 15302 is equipped with E1 ports.)

5.4.1 Setting the Port Mode for ONS 15305

How to set the port mode for ONS 15305:

-
- Step 1** Select a PDH port, [Figure 5-5](#).
- 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), **pra** (ISDN PRA) or **pra-fixed** (ISDN primary rate access with fixed timing)

Figure 5-5 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.
-

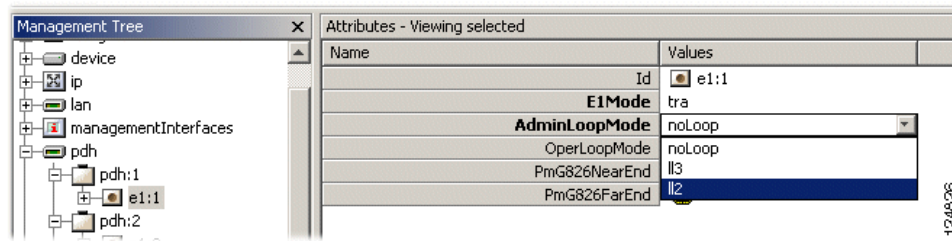
5.4.2 Setting a Loop in an ONS 15305 PDH Port

How to set a loop in an ONS 15305 PDH port

-
- Step 1** Select a PDH port, [Figure 5-6](#).
- Step 2** When the PDH port managed object is expanded, select the **e1** or **e3** managed object.
- Step 3** Set the Admin Loop Mode attribute to **ll2** (loop back to network) or **ll3** (loop back to customer).

5.4.3 Setting a Loop in an ONS 15302 PDH port

Figure 5-6 Set Admin 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 PDH port AdminStatus is set to disabled.

5.4.3 Setting a Loop in an ONS 15302 PDH port

How to set a loop in an ONS 15302 PDH port

- Step 1** Select desired PDH port.
- Step 2** When the PDH port managed object is expanded, select the **e1** managed object.
- Step 3** Set the **AdminLoopMode** attribute to **ll2** (loop back to network) or **ll3** (loop back to customer).
- Step 4** Click **Save** on the toolbar.

5.4.4 Releasing a Loop in a PDH Port

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 **AdminLoopMode** attribute to **noLoop**.
- Step 4** Click **Save** on the toolbar.

**Note**

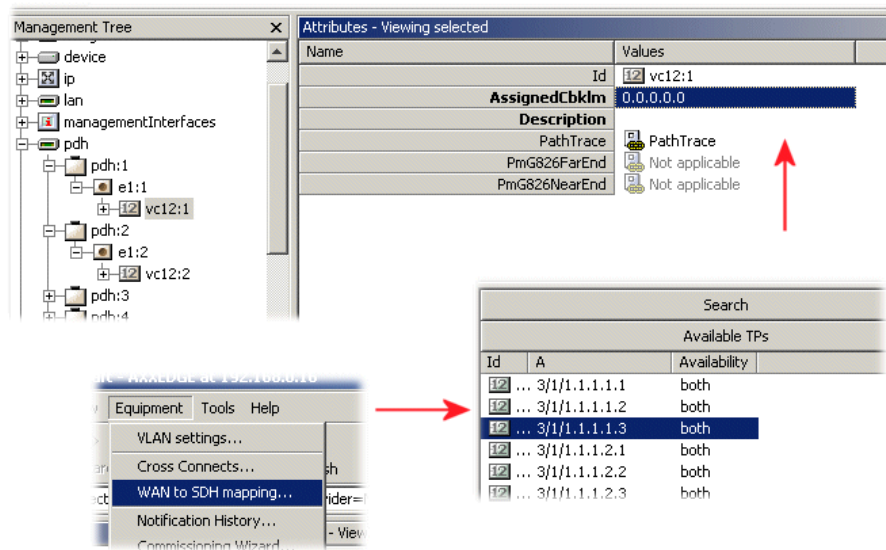
Alternatively, any loop will be released if PDH port **AdminStatus** is set from enabled to disabled.

5.4.5 Assign VC12s in ONS 15302

Assign VC12s in ONS 15302:

- Step 1** Expand desired PDH port in the management tree, to view VC12 managed object attributes, [Figure 5-7](#).
- Step 2** Set **AssignedCbklm** to desired value, [Figure 5-7](#).
- You can use the WAN to SDH mapping window to view available VC12s with cbklm values.
- Step 3** Click **Save**.

Figure 5-7 Assign VC 12 Port



124857

5.4.6 Setting and Reading Path Trace Identifiers

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 **PathTrace**.

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.



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.

5.4.7 Monitoring PDH Port VC-n Performance

Monitor PDH port VC-n 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 the **PMG826** link for PmG826NearEnd to read near end PM data or PmG826FarEnd to read far end PM data.

Step 5 The following attributes are available:

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

Step 6 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, [Figure 5-8](#) and [Figure 5-9](#).

Step 7 The following attributes are available

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

Figure 5-8 Select Interval24Hour

Attributes - Viewing selected

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	Interval15Min
Interval24Hour	Interval24Hour

Figure 5-9 Set Interval24Hour Attributes

Attributes - Viewing selected

Name	Values
Id	interval24Hour.pmG826NearEnd.vc12:1.3.1.1.1.1
BBE	0
ES	0
EndTime	2002/12/02 00:00:00
SES	0
Status	valid
UAS	0

5.4.8 Monitoring PDH E1 Port Performance

The E1 counters are based on CRC-4 counters for near end and E-bit counters for far end monitoring.

Defect criteria for near end is LOS-TX(Loss Of Signal), LOF-TX(Loss Of Frame) and module/slot alarms. For far end there are no alarms present to indicate any defects.

The valid flag for previous intervals and past 24 hours is set only when the port has been in PRA-mode during the whole period. For ports in TRA-mode, the PM counters can only be used to indicate SES/UAS due to LOS-TX or module/slot alarms.

-
- Step 1** Select a PDH E1 port.
- Step 2** When the PDH port managed object is expanded, select the **e1** managed object.
- Step 3** Click on the **PMG826** link for PmG826NearEnd to read near end PM data or PmG826FarEnd to read far end PM data.
- Step 4** 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 on **Interval15Min**, or click on **Interval24Hour** to see the previous 24 hour counter.

- Step 6** The following attributes are available
- Interval15Min ES, SES, BBE and UAS
 - Interval24Hour ES, SES, BBE and UAS

5.4.9 Enabling 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.

5.4.10 Cross-connect the ONS 15305 PDH Port to another Port

See the [“5.6 ONS 15305 SDH Cross-Connection Management” section on page 5-16](#).

5.5 LAN Ports

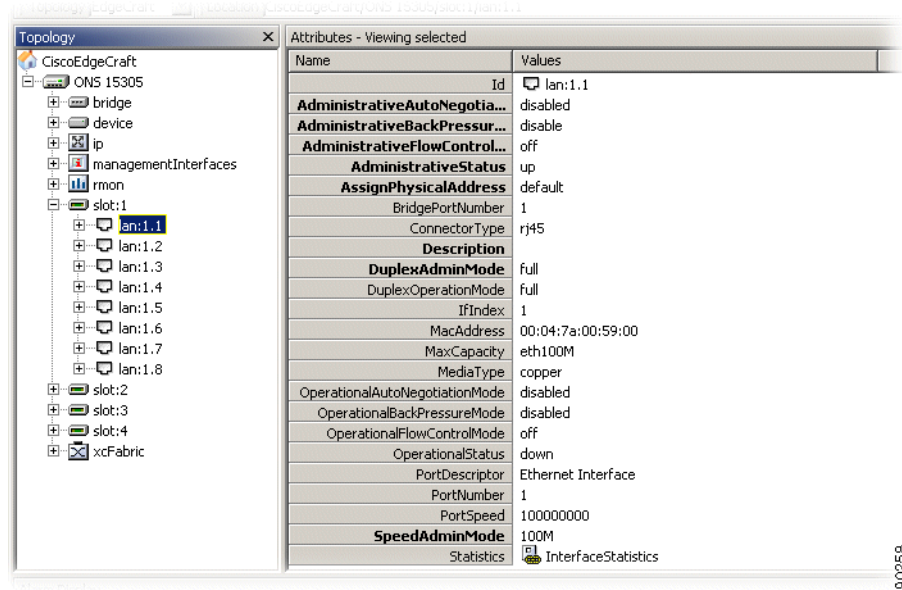
About port attributes and their modification options.

5.5.1 ONS 15305 - LAN Port Attributes

An ONS 15305 slot can for example be configured to carry an E100-WAN-8 module, see [“4.11 Manage Slots on ONS 15305” section on page 4-85](#) for details.

- Step 1** When the module is installed in the desired slot, click desired LAN port to view modifiable attributes, [Figure 5-10](#).
- Step 2** Attributes marked as bold are modifiable.

Figure 5-10 LAN Port Attributes



These Attributes are modifiable:

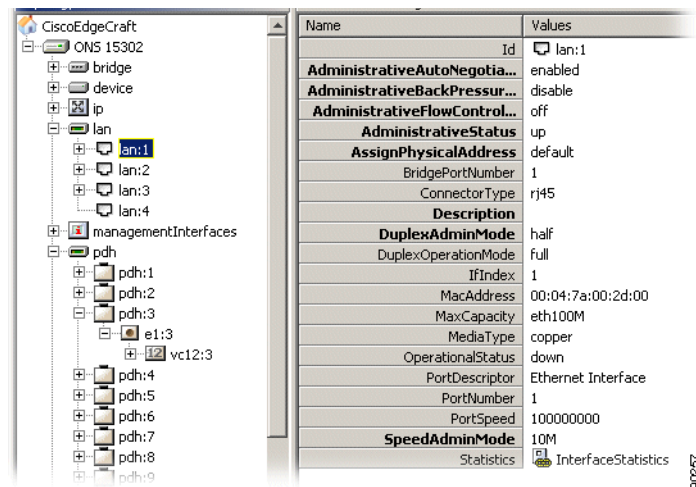
- AdminAutoNegotiationMode
disabled or enabled
- AdminBackPressureMode
disabled or enabled
- AdminFlowControlMode
on, off or auto negotiation
- AdminStatus
up, down or testing
- AssignPhysicalAddress
reserve or default
- Description
string
- DuplexAdminMode
none, half or full
- SpeedAdmin mode
not set, 10M, 100M or 1000M

Step 3 Click **Save** if attribute modifications are performed.

5.5.2 ONS 15302 LAN Port Attributes

The ONS 15302 is equipped with 4 LAN ports, [Figure 5-11](#). For configuration of LAN ports see [“5.5.1 ONS 15305 - LAN Port Attributes”](#) section on page 5-14.

Figure 5-11 LAN Port Attributes - ONS 15302



5.6 ONS 15305 SDH Cross-Connection Management

The purpose of this section is to describe the tasks involved when managing cross connections between termination points on the network element.

The section involves management of the complete life cycle of a cross connection, including creation, presentation, modification, deletion and manual operation of the sub-network connection protection 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.

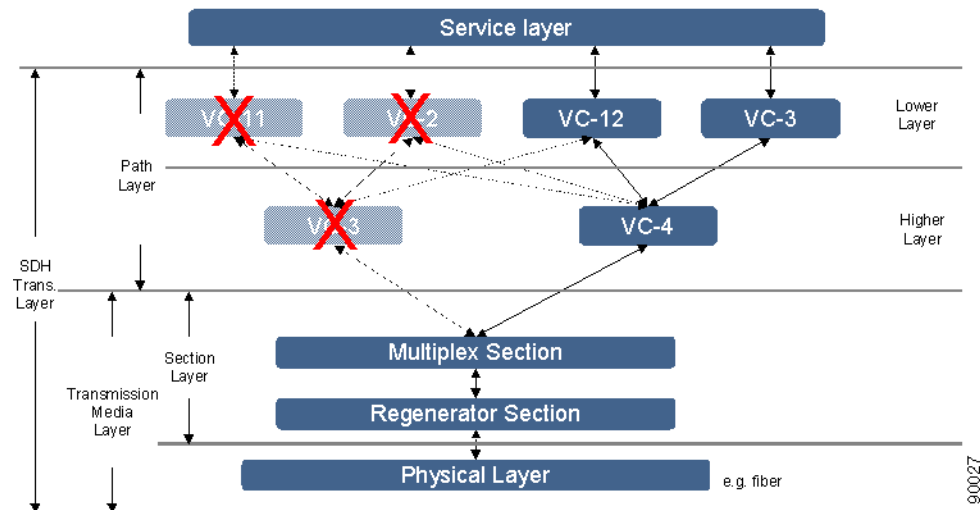
The protection scheme supported by the first release of ONS 15305 is SNC/I, (inherent monitoring). ONS 15305 Release. 2.0 supports Non-intrusive monitoring SNC/N

The first part of this section gives a short introduction to SDH layers and cross connections which is meant to help the reader in understanding the requirements specified in this document. For further reading on SDH and cross connections, please see ITU-T Recommendations G-Series.

5.6.1 SDH Layer Network and Cross Connections

An SDH network has layered structure as depicted in Figure 5-12. 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 are performed. The path layer works on containers.

Figure 5-12 SDH Layer Network



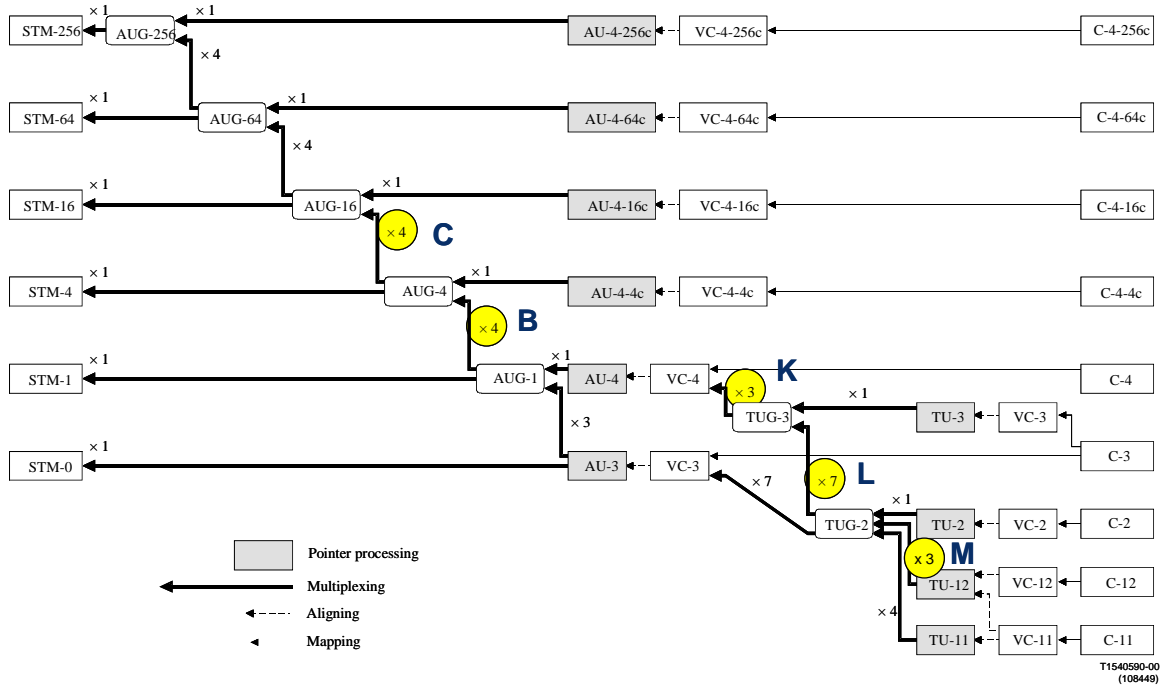
The ONS 15305 network element has support for VC-4 in the higher order layer and in the lower order layer VC-12 and VC-3.

5.6.1.1 SDH Port Structuring

The multiplexing structure of the SDH ports determine which layers and their termination points that are available to be cross connected. The multiplexing structure for SDH in all layers are shown in Figure 5-13 (taken from ITU-T Recommendation G.707.) The C.B.K.L.M value determines the path through the structure. The usage of the C.B.K.L.M value follows the rules defined in Table 5-1.

Only traffic on non-terminated containers called connection termination points can be cross connected, that means 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 5-13 SDH Multiplexing Structure



The original illustration used in Figure 5-13, is found in ITU-T G.707/Y1322 (10/2000).

C.B.K.L.M Value Usage

Table 5-1 C.B.K.L.M Value Usage

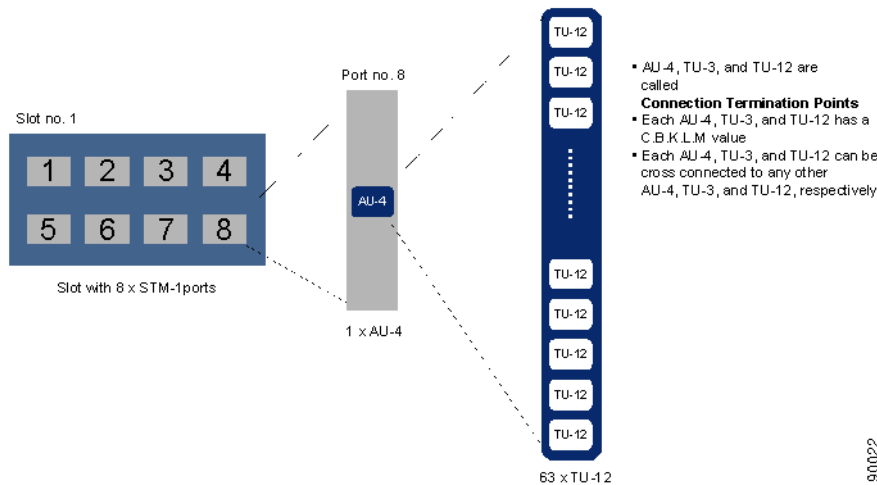
Rules	Examples
When referring to SDH objects the complete C.B.K.L.M value is used even if some fields are in-significant.	
Not significant fields in C.B.K.L.M are set to 0.	AU-4 in STM-16: C.B.0.0.0 TU-3 in STM-16: C.B.K.0.0

Table 5-1 C.B.K.L.M 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 one 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 C.B.K.L.M 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 release 1) 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.	

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, or between TU-3s, between VC-12 and TU-12, or between two VC-12s.

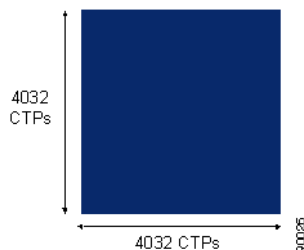
Figure 5-14 Slot - Port - CTP Relations

In ONS 15305 there are 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.

5.6.1.2 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 5-14. 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 ONS 15305 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 ONS 15305 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 4032×4032 .

Figure 5-15 Largest Possible Cross Connect Matrix

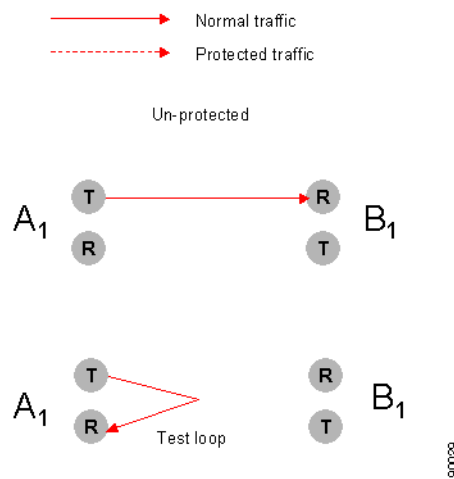
This is a very large number of choices and impossible for a user to keep track of.

In addition there are several different types of cross connections:

- Point-to-point
- WAN XCs (special type of point-to-point, see the “5.15.1.1 WAN Ports and the Mapping” section on page 5-53).
- Drop and continue (not in R1).
- Broadcast (not in R1)

All of these types can be with or without protection and uni-directional or bidirectional, [Figure 5-16](#) to [Figure 5-21](#).

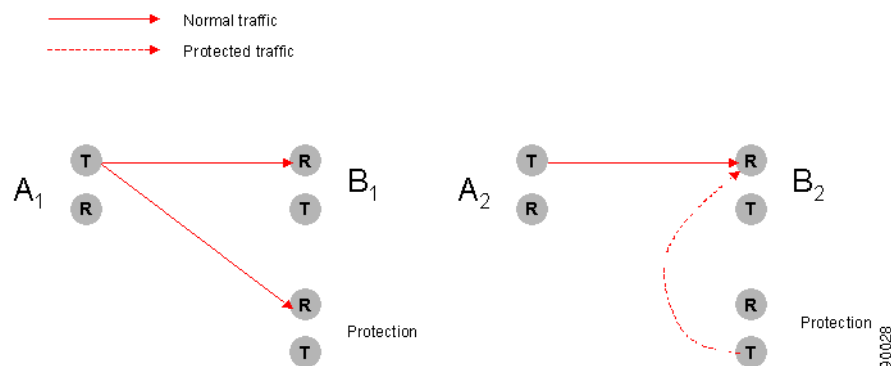
Figure 5-16 Unidirectional XC, Unprotected



Unprotected, unidirectional cross connects can be used for test loops, as illustrated in [Figure 5-16](#).

In [Figure 5-17](#) 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 5-17 Uni-directional XC, Protected



The bidirectional, unprotected cross connection is depicted in Figure 5-18. For bidirectional cross-connections all termination points have switching possibilities when protected. In Figure 5-19 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 5-18 Bidirectional XC, Unprotected

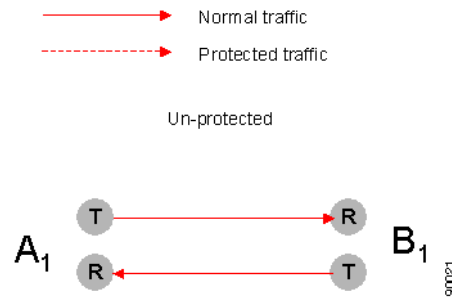


Figure 5-19 Bidirectional, Protected

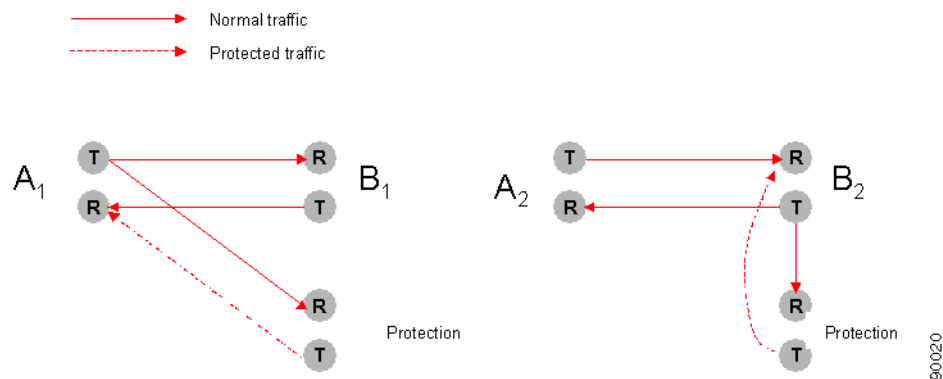


Figure 5-20 Example of Bidirectional, Unprotected, Point-to-point XC

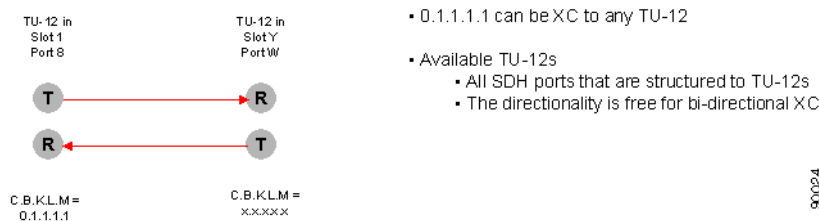
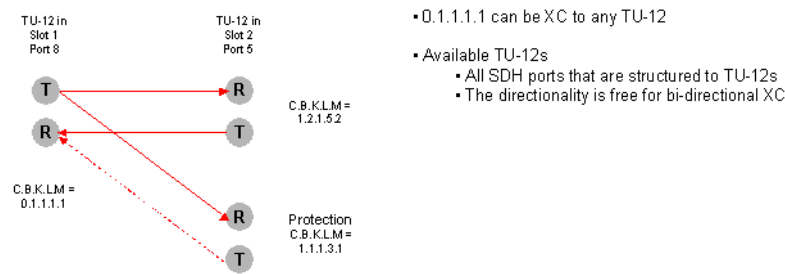
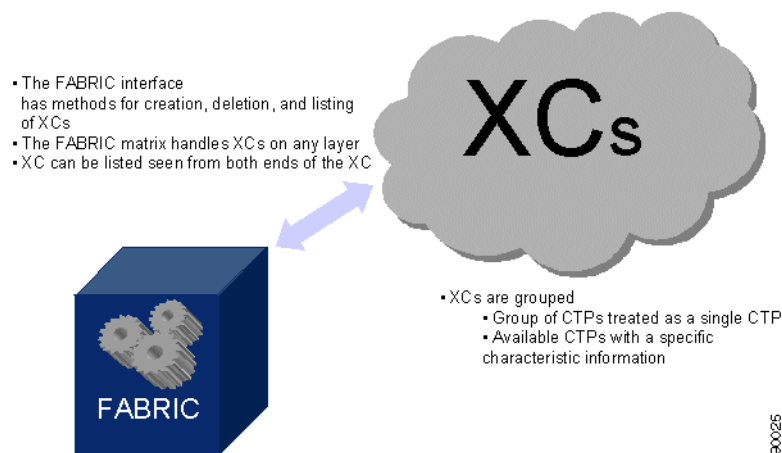


Figure 5-21 Example of Bidirectional, Protected, Point-to-point XC

Examples of an unprotected, bidirectional, point-to-point cross connect and a protected, bidirectional, point-to-point cross connect are given in [Figure 5-20](#) and [Figure 5-21](#), respectively.

5.6.1.3 XC Fabric

The connection management is taken care of by a Fabric as depicted in [Figure 5-22](#). 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 of XCs, for example, all XCs with the same characteristic information, 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 that is used in a 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 5-22 XC Fabric

5.6.2 Open the Cross Connection GUI

You have two possible choices for opening of 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 5-23](#).

5.6.2 Open the Cross Connection GUI

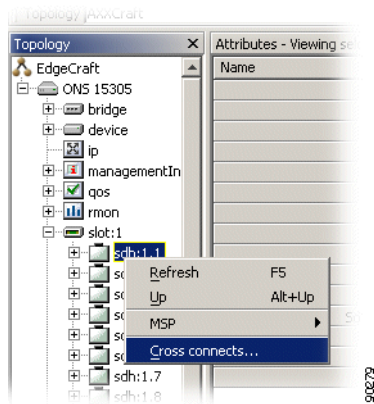
Figure 5-23 Select Cross Connect



or;

Step 2 Click on an SDH port, [Figure 5-24](#)

Figure 5-24 Select SDH Port Cross Connect



The system presents the cross-connection GUI with the relevant data from the selected managed object in the management tree.

The cross-connection GUI allows you to filter the selection based on predefined set of queries.

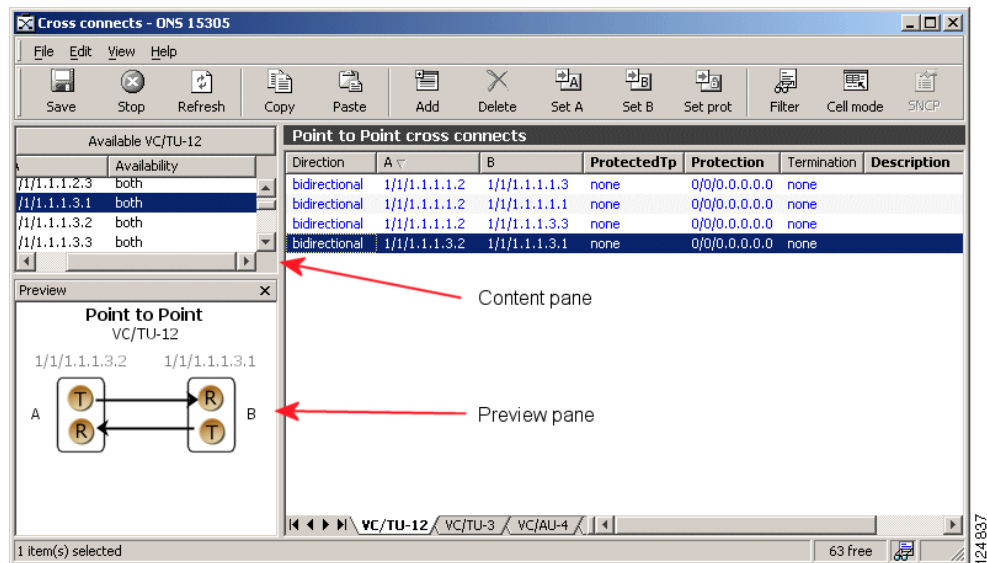
5.6.2.1 Cancelling a query

Queries in progress can be cancelled by selecting the Stop operation from the tool bar or the menu.

5.6.2.2 Cross-connection GUI - Overview

[Figure 5-18](#) displays the cross-connection screen.

Figure 5-25 Cross-connection GUI - Overview



5.6.3 Browsing Existing Cross-connections

Cross connections can be browsed in the cross connect window in the following manner:

5.6.3.1 Browsing all Cross-connections

To browse all:

Step 1 Open the cross-connects window from the equipment menu.

Step 2 A list of all cross-connections is shown.



Note

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.

5.6.3.2 Browsing Cross-connections of a Port

Browse a port:

Step 1 Select a port.

Step 2 Right click on the port and select cross-connections.

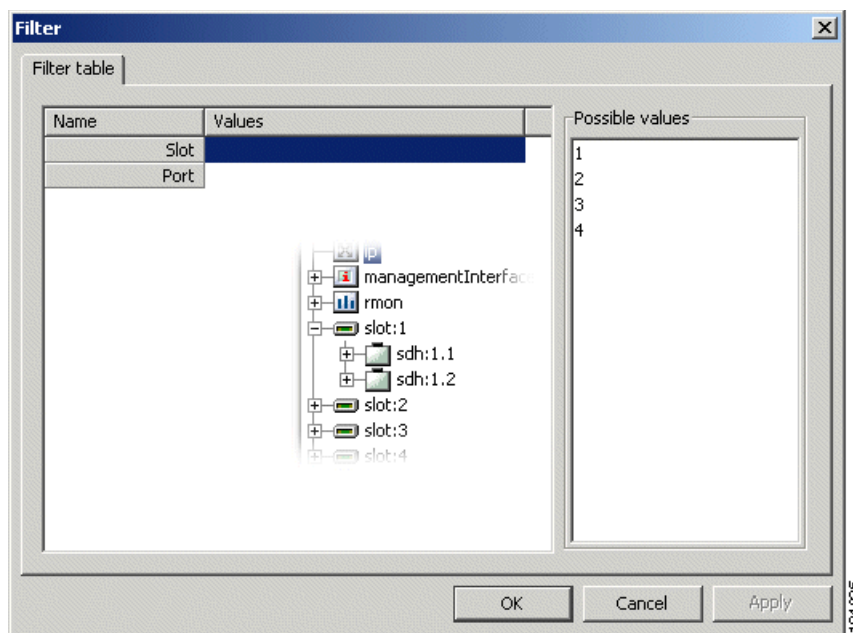
A list of all cross-connections to and from the port is shown.

5.6.3.3 Filtering the Content of the Cross-connection List

To filter the content of the cross connection list, follow these steps:

- 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 5-26](#).
- Step 3** Select the filtering criteria you want for slot and port or combinations of them.

Figure 5-26 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 are included in the filtering criteria.

A filter icon is displayed in the status bar of the window to indicate that the filter is active.

5.6.3.4 Refreshing the Cross-connect Window

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.

- Step 1** Select **Refresh** from the View menu or click the **Refresh button** on the toolbar or press **F5**.

5.6.4 Setting up Cross-connections

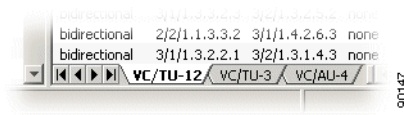
Cross connections can be set up between a number of different ports.

5.6.4.1 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 5-27](#).

Figure 5-27 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, [5.4.1 Setting the Port Mode for ONS 15305, page 5-9](#).



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, [5.3.1 Configuring ONS 15305 SDH Port Structure \(Channelization\), 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, ([5.3.5 Enabling the SDH Port to Carry Traffic and Report Alarms](#), page 5-8 and [5.3.6 ONS 15305 SDH Port Synchronization Quality Output Signaling](#), page 5-8.)

5.6.4.2 From a 45 Mbps E3 (T3) Port to a Timeslot in an SDH Port

Creating 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 5-28](#).

Figure 5-28 Select the VC/TU12 Tab



5.6.4.3 Creating a Pass-through Cross-connection

Creating 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.
-

5.6.5 Modifying Cross Connections

A cross-connection is a relationship between termination points and 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, [5.6.6 Protecting Cross Connections](#), page 5-28.

5.6.6 Protecting Cross Connections

The A-end or B-end of a cross-connection can be protected by the SNC protection scheme when a cross-connection is being set up or after the cross-connection has been set up.

**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, a SNC protection switch is created where the signal from A is working connection and the signal from protection is 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 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 or 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, [5.3.1 Configuring ONS 15305 SDH Port Structure \(Channelization\)](#), 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 protect your a or b-end with.
- Step 7** Click on 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. Proceed until all cross-connections are protected (cross-connections that have the protected TP attribute set to a or b).
- Step 9** Click **Save** on toolbar.

**Note**

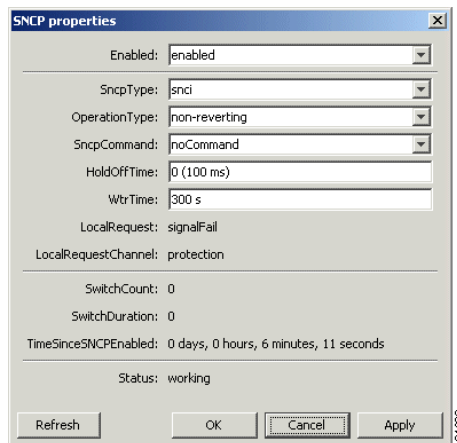
By default the protection is disabled and will not work before it is enabled. Follow instructions below to enable SNC protection SNC protection.

5.6.6.1 SNC Protection

How to set up a Sub network connection 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 5-29](#).
- Step 3** Set the Enabled attribute to enabled and click **OK**.

Figure 5-29 Select Enabled Attributes



- Step 4** Click **Save** on 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 Protected TP back to a or b.

5.6.6.2 Modifying Protection Parameters of a Cross-connection

A-end or B-end of cross-connections are protected as described in the [“5.6.6 Protecting Cross Connections” section on page 5-28](#). The SNC is then set up with a number of default parameters. The parameters can easily be modified.

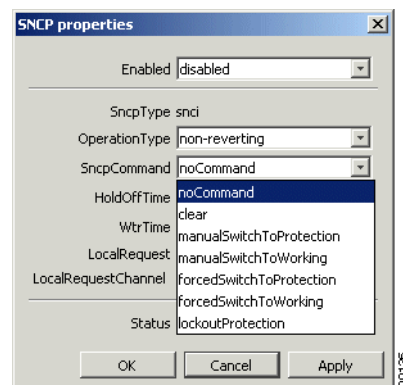
- Step 1** Open the Cross-connects window from the Equipment menu.
- Step 2** Select a cross-connection in the Cross-connect Window.
- Step 3** Select the cross-connections where you want to modify protection parameters (Shift and Ctrl buttons can be used for multiple selection).
- Step 4** Click the **SNCP** button in the toolbar.
- Step 5** Modify the SNC protection parameters and click **OK**.
- Step 6** Click **Save** on toolbar.

5.6.6.3 Commanding Cross-connection Protection Switch

The Cisco Edge Craft user 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 5-30](#).
 - Step 4** Select the SncpCommand and click **OK**.

Figure 5-30 Select SNCP Command



- Step 5** Click **Save** on toolbar.
- Depending on the priority of the command and current status of each channel, a switch can now take place for some or all selected cross-connections.
-

5.6.7 Deleting Cross-connections

A cross connection can be deleted in the following manner:

-
- Step 1** Open the cross-connection GUI by selecting cross-connects from equipment menu.
 - Step 2** Select the panel for the type of cross-connection(s) you want to delete (VC or TU12, VC or TU3 or VC or AU4).
 - Step 3** Select the cross-connections that you want to delete.
 - Step 4** Click **Delete** on the toolbar.
 - Step 5** Click **Save** on toolbar.
-

5.6.8 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.

5.6.8.1 Setting up of Multiple Cross-connections by Multiple Selection

You can set up multiple cross connections this way:

-
- Step 1** Select the Termination points that you want to use as A-ends. Use Shift or Ctrl buttons to select more than one termination point.
 - Step 2** Click **Add** on toolbar. The same number of cross-connections as the selected TPs are created with the A-end filled in.
 - Step 3** Select the TU-12 termination points that you want to add to the B-ends of the cross-connections in the same way.
 - Step 4** Click the **Set B** button on the toolbar.
 - Step 5** If you want to protect the connections, select the TU-12 termination points that you want to add to the cross-connections.
 - Step 6** Click the **Set Prot** button on the toolbar. Remember to set ProtectedTP to a or b.
 - Step 7** Click **Save** 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.

5.6.8.2 Setting up Multiple Cross-connections by Repeated Operations

Another way to set up multiple cross connections is to repeat an operation:

-
- Step 1** Double-click the termination point you want to use as A-end. A new cross-connection is created.
 - Step 2** Double-click the termination point you want to use as B-end. B-end is filled in.
 - Step 3** Repeat [Step 1](#) and [Step 2](#) for as many cross-connections as you want.

Step 4 Click **Save** on toolbar.

5.6.8.3 Entering Termination Points Manually

You can enter termination points manually like this:

Step 1 Add a new cross-connection.

Step 2 Click on 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>

5.7 ONS 15305 SDH Protection Management

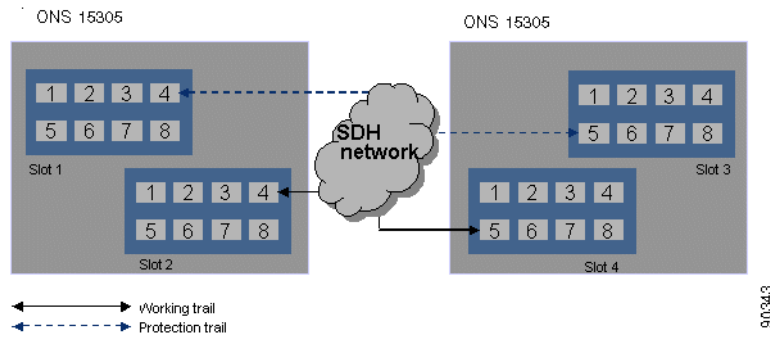
The purpose of this section is to guide the user through management of the 1+1 linear multiplex section Protection (MSP) between two SDH ports.

5.7.1 Introduction

The section involves management of the complete life cycle of an MSP, including creation, presentation, modification, deletion and manual operation the MSP switch.

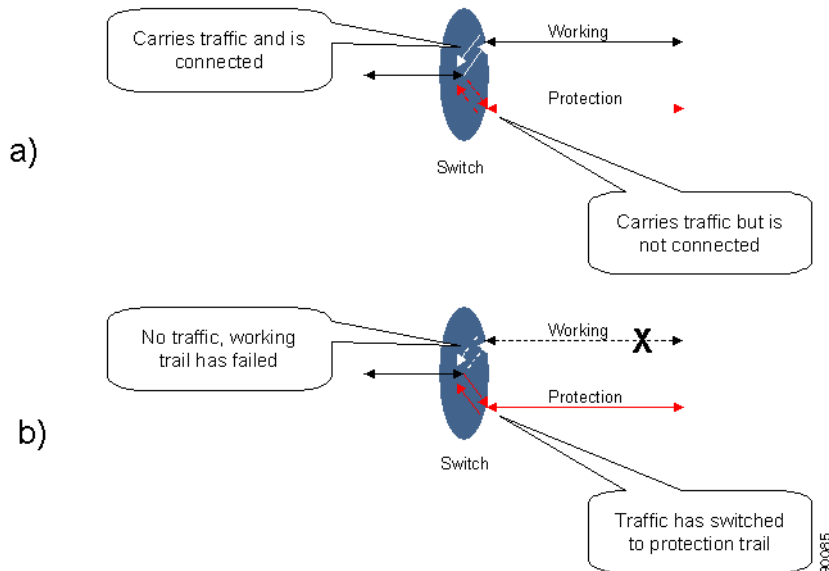
5.7.1.1 Multiplex Section Protection

Figure 5-31 1+1 MSP between two ONS 15305



The 1+1 MSP provides protection of the SDH ports by replacing the supporting trail when it fails as illustrated in Figure 5-31. This is a 100% redundant protection scheme.

Figure 5-32 Protection Switching Scenarios



Both working and protection trails are enabled and the signal is bridged to both, Figure 5-32.

- 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 5-32.

- b. Traffic from working trail is ignored. The network element uses a bidirectional switching protocol, that means, both ends of the trails switches simultaneously. To synchronize this simultaneously 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 a better control of the traffic in the network but uses a little more time to perform the switching than a uni-directional switching protocol does.

The switching has two different modes:

- Revertive traffic returns to the working trail when recovered.
- Non-revertive traffic stays on protection trail indefinitely or until told otherwise.

The time to wait before restoring the trail can be defined.

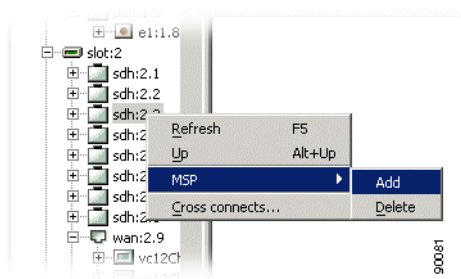
When switching either from or to protection, an event notification will be emitted.

5.7.2 Protect Section by MSP

MSP object for SDH port protection:

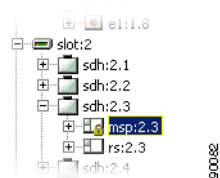
- Step 1** In the management tree right click the SDH port that should be the working port.

Figure 5-33 Select SDH Port



- Step 2** Click **Add** in the pop-up menu. An msp object is created below the port, [Figure 5-33](#).
- Step 3** Select the msp object in the management tree, [Figure 5-34](#).

Figure 5-34 Select MSP Object



- Step 4** Fill in the ProtectionSlot and ProtectionPort attributes, [Figure 5-35](#).

Figure 5-35 Select Protection Port Attributes

Name	Values
Enabled	enabled
Id	
LocalRequest	NA
LocalRequestChannel	NA
Mode	unidirectional
MspCommand	noCommand
OperationType	reverting
ProtectionSlotAndPort	NA
RemoteRequest	NA
RemoteRequestChannel	NA
Status	NA
SwitchCount	0
SwitchDuration	0
TimeSinceMSPEnabled	----
WorkingSlotAndPort	1.2
WtrTime	300

Step 5 The list will only contain ports when the conditions below are fulfilled:

Working and Protection port must be selected from slot 1 and 2 or 3 and 4. Thus it is not possible to set up MSP protection with Working port from slot 1 and Protection port from slot 3. Working and Protection ports can be selected from the same slot.

A Protection port must be unstructured on the highest structurable level:

- ONS 15305 Release 1.1 / 1.0:
 - aug1
- ONS 15305 Release 2.0:
 - aug4 for STM4 and STM16,
 - aug1 for STM1.

See the [“5.3.2 Modifying or Removing ONS 15305 SDH Port Structure”](#) section on page 5-4

The port must not be connected to a remote module.

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.

5.7.3 Modify MSP

How to modify an MSP object:

Step 1 In the management tree 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 toolbar.



Note If the link is operating on the protection section in bidirectional mode, you might brake traffic if you set the 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 to command it to lockout of protection before making the modifications.

5.7.4 Delete MSP

How to delete an MSP object:

- Step 1** In the management tree 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 management tree.
- Step 3** Click **Save** on the toolbar.



Note Be aware that 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).



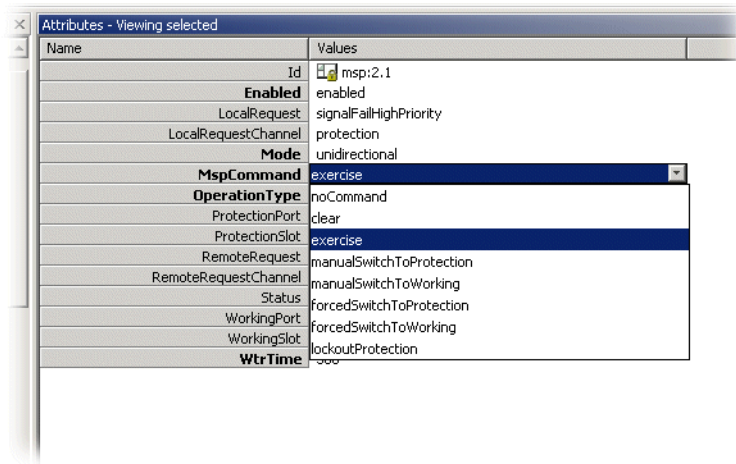
Note To avoid problems always make sure the link is operating on the Working section and to command it to lockout of protection before deleting the MSP.

5.7.5 Command MSP Switch

How to set an MSP switch command:

- Step 1** In the management tree 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 5-36](#).

Figure 5-36 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 might 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 protection command instead of a forced switch to 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.

5.7.6 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 can not, 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.

5.7.7 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 can 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 can 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.

5.7.7.1 Protect Connection by SNCP

See the [“5.6.6.1 SNC Protection”](#) section on page 5-29.

5.7.7.2 Modify SNCP

See the [“5.6.6.2 Modifying Protection Parameters of a Cross-connection”](#) section on page 5-30.

5.7.7.3 Command SNCP Switch

See the [“5.6.6.3 Commanding Cross-connection Protection Switch”](#) section on page 5-31.

5.8 ONS 15302 SDH Protection Management

The ONS 15302 offers 1+1 linear multiplex section protection (MSP).

5.8.1 Multiplex Section Protection

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.

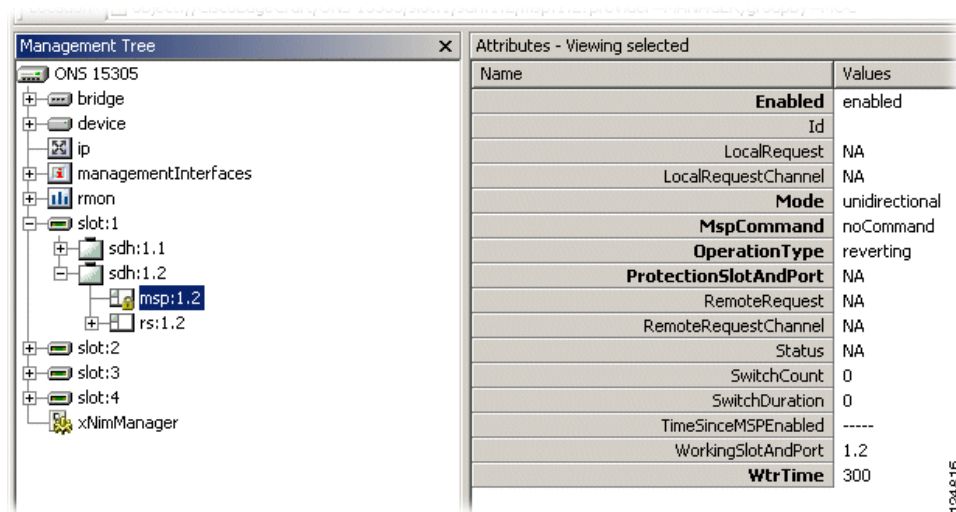
The operation of the protection switch is configurable as described in the [“5.8.1.1 Modify MSP Parameters”](#) section on page 5-39.

5.8.1.1 Modify MSP Parameters

How to modify MSP parameters.

-
- Step 1** Select **SDH1** port (working) and click on the **msp** object, [Figure 5-37](#) and [Figure 5-38](#).

Figure 5-37 Select SDH1/MSP1 Attributes



Modifiable parameters:

- Enabled

Set to enabled or disabled.

- Mode

Set to unidirectional or bidirectional.

- MspCommand

Set one of the following.

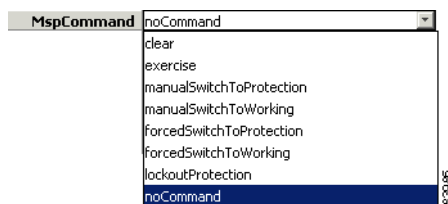
- OperatingType

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 5-38 Set MSP Command



Step 2 Click **Save**.

5.9 Ethernet Standardized Mapping

The Cisco network elements (ONS 15305 2.0 and ONS 15302 2.0) support two different modes of Ethernet over SDH (EOS) mapping:

- Cisco proprietary mapping combined with inverse multiplexing at VC-12 level. See the [“5.15 ONS 15305 Proprietary NxVC-12 EoS Mapping”](#) section on page 5-53 and the [“5.16 ONS 15302 Proprietary NxVC-12 EoS Mapping”](#) section on page 5-67.
- Ethernet over standardized mapping (EOS): GFP-F mapping, combined with Virtual Concatenation (VCAT) at VC-12, VC-3 and VC-4(ONS 15305) level, and Link Capacity Adjustment Scheme (LCAS).

**Note**

See the ONS 15305 2.0 and ONS 15302 2.0 Installation and Operation Guides for Hardware details (modules and network elements).

This section describes EOS. The support of the different EOS modes are module dependent. WAN traffic modules support standardized mapping:

- Octal LAN 10/ 100Base-TX module with standard mapper circuits (E100-WAN-8)
- Dual Optical LAN 1000Base-LX Module with standard mapper circuits (GigE-WAN-2)

Presentation and modification of other WAN port parameters are described in the [“5.3.1 Configuring ONS 15305 SDH Port Structure \(Channelization\)”](#) section on page 5-2.

5.9.1 Introduction

The GFP, VCAT and LCAS standards provide a standardized (non-proprietary) way of allocating bandwidth for packet services through circuit switched networks such as SDH and SONET.

**Note**

SONET is the American National Standards Institute standard for synchronous data transmission on optical media. This is mentioned as SDH in this section.

These standards ensure inter-operability between mixed vendor transport networks, providing the required support for establishing packet (Ethernet) services over a circuit switched transport network. These are much required properties when extending packet switched GFP- Generic Framing Procedure

A main benefit of these standards compared to pure Ethernet/MPLS metro and national wide networks is that all the SDH benefits of network resilience provided by protection schemes (MSP, SNC) are maintained while still providing full Ethernet service interfaces at the endpoints of the transport network.

This also enables owners of existing SDH network infrastructure to adapt their existing networks to the mixed packet- and circuit switched client environments of today.

GFP is a generic format for encapsulating client-side data and control packets in order to enable controlled transport through an SDH network.

**Note**

GFP is an ITU-T standard providing a common reference for inter working between different vendors transport network components, eliminating the need for the proprietary schemes used by today's network element manufacturers (such as Cisco).

GFP is a method used to encapsulate and map packet traffic in a way that is optimal for transport through circuit switched (line switched) networks such as SDH networks. The packaging conserves both client-side data and control information transparently through the switched network.

The packaging process performs the following:

- Adding and removing GFP overhead at the entry/exit points of the transport network, providing administrative information to the SDH network to allow it to transport the packages through the network according to the client side quality requirements.
- Allow better bandwidth utilization through the SDH network when mapping packets to SDH transport channels by transforming client side line character stream coding (Layer 1 coding) to a more bandwidth efficient scheme.
- Providing generic support for transport network services such as VCAT and LCAS
- Adding packet (Ethernet) service information, allowing the SDH network the possibility to differentiate between client side service requirements at the same port (for example point-to-point Ethernet services and multipoint-to-multipoint (LAN) services).
- Providing an end-to-end (near-end to far-end) management channel to be used by the VCAT/LCAS (or other) methods

5.9.2 GFP Alarm and Event Conditions

The following alarm and event conditions apply:

- Client Signal Fail
- GFP Frame Delineation Loss Event
- Payload Type Mismatch
- Client Payload Type Mismatch

5.9.3 GFP Performance Monitoring

The following performance parameters apply:

- Total number GFP frames transmitted and received
- Total number Client management frames transmitted and received
- Number of bad GFP frames received, based upon payload CRC calculation
- Number of HEC uncorrected errors

A degrade alarm is available for the error type PMs, which are:

- Number of bad GFP frames received, based upon payload CRC calculation
- Number of HEC uncorrected errors

The error type PMs are handled in a similar way as the SDH performance parameters. The non error type PMs are handled in the same way as the RMON counters, the non error type PMs are:

- Total number GFP frames transmitted and received
- Total number Client management frames transmitted and received

5.9.4 VCAT - Virtual Concatenation

VCAT provides efficient bandwidth allocation for mapped packet traffic in the SDH network. Bandwidth is provided by assigning a group of SDH VCs to transport the GFP packet belonging to a client interface.

VCAT is a standardized end-to-end method for better bandwidth utilization of the SDH channels by allocating SDH bandwidth in increments in steps corresponding to increments of the SDH specific VC bandwidth ($n \times \text{VC12}$, $n \times \text{VC3}$, $n \times \text{VC4}$ etc.).

This is a non-proprietary method similar to, but exceeding the Cisco proprietary Ethernet port bandwidth allocation by using several VC12's to provide the required bandwidth, as described in the [“5.4.5 Assign VC12s in ONS 15302” section on page 5-11](#).

VCAT allows using VC12's, VC3's, VC4's into VC groups, routing it through selectable AUs/TUs on different ports. Further, it compensates for delays caused by different routes through the network, and assures that end-point traffic is assembled in the same sequence as it was disassembled at the entry-points.

5.9.5 VC Level for VCAT

The VC available VCAT VC levels depends on the Ethernet port:

Fast Ethernet

- VC-12-nv ($n=1,50$)
- VC-3-nv ($n=1,2,3$)
- VC-4-nv ($n=1$) - (ONS 15305)

Gigabit Ethernet (ONS 15305)

- VC-3-nv ($n=1,21$)
- VC-4-nv ($n=1,7$)

The VC- level is individually configurable pr. mapper port. A mix of different VC- levels in one VC Group is not allowed and will result in an error.



Note

The number of available Ethernet ports varies between the different network elements. Mapping type is defined per Ethernet port, and will apply to all VCs in the VC Group assigned to the port.

The mapping is flexible, and can be done to several SDH ports per Ethernet port within the mapping layer:

- VC12 channels to TU12
- VC3 channels to TU3
- VC4 channels to AU4

5.9.6 LCAS- Link Capacity Adjustment Scheme

LCAS provides on-the-fly bandwidth adjustments within a VCAT VC Group by allocating or de-allocating VCs from the VC Group. This is normally done to remove failing VCs from a VCAT VC Group, and provides both failure resilience and rapid restoration of traffic capacity.

VCAT works similar to Cisco proprietary mapping, but has more features, and is ITU-T standardized, allowing for inter operability with other vendors.

LCAS is a feature added to VCAT VC Groups, allowing for dynamic allocation and re-allocation of bandwidth in an operative Ethernet port.

LCAS is a standardized method to adjust the bandwidth of the packet transport channel through the SDH network on the fly. This bandwidth adjustment will typically be caused by the operative status (ok/fail) of the different VCs used in a VCAT Virtual Circuit group.

5.9.7 VCAT and LCAS Alarms and Events

The following alarms are related to the VCAT and LCAS:

Table 5-2 VCAT and LCAS Alarm and Event Conditions

Alarm expression	Description
lom	Vcat, loss of
sqm	Vcat sequence indicator mismatch
loa	Lcas loss of alignment for channels with traffic
loaNoTraf	Lcas loss of alignment channels w/wo traffic
acMstTimeout	Lcas acMst timeout
rsAckTimeout	Lcas RS-ack timeout
eosMultiple	Lcas two or more channels have EOS
eosMissing	Lcas one channel has EOS
sqNonCont	Lcas missing SQ detected in set of channels
sqMultiple	Lcas equal SQ for two or more channels
sqOor	Lcas SQ outside of range
gidErr	Lcas Group Id different for active channels
ctrlOor	Lcas undefined Ctrl-word for one or more channels
lcasCrc	Lcas CRC error detected
nonLcas	Lcas non-Lcas source detected
mnd	Lcas member not deskewable
fopr	Lcas failure of protocol
plcr	Lcas partial loss of capacity receive
tlcr	Lcas total loss of capacity receive
plct	Lcas partial loss of capacity transmit
tlct	Lcas total loss of capacity transmit

5.10 VCAT and LCAS Configuration Modes

The two different operation modes for the VCAT and LCAS functionality are:

- VCAT with LCAS enabled - Mode 1
- VCAT without LCAS enabled - Mode 2

5.10.1 VCAT with LCAS Enabled- Mode 1

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

The connections will however very often be bi-directional, and to reduce the number of configuration steps it is possible to enable the following parameter:

- Symmetric capacity

If symmetric capacity is enabled the VC Group is automatically set up with the same capacity in each direction, but the symmetric capacity consists of two uni-directional connections. With the symmetric mode disabled the capacity of the VC Group will need to be configured separately in each direction.

5.10.2 VCAT Without LCAS Enabled- Mode 2

When VCAT is used without LCAS, there is no mechanism for removing of a faulty VC container in a VCG group. To solve this problem the network element has, in addition to the standard mode, a proprietary mode.

The following configurations are available in mode 2:

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

If bidirectional mode is enabled, the cross connections should not be uni-directional, but bi-directional. In addition RDI signalling is enabled. A faulty container in a VC Group is removed based upon the VC alarm condition or based upon RDI signalling (similar to Cisco proprietary mapping). This will allow a VC Group to continue operation even if the VCG has a failed member. This configuration mode is proprietary.

5.11 Administrative Bandwidth for VCAT

Network elements use the administrative bandwidth as a separate defined parameter, independently of the actual assignment of TPs. The administrative bandwidth is used as a notification in case the actual (operative) bandwidth differs from the administrative bandwidth. In ONS 15302, the administrative bandwidth is implicit when selecting the TPs to be mapped to the Ethernet port.

5.11.1 Bandwidth for uni-directional VCAT

The administrative bandwidth can be:

- Symmetrical
Same bandwidth downstream and upstream.
- Asymmetrical
Different defined bandwidths for the two directions.

In uni- directional VCAT, the upstream (traffic flow towards the SDH ports) and downstream (traffic flow towards the Ethernet port) is routed in separate, uni-directional VC Groups. An ethernet port is a LAN port with Layer 1 or WAN port, expressed with character 'x' in GUI.

The bandwidth is provided by mapping STM-n port(s) as termination points to the Ethernet port. The TPs will carry VCs in a VC Group assigned to the Ethernet port.

**Note**

The configuration is manually set for both directions.

5.11.1.1 Bandwidth for Bi-directional VCAT

The administrative bandwidth for bi-directional VCAT (Equivalent to Cisco proprietary mapping) is identical for both directions (transmit and receive), as the same TUs and AU's are used to provide the bandwidth.

**Note**

The bandwidth must also be implemented through cross-connecting the Ethernet port channels (ONS 15305) to the designated AU's or TUs.

Bi-directional VCAT is a Cisco proprietary version of VCAT. It has symmetric capacity, and LCAS is not allowed.

To circumvent transmission failures due to the loss of VCs in a VC Group, RDI signaling is enabled, allowing the network element to automatically detect and remove faulty VCs in the VC Group. Failures will be indicated by error notifications and the reduction of the displayed operative capacity.

5.12 Circuit Protection for VCAT

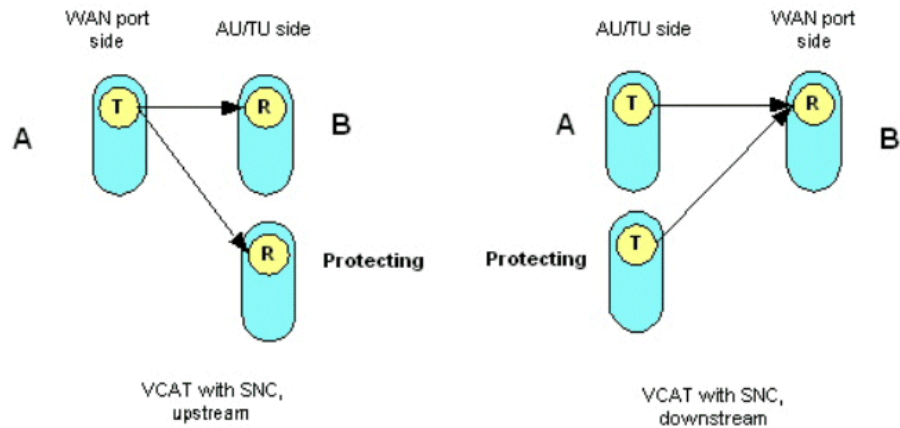
If the network element contains an SDH cross connect, SNC/N or SNC/I is allowed when supported by the network element.

See the [“5.15.5 Protecting a WAN Port”](#) section on page 5-61 and the [“5.6.6 Protecting Cross Connections”](#) section on page 5-28.

5.12.1 Circuit Protection For Uni-directional Modes For ONS 15305

You define circuit protection when cross connecting Ethernet port channels to the SDH ports. Since the VCs are unidirectional, the VC termination can be both A-side (transmit) and B-side (receive), as illustrated in the figure below:

Figure 5-39 VCAT with SNC- Illustration



See the [“5.6.6 Protecting Cross Connections”](#) section on page 5-28.

131072

5.12.2 Circuit proTectIon For Symmetrical VCAT

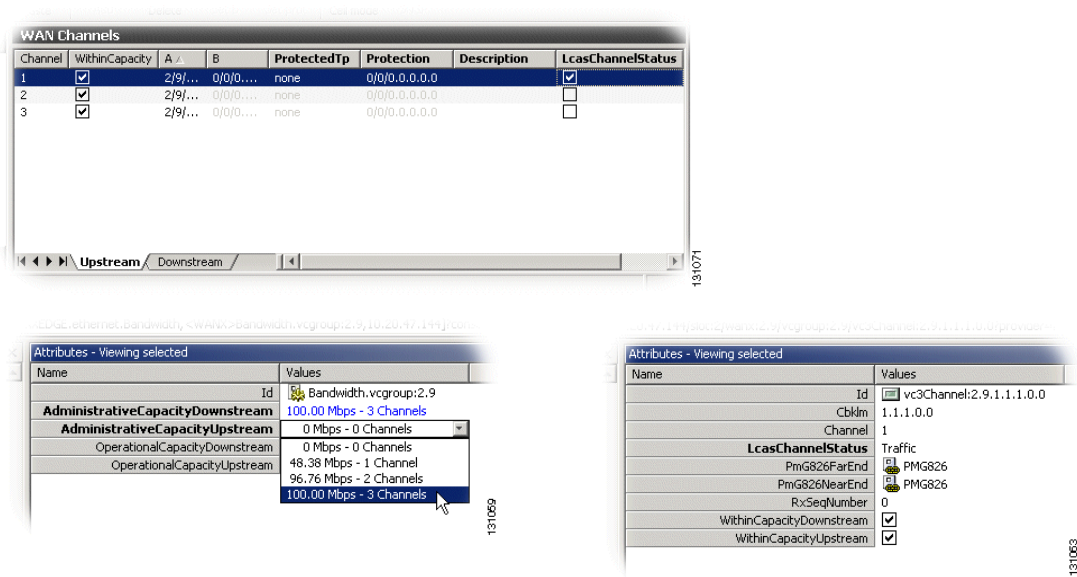
Circuit protection is the same for symmetrical VCAT and Cisco proprietary mapping modes.

5.13 Establish a standardized Mapping With CEC

You establish, modify and delete an Ethernet mapping at the endpoints of a Ethernet path through the network.

You can perform the standardized mapping in the Management Tree or in the WAN mapping GUI. Each mapping operation on an attribute in Management Tree results in a corresponding update of the associated network element attribute(s) in the WAN mapping GUI, see Figure 5-40.

Figure 5-40 standardized mapping- GUI overviews



5.13.0.1 Before You Start

- The STM-n port(s) are structured to the required level (TU12, TU3, AU4). See the [“5.6 ONS 15305 SDH Cross-Connection Management”](#) section on page 5-16.
- The slot(s) expects an Ethernet port with a mapper module.

The following procedures exemplifies standardized mapping types:

- [5.13.0.2 Uni- directional VCAT with LCAS](#), page 5-48
- [5.14 Bi-directional VCAT Without LCAS](#), page 5-52 (Remains - GHE)



Note

The activities in the examples can be parallel, and the order is less significant.

5.13.0.2 Uni- directional VCAT with LCAS

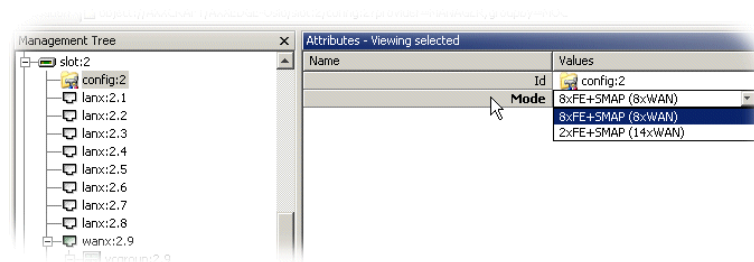
You have selected the Ethernet mapping to be symmetrical uni- directional VCAT VC- level 3 with LCAS. ONS 15305 with Mapper module E100-WAN-8 as the Ethernet port (here: WANx) is used as an example.



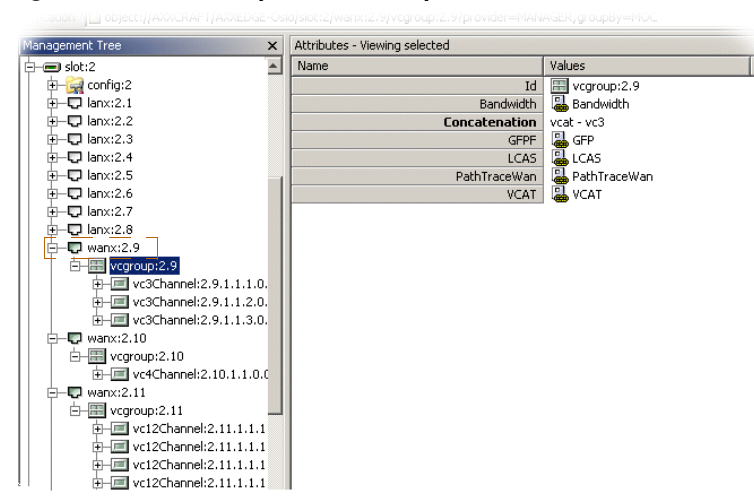
Note

This procedure is generic, and the example can easily be used for Uni- directional without LCAS by disabling the LCAS attribute(s).

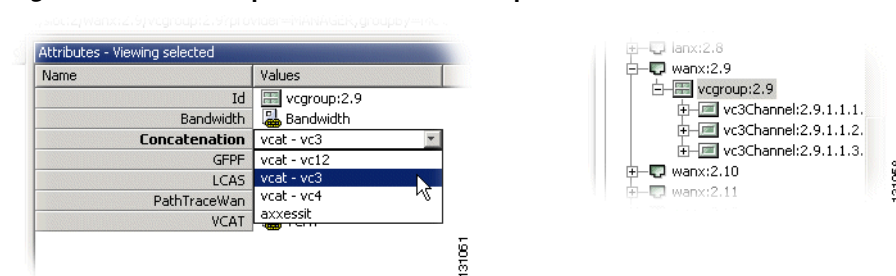
Step 1 Select configuration **Mode** to expected Ethernet port.

Figure 5-41 Slot configuration- ONS 15305 example

Step 2 Select the **VC Group** from desired Ethernet port (here: WANx)

Figure 5-42 Ethernet port - VC Group view

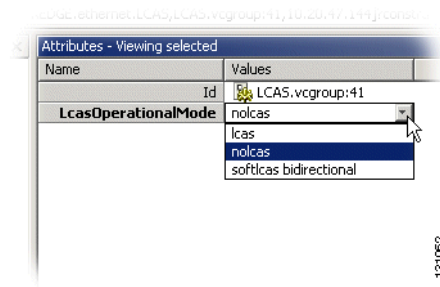
Step 3 Select **VC level** from **Concatenation**.
The appropriate structuring level is set to VCAT enabled port.

Figure 5-43 VC Group concatenation- Example VC level

Step 4 Press **LCAS** from VC Group and select **LCAS** as LCAS Operational mode.
LCAS is enabled for the VCAT enabled port, independent direction.

5.13 Establish a standardized Mapping With CEC

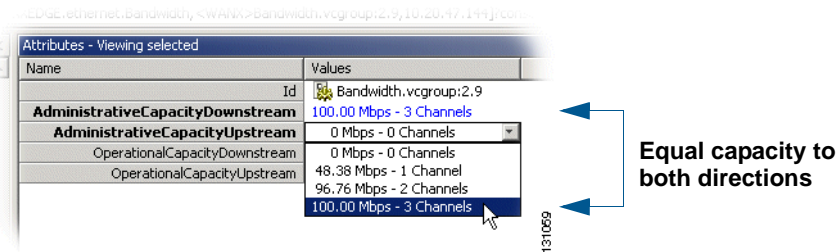
Figure 5-44 Enable LCAS



Step 5 Select **VC Group** and press **Bandwidth**.

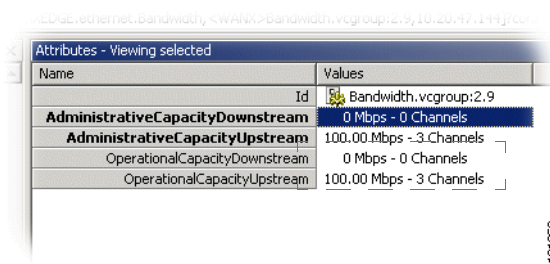
Step 6 Set the same **Administrative Capacity** for downstream and upstream.

Figure 5-45 Administrative Capacity- Symmetrical Uni- directional VCAT



Step 7 View **Operational capacity** (optional verification.)

Figure 5-46 Operational Capacity- example asymmetrical capacity



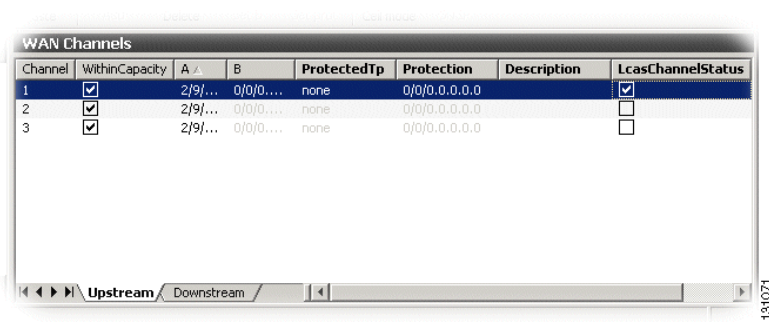
Step 8 Save the Ethernet port configuration to the network element.

Step 9 Open **WAN- to- SDH mapping** GUI.

Step 10 Browse **Ethernet port** from Search bar.

Step 11 Check **LCAS Channel Status** for VC channels (here: WAN).

Figure 5-47 WAN- to- SDH Mapping- LCAS Traffic Status



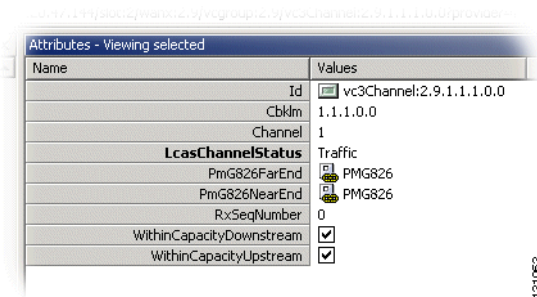
Channel	WithinCapacity	A	B	ProtectedTp	Protection	Description	LcasChannelStatus
1	<input checked="" type="checkbox"/>	2/9/...	0/0/0....	none	0/0/0.0.0.0.0		<input checked="" type="checkbox"/>
2	<input checked="" type="checkbox"/>	2/9/...	0/0/0....	none	0/0/0.0.0.0.0		<input type="checkbox"/>
3	<input checked="" type="checkbox"/>	2/9/...	0/0/0....	none	0/0/0.0.0.0.0		<input type="checkbox"/>

Upstream Downstream

Alternative procedure:

Select one **VC channel** from VC group in Management Tree and choose Traffic as **LCAS Channel Status**. Repeat the operation for all VCs.

Figure 5-48 LCAS traffic set for one VC Channel



Name	Values
Id	vc3Channel:2.9.1.1.1.0.0
Cbklm	1.1.1.0.0
Channel	1
LcasChannelStatus	Traffic
PmG826FarEnd	PMG826
PmG826NearEnd	PMG826
RxSeqNumber	0
WithinCapacityDownstream	<input checked="" type="checkbox"/>
WithinCapacityUpstream	<input checked="" type="checkbox"/>

Step 12 Select one direction (upstream/ downstream) pane.

Step 13 Replace Search bar with **Available TPs** pane.
A list of available VC termination points is presented.



Note If the list is empty, you should see “BeFore You Start” on page -48 or/ and [5.3.1.1 SDH Structuring Wizard, page 5-2](#).

Step 14 Select the **desired TPs**, see the “[5.15.11 Advanced WAN Port Operations](#)” section on page 5-66.
The bandwidth is provided for distribution of the Ethernet port traffic through the STM port.



Note Repeat the mapping steps for **traffic distribution in both directions** in accordance to the chosen symmetrical uni- directional VCAT mode.

Step 15 Define VC cross connection point for circuit protection.

For procedure and scheme (SNC/I, SNC/N), see the “[5.15.5 Protecting a WAN Port](#)” section on page 5-61 and the “[5.6.6 Protecting Cross Connections](#)” section on page 5-28.

5.14 Bi-directional VCAT Without LCAS

With this VCAT configuration mode, each VC is used for traffic in both directions (equivalent to symmetrical uni- directional VCAT).

- Mode (**no LCAS** or **softLCAS bi- directional**)
- Directionality (**bi-directional**)
- The VC-to-TP cross connections is defined to be bi-directional.

Figure 5-49 Lcas Operation Mode

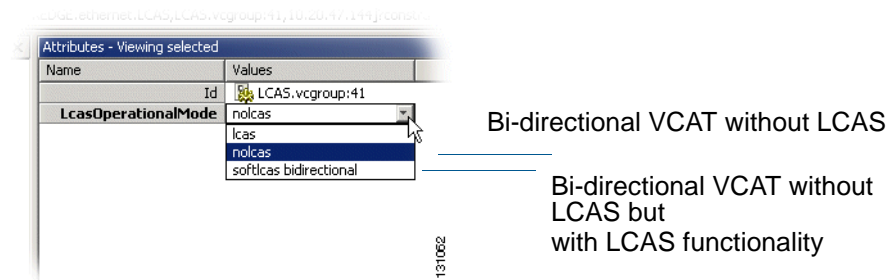
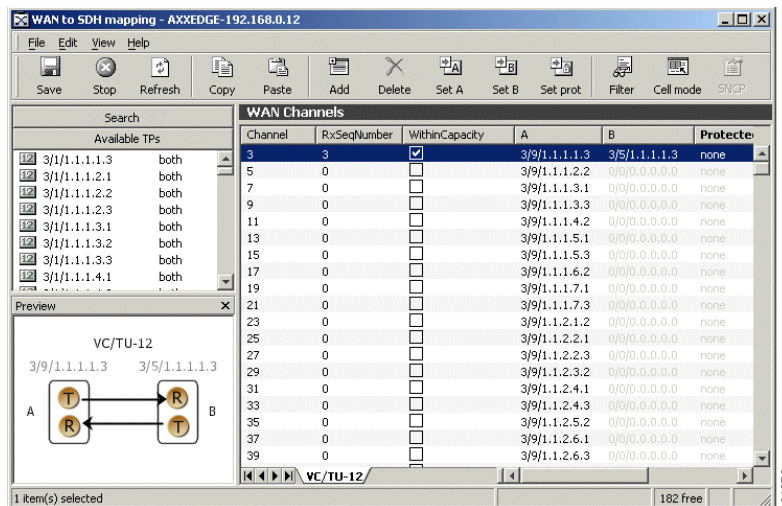


Figure 5-50 Bi- directional VCAT- Example VC- level 12



A WAN port is mapped to the SDH network with the following parameters settings:

- The required bandwidth provided for the WAN port through the SDH network
- The specified mapping mode is established
- Cross connections of WAN port channels to the target SDH Port(s) TPs established with the intended directionality and circuit protection schemes.

5.15 ONS 15305 Proprietary NxVC-12 EoS Mapping

The purpose of this section is to describe the tasks involved in assigning capacity from the SDH server layer to WAN ports with proprietary NxVC-12 EoS Mapping.

5.15.1 Introduction

The total assigned WAN capacity is made up of SDH channels.

One SDH channel is equivalent to a VC-12 (2 Mbps). Mapping to VC-3 and VC-4 is also supported. This section only describes the VC-12/TU-12 layer rate.

ONS 15305 supports Fast Ethernet module; Dual Optical LAN 1000Base-LX Module with Mapper, GigE-WAN-2 and

GigaBit Ethernet module; Octal LAN 10/100Base-TX Module with Mapper, E100-WAN-8.

The table below shows how many VC channels there are on each WAN port on the two modules.

Table 5-3 Mapping to VC-n

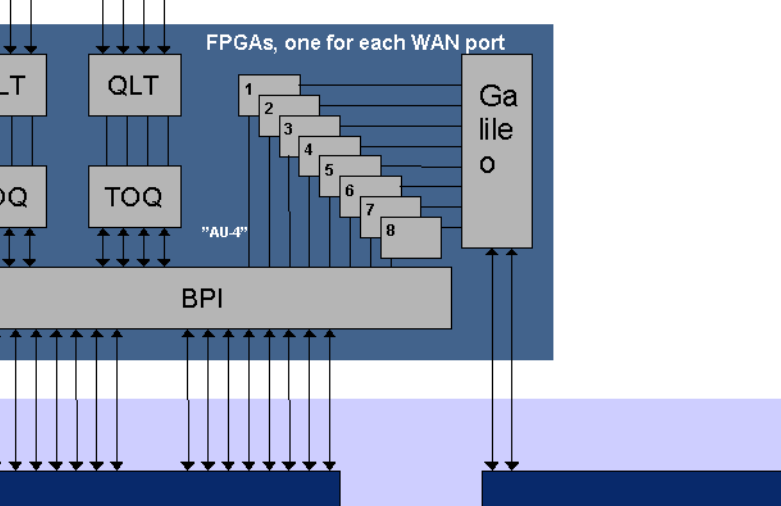
Module	VC-12	VC-3	VC-4
E100-WAN-8	50	3	1
GigE-WAN-2	NA	21	7

The SDH channels can be from different SDH ports.

The WAN channels can be sub-network connection (SNC) protected. ONS 15305 supports the protection schemes SNC/I (inherent monitoring) and SNC/N (Non-Intrusive monitoring).

5.15.1.1 WAN Ports and the Mapping

The eight WAN ports are located on the 8xSTM-1 module. They are connected to a Galileo switch, [Figure 5-51](#). A WAN port has a maximum capacity of 100 Mbps.



A WAN port can be mapped to one STM-1 port, that means there are potentially 63 available VC-12s. Only the 50 first 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 “C.B.K.L.M Value Usage” section on page 5-18.

Diagram illustrating the mapping from WAN ports to channels and then to VC-12s:

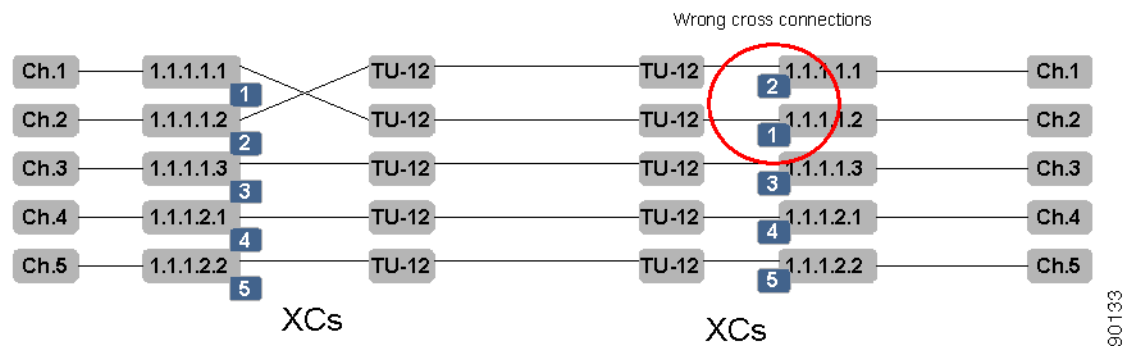
- WAN X** (where X = 1-8) connects to multiple channels.
- Channels:** Ch.1, Ch.2, Ch.49, Ch.50. Each channel represents a capacity of 2.160 Mbit/s.
- VC-12s:** The channels are mapped to VC-12s using a C.B.K.L.M value structure.
 - Ch.1 and Ch.2 map to VC-12s with values 1.1.1.1.1 and 1.1.1.1.2.
 - Ch.49 and Ch.50 map to VC-12s with values 1.1.3.3.1 and 1.1.3.3.2.
- Legend:**
 - Channel:** Each channel represents a capacity of 2.160 Mbit/s.
 - VC-12:** Can be cross connected to TU-12s.
 - C.B.K.L.M Value:** Hardcoded mapping between channel and C.B.K.L.M value.

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

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

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. If the connection is not between two ONS 15305, the sequence number will be zero. A scenario where the cross connection between two TU-12s and two VC-12s in one ONS 15305 is wrong is illustrated in [Figure 5-53](#).

Figure 5-53 Sequence Numbers for Correct Order of TU-12 to VC-12 Cross Connects.



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

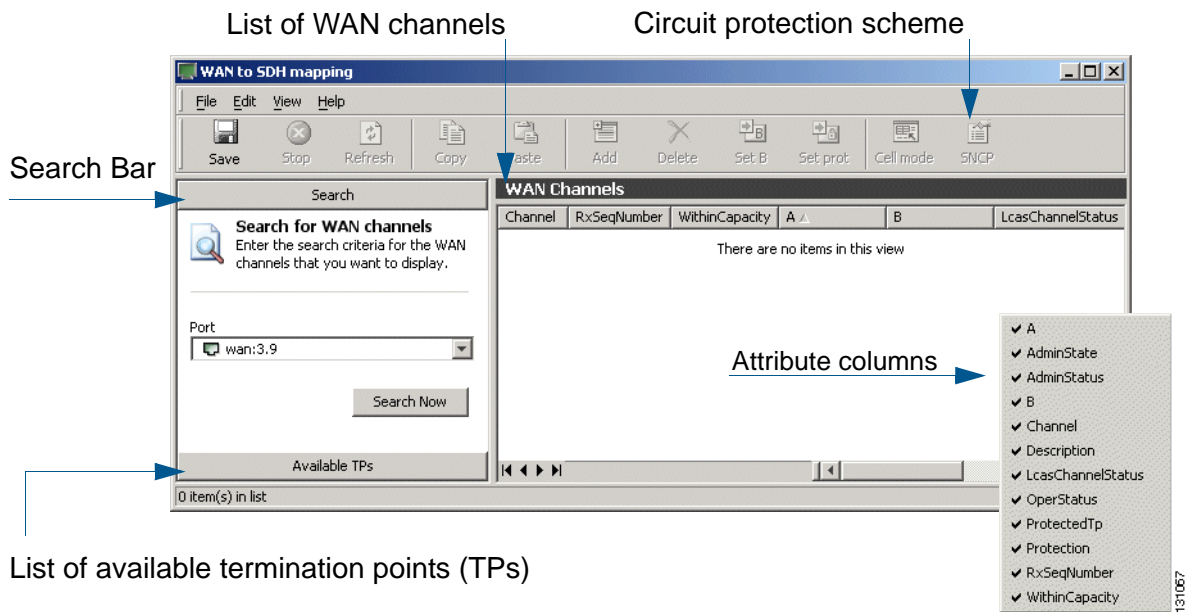
5.15.2 WAN to SDH mapping- Custom GUI

How to search, list and open terminations points for mapping

5.15.2.1 Open WAN to SDH Mapping

- Step 1** Open **WAN to SDH mapping** from Equipment menu.
The list of WAN Channels will be empty.

Figure 5-54 WAN- to- SDH Mapping- GUI Overview



List of available termination points (TPs)

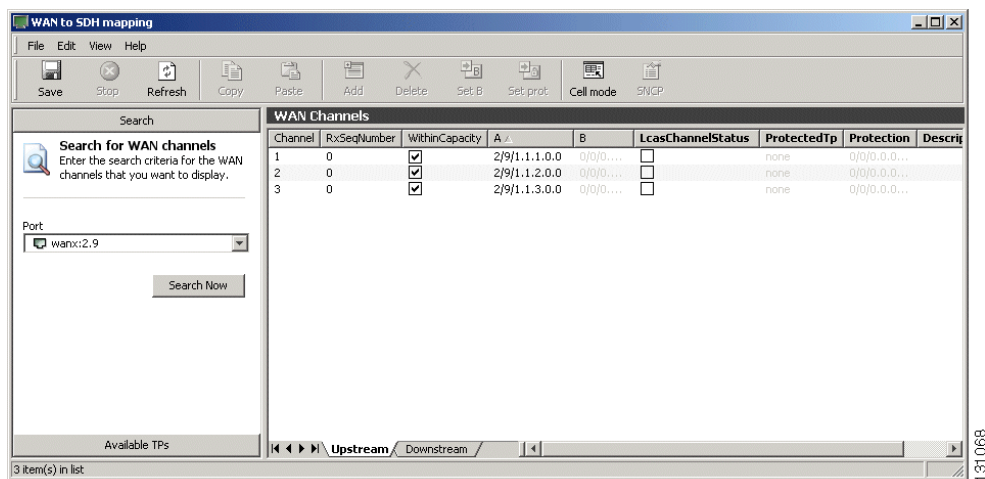
A search bar is available for browsing Ethernet ports.

Step 2 Select the desired **Port**.

Step 3 Press **Search Now**.

The list of WAN Channels will be displayed for the selected Ethernet port.

Figure 5-55 WAN port search- example uni- directional

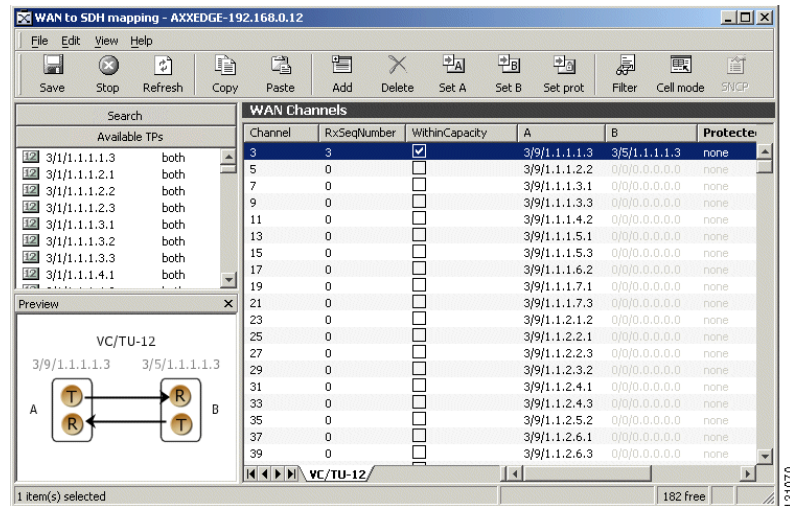


5.15.2.2 List Available Termination Points

Step 4 Click **Available TPs List**.

A list of available STM- n ports is presented in accordance to VC- level.

Figure 5-56 WAN channels list- example VC/ TU 12



5.15.2.3 Cancelling a Query

Queries in progress can be cancelled by selecting the **Stop** operation.

5.15.3 Add Initial WAN Port Capacity

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

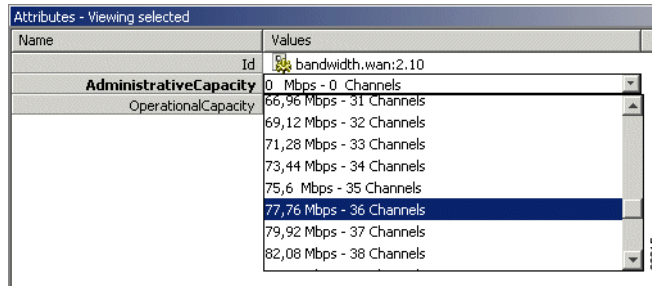
The first step is to set the administrative capacity of the WAN port. This will tell ONS 15305 how many of the 50 possible WAN channels to use for mapping into the SDH server layer.

Step 1 Select a WAN port.

Step 2 When the WAN port managed object is expanded, select **Bandwidth**.

5.15.3 Add Initial WAN Port Capacity

Figure 5-57 Set Bandwidth



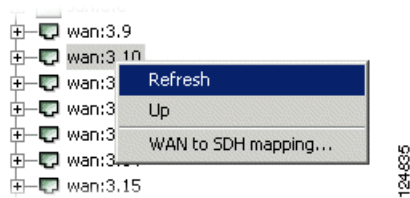
Step 3 Set the Bandwidth to a value between 0 and 100 Mbps, [Figure 5-57](#).

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.

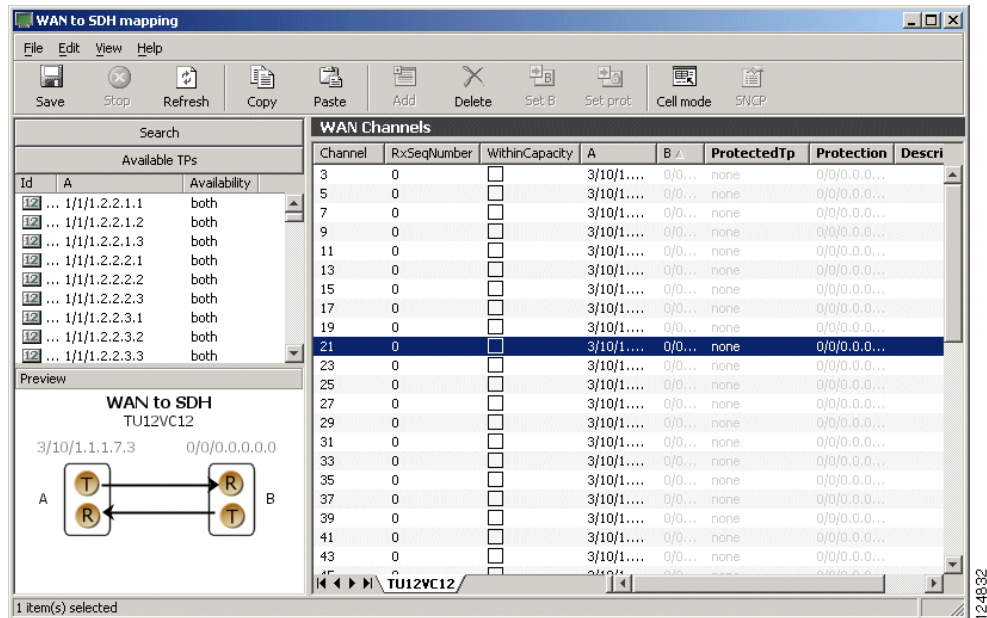
Step 5 Select the WAN port again, right click and select **WAN to SDH mapping**, [Figure 5-58](#).

Figure 5-58 Select WAN Port Attributes



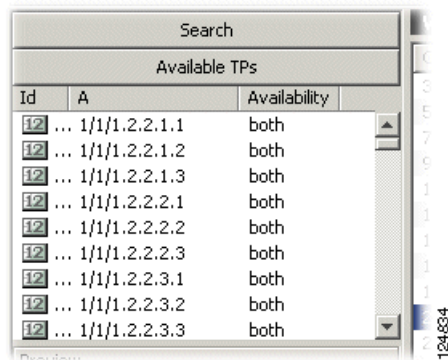
A list of all the WAN channels of the WAN port is shown. The list shows the static relation between each channel number and a VC12 object in the WAN port. The WithinCapacity attribute indicates if the channel is in use by the WAN channel (that means if it was included when setting the administrative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

Figure 5-59 Set WAN Port Attributes



- Step 6** Make sure the Content panel is available in the left part of the window, [Figure 5-59](#). 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 5-60](#).

Figure 5-60 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 [“5.3.1 Configuring 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 your 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 your WAN channel number 2.

Step 10 Continue until all channels that are within capacity has 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 add 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.

5.15.4 Modify WAN Port Capacity

You can modify the WAN port capacity in the same way as you added the initial WAN capacity, [“5.15.3 Add Initial WAN Port Capacity” section on page 5-57](#).

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 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).

Step 6 If you increased the administrative capacity ([5.15.3 Add Initial WAN Port Capacity, page 5-57](#)), more channels have the WithinCapacity attribute set and they need a B termination point to be mapped to the SDH server layer, [5.15.3 Add Initial WAN Port Capacity, page 5-57](#).

Step 7 If you decreased the administrative capacity ([5.15.3 Add Initial WAN Port Capacity, page 5-57](#)), less channels have the WithinCapacity attribute set and the B termination points can be released for other purposes, [5.15.3 Add Initial WAN Port Capacity, page 5-57](#).

5.15.4.1 Increasing 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 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, [5.3.1 Configuring ONS 15305 SDH Port Structure \(Channelization\)](#), 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 has 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 adding cross-connections in intermediate SDH nodes.

5.15.4.2 Decreasing 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 5-61](#).
- Step 2** Click **Delete** on the toolbar. The selected channels become red.

Figure 5-61 Select WAN Channels

WAN port channel 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	0/0/0.0.0.0.0	
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**

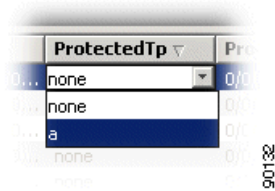
It is not possible to modify the B termination point after it has been saved. If you want to modify the B termination point the channel must first be deleted, and then a new termination point can be added.

5.15.5 Protecting a WAN Port

WAN ports can be protected by the SNC protection scheme in the VC12 or TU12 SDH layer. That means 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 “5.15.3 Add Initial WAN Port Capacity” section on page 5-57.
- Step 2** Set the ProtectedTP attribute to **a** for the WAN channels you want to protect, Figure 5-62.

Figure 5-62 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, 5.3.1 Configuring ONS 15305 SDH Port Structure (Channelization), page 5-2.

- Step 6** Select the TU12 termination point that you want to protect your WAN channel with.
- Step 7** Click on 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. Proceed 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 adding 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 5-63.
- Step 12** Set the Enabled attribute to **enabled** and click **OK**.

Figure 5-63 Set SNCP Properties Enabled

The image shows a dialog box titled "SNCP properties". It contains several configuration fields:

- Enabled:** A dropdown menu set to "enabled".
- SncpType:** A dropdown menu set to "sncl".
- OperationType:** A dropdown menu set to "non-reverting".
- SncpCommand:** A dropdown menu set to "noCommand".
- HoldOffTime:** A text field containing "0 (100 ms)".
- WtrTime:** A text field containing "300 s".
- LocalRequest:** A text field containing "signalFail".
- LocalRequestChannel:** A text field containing "protection".
- SwitchCount:** A text field containing "0".
- SwitchDuration:** A text field containing "0".
- TimeSinceSNCPEnabled:** A text field containing "0 days, 0 hours, 6 minutes, 11 seconds".
- Status:** A text field containing "working".

At the bottom of the dialog box are four buttons: "Refresh", "OK", "Cancel", and "Apply".

- 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).

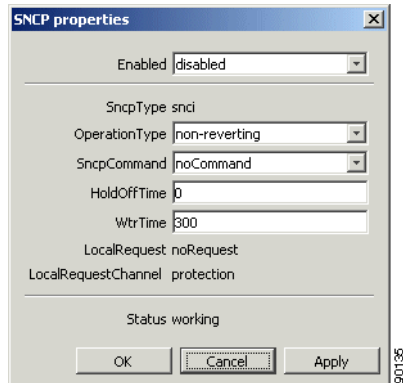
**Note**

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" (See Figure 5-62).

5.15.6 Modifying Protection Parameters of the WAN Port

WAN ports are protected as described in [“5.15.5 Protecting a WAN Port” section on page 5-61](#). The SNC is then set up with a set of default parameters. The parameters can easily be modified, [Figure 5-64](#).

- 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 (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**.

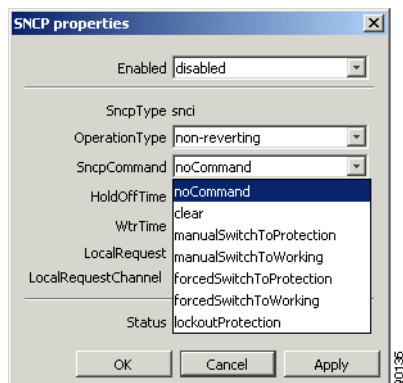
Figure 5-64 Set SNCP Properties Protection

Step 6 Click **Save** on toolbar.

5.15.7 Commanding WAN Port Protection Switch

The Cisco Edge Craft user can control the SNC protection switch by sending a command, [Figure 5-65](#).

- 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 (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 5-65 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 can now take place for some or all selected WAN channels.

5.15.8 Setting Path Trace Identifiers for 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.

5.15.9 Reading Path Trace Identifiers for 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**
- Step 4** 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.

5.15.10 Monitoring WAN Port Performance

Follow the steps below to set up monitoring of WAN port performance.

-
- 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 Performance data.
 - Step 3** Click on **PmG826NearEndVc12** to read near end PM data or **PmG826FarEndVC12** to read far end PM data.
 - Step 4** 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 on **Interval15Min**, or click on **Interval24Hour** to see the previous 24 hour counter.
 - Step 6** The following attributes are available
 - Interval15Min ES, SES, BBE and UAS
 - Interval24Hour ES, SES, BBE and UAS
-

5.15.11 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.

5.15.11.1 Selection and Insertion of Multiple Termination Points

Multiple termination points are selected like this:

-
- 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.

Entering Termination Points Manually

How to enter termination points manually.

- Step 1** Select an unconfigured WAN channel.
- Step 2** Click on 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 list. Remember to use the following format: <slot/port/C.B.K.L.M>

5.16 ONS 15302 Proprietary NxVC-12 EoS Mapping

The purpose of this chapter is to describe the tasks involved in assigning capacity from the SDH server layer to WAN ports by proprietary NxVC-12 EoS Mapping.

ONS 15302 supports the Fast Ethernet module: WAN+

Each SDH channel is equivalent to a VC-12 (2.160 Mbps). ONS 15302 has one or four WAN ports depending on the hardware configuration. The table below shows how many VC channels there are on each WAN port.

Table 5-4

Module	VC-12	VC-3	VC-4
WAN MODULE +	50	3	NA

5.16.1 WAN ports and the Mapping

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

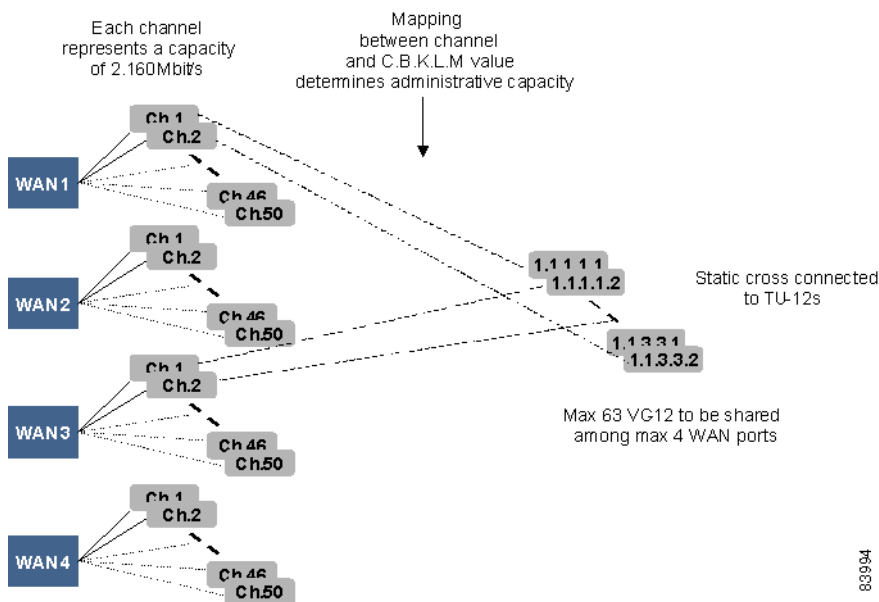
The WAN ports are logical ports and not physical ports. The potential capacity of 100 Mbps is realized and guaranteed through 47-50 VC12s each able to carry 2.160 Mbps. The overhead, that means, extra bits, are used to handle escaped characters. The capacity of the WAN port is therefore decided by how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

ONS 15302 has one STM-1 port and potentially 63 VC12s are available from 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 5-66](#).

Figure 5-66 View of the WAN Ports and their Logical View



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

5.16.2 Differences between ONS 15305 and ONS 15302

In ONS 15305 each WAN port always has 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 ONS 15302 each WAN port also has a potential capacity of 100 Mbps, but the available capacity is dependent of 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.

In ONS 15302 the Admin Capacity only indicates the number of channels that are mapped from the WAN to SDH GUI, and cannot be altered to choose bandwidth allocation in the way you can in ONS 15305.

5.16.3 Force LAN Down

This feature requires alternate routes for the IP traffic.

In situation where the WAN-connection is lost, the network element must be informed in order to initiate a switch-over. You can make this happen by forcing the equivalent LAN-port down.

A WAN Down situation will force down an equivalent Ethernet port. This situation will trigger the WanDown alarm. WanDown is the only trigger mechanism in forcing an equivalent LAN-port down.



Note

This criteria covers all traffic-affecting alarms at levels higher than VC-12 by means of SSF (Server Signal Failure).

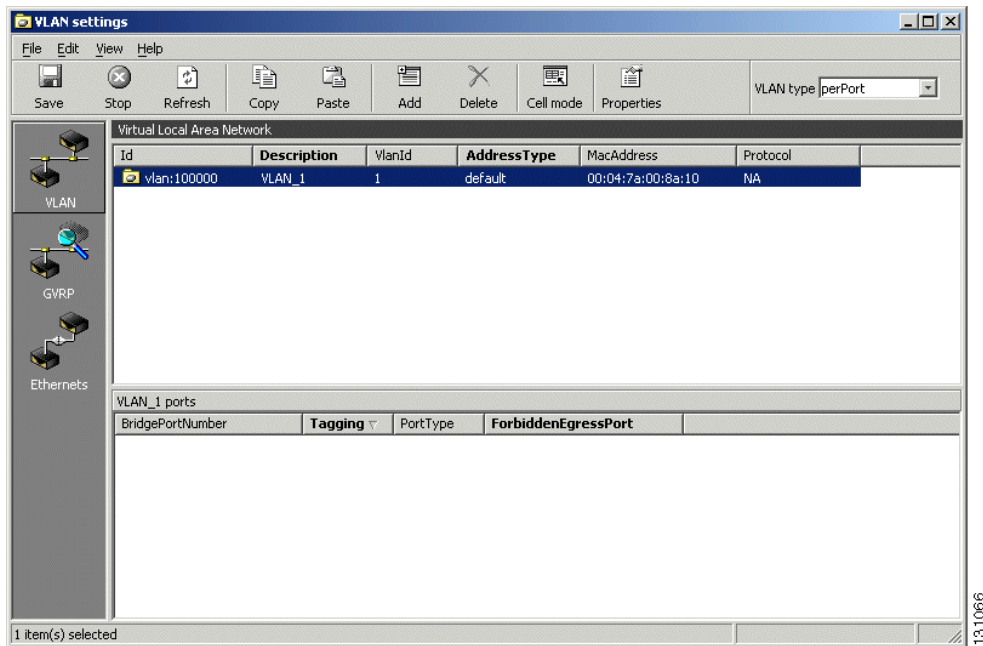
ONS 15302 supports the Force Ethernet Status Down feature- functioning as a new switch mode. When the mode is activated, a fixed relation between WAN-ports and LAN-ports is established, for example 1-5, 2-6, 3-7 and 4-8, that is, a WanDown alarm on WAN port 7 will autonomously force LAN port 3 down and so on. This requirement applies to all types of ONS 15302 WAN-ports, for instance ports with proprietary VC-12 mapping and ports with VC-12 or VC-3 GFP mapping, see the [“5.9 Ethernet Standardized Mapping”](#) section on page 5-41.

5.16.3.1 Force LAN down on WAN down alarm

In cases of mode transitions, you are recommended to follow this procedure:

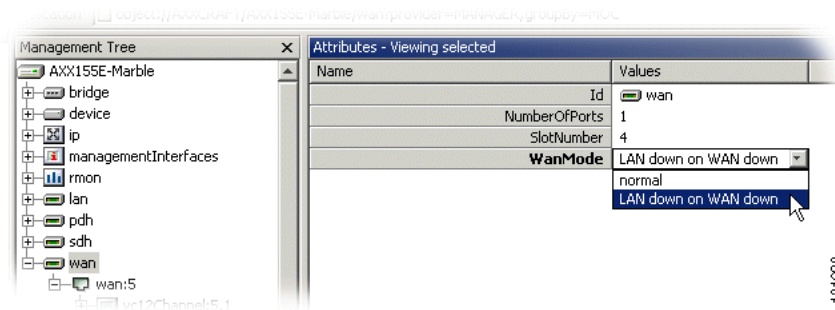
-
- Step 1** Delete all **VLAN** entries in VLAN-tables for desired network element.

Figure 5-67 VLAN entry- example



- Step 2** Click **WAN** in Management Tree.
- The WAN mode is displayed as normal (default setting.) in Attributes.
- Step 3** Change **WANmode** from Normal to LAN down on WAN down.
- Step 4** Press **Save**.

Figure 5-68 Force LAN down on WAN down

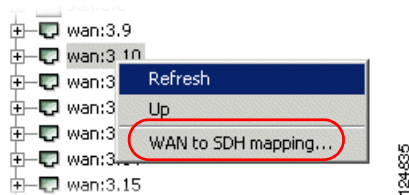


- Step 5** Restart device.

5.16.3.2 Cross-connect the WAN Channels

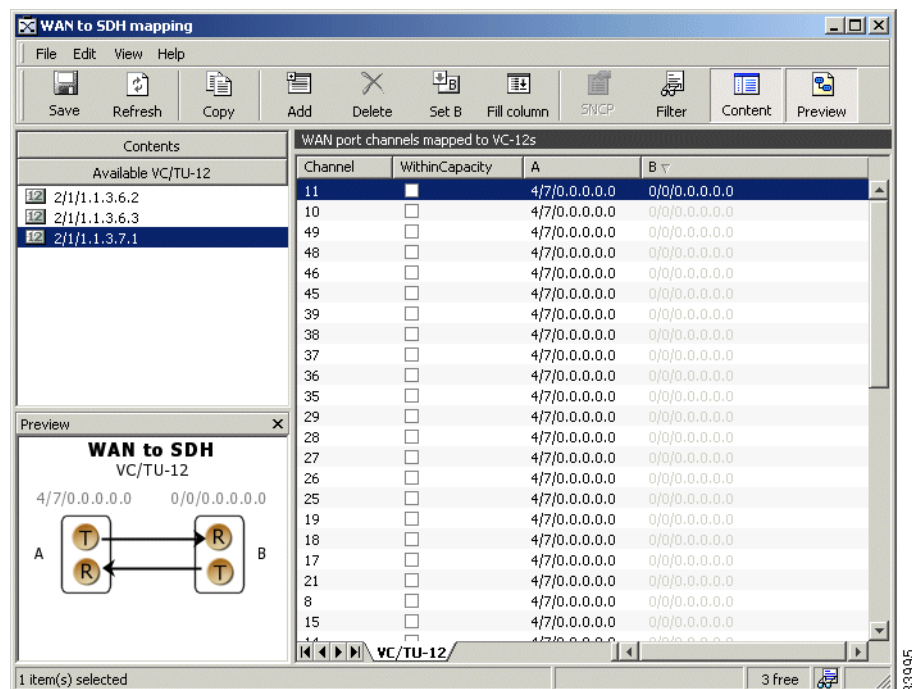
How to cross connect WAN channels:

- Step 1** Select the WAN port again, right click and select **WAN to SDH mapping**, [Figure 5-69](#).
- 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 5-69 Select a WAN port

If the Administrative Capacity is set, the **WithinCapacity** attribute indicates if the channel is in within the desired capacity, [Figure 5-70](#).

If the Administrative Capacity is not set, the WithinCapacity attribute indicates numbers of channels mapped.

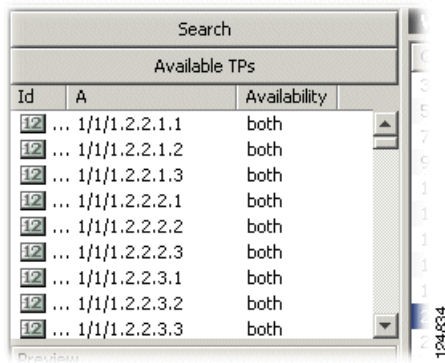
Figure 5-70 Set WAN Attributes

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 5-71](#).

Figure 5-71 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, continue 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.

5.16.4 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 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 to.
- Step 4** If **AdministrativeCapacity** is set, continue until all channels that are within capacity has a B termination point.

Step 5 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 SDH nodes.

5.16.5 Decrease Capacity in the SDH Server Layer

How to decrease the capacity in the SDH server layer:

Step 1 Select the WAN channels that are not used anymore 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, deleting mappings, must be performed in a continuous range.

Step 2 Click **Delete** on the toolbar. The selected channels become red, [Figure 5-72](#).

Figure 5-72 Delete WAN Port

WAN port termination 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	0/0/0.0.0.0.0	
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 mapping must first be deleted, and then a new termination point can be added.

5.16.6 Setting Path Trace Identifiers for 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 on the **PathTraceWAN** parameter group

Step 3 The following attributes can be set 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.

5.16.7 Reading Path Trace Identifiers for 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 on **PathTraceVC12**.

Step 4 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.

5.16.8 Monitoring WAN Port Performance

The WAN port's near and far end PM data can be monitored:

-
- 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 Performance data.
- Step 3** Click on **PmG826NearEndVc12** to read near end PM data or **PmG826FarEndVC12** to read far end PM data.
- Step 4** The following attributes are available:
- Current15Min ES,SES, BBE and UAS
- Step 5** To see the Performance history of the previous 16x15 minute counters click on **Interval15Min**. The following attributes are available:
- Interval15Min ES,SES, BBE and UAS
-

5.16.9 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.

Selection and Insertion of 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.



Link Aggregation - ONS 15305

The purpose of this section is to describe the tasks involved when managing 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.

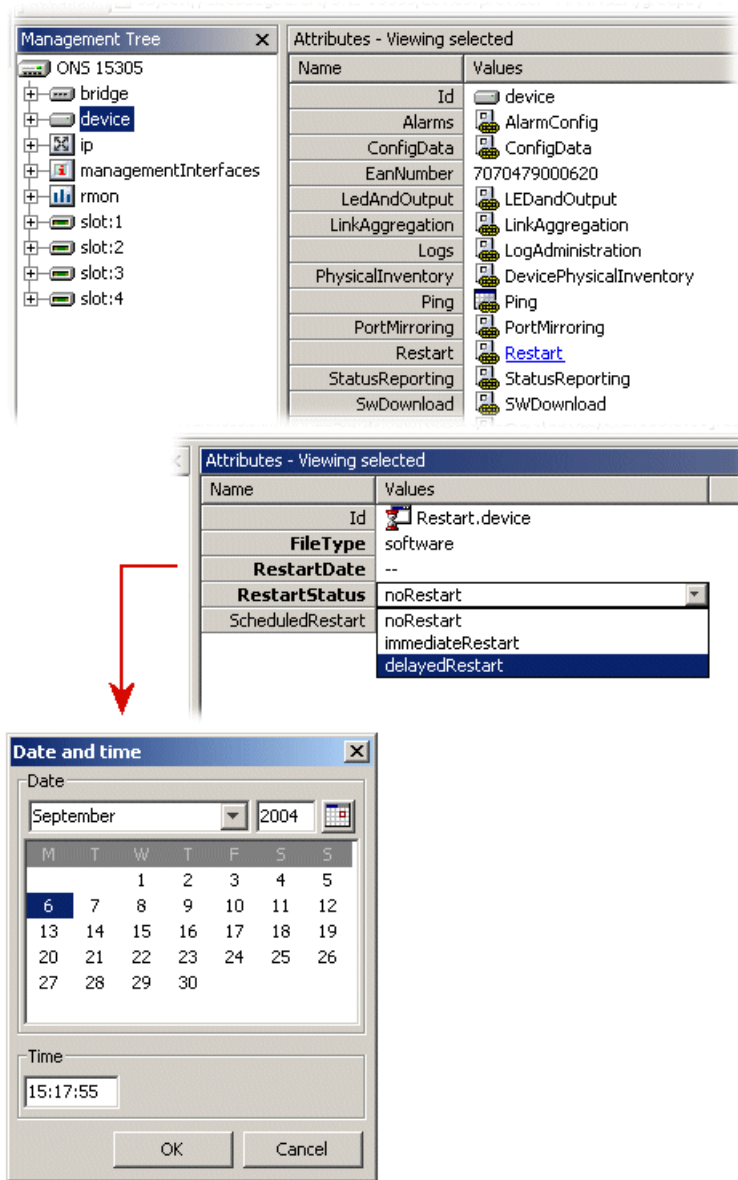
The network element defines the number of link aggregations and a maximal number of ports in each link aggregation.

6.1 View Link Aggregation

You can view specific object properties in the attributes pane:

-
- 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



124942

6.1.1 Modify Link Aggregation

You can modify the modifiable Link Aggregation parameters, and this involves:

- Modification of attributes for an aggregation.
- MAC address type for an aggregation.
- Balancing attributes for an aggregation.

- Adding of new port(s) to an aggregation.
- Deletion 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).

The number of trunks configured simultaneously is limited by equipped module type(s). Notice the following:

- Modules equipped with < 8 Ethernet LAN- and/or WAN-ports support one link aggregation trunk each.
- Modules equipped with 9-16 Ethernet LAN- and/or WAN-ports support two link aggregation trunks each, though limited within groups of bridge port numbers for configuration. Table below shows valid configurations for link aggregation using modules with 16 FE ports (FE = WAN- and/or LAN-ports).

Table 6-1 Valid Link Aggregation configuration for 16xFE port module

Slot	Trunk	Valid groups of bridge port numbers
1	1	1-8
1	2	9-16
2	1	17-24
2	2	25-32
3	1	33-40
3	2	41-48
4	1	49-56
4	2	57-64

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.

6.1.1.1 Assigning a Port to a Trunk

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, 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**.
-

6.1.2 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, a 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.

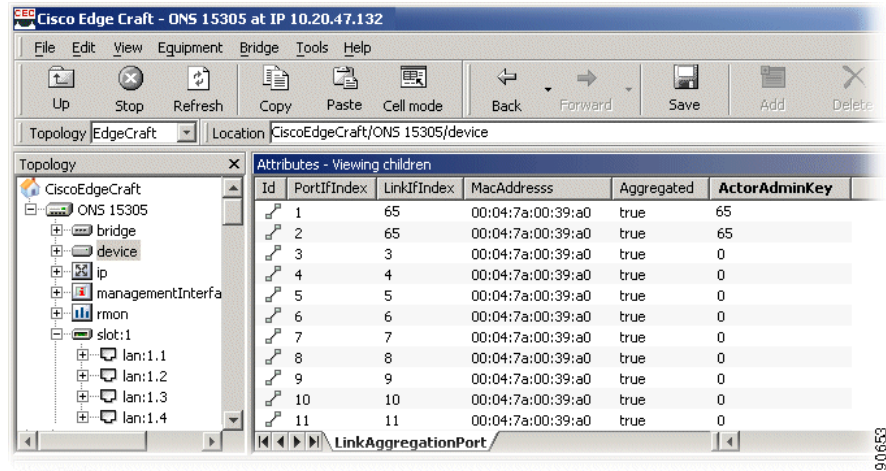
STM-1 modules are special since they are a combination of 8 SDH ports and 8 WAN ports. WAN ports in an 8XSTM1 module are numbered x/9 to x/16 (x is the slot), while the ifIndexes corresponds to x/1 to x/8. For an 8xSTM-1 module located in slot 2, the ifindex range is 17 to 24 (17 for port 2/9, 24 for 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 on page 6-5](#).

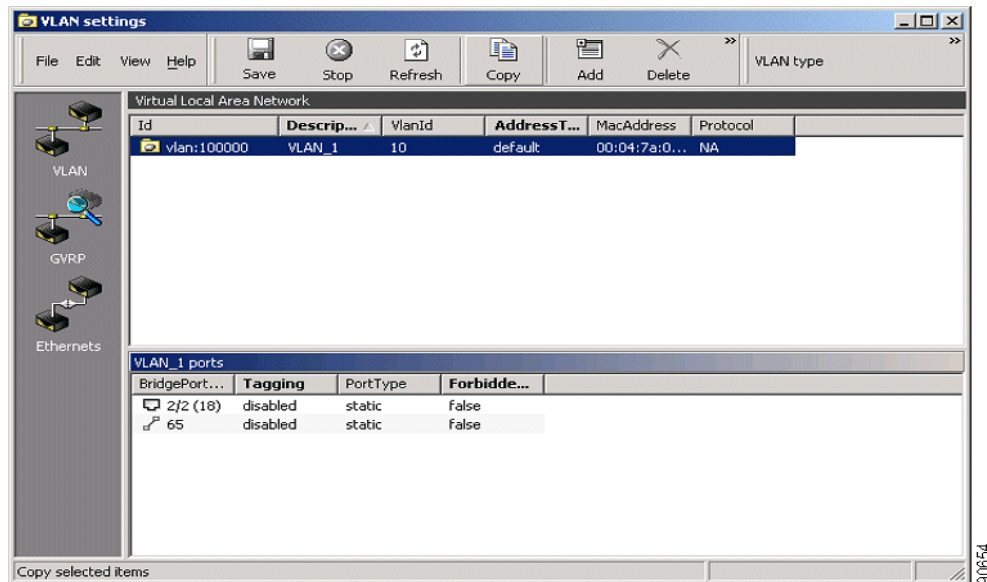
The first two WAN ports of slot 1 are used to create a trunk with ifindex 65.

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

The purpose of this chapter is guide you through management of the bridging service (L2 forwarding) on the network element.

This includes:

- Presentation and modification of the bridge.
- QoS for 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 ONS 15305, but the features described, also apply for ONS 15302.

7.1 Bridge

This chapter describes the configuration operations supported by the Bridge M.O. It is organized in two sections:

- Introduction
- Examples: this chapter is a repository of simple, but yet typical configuration scenarios.

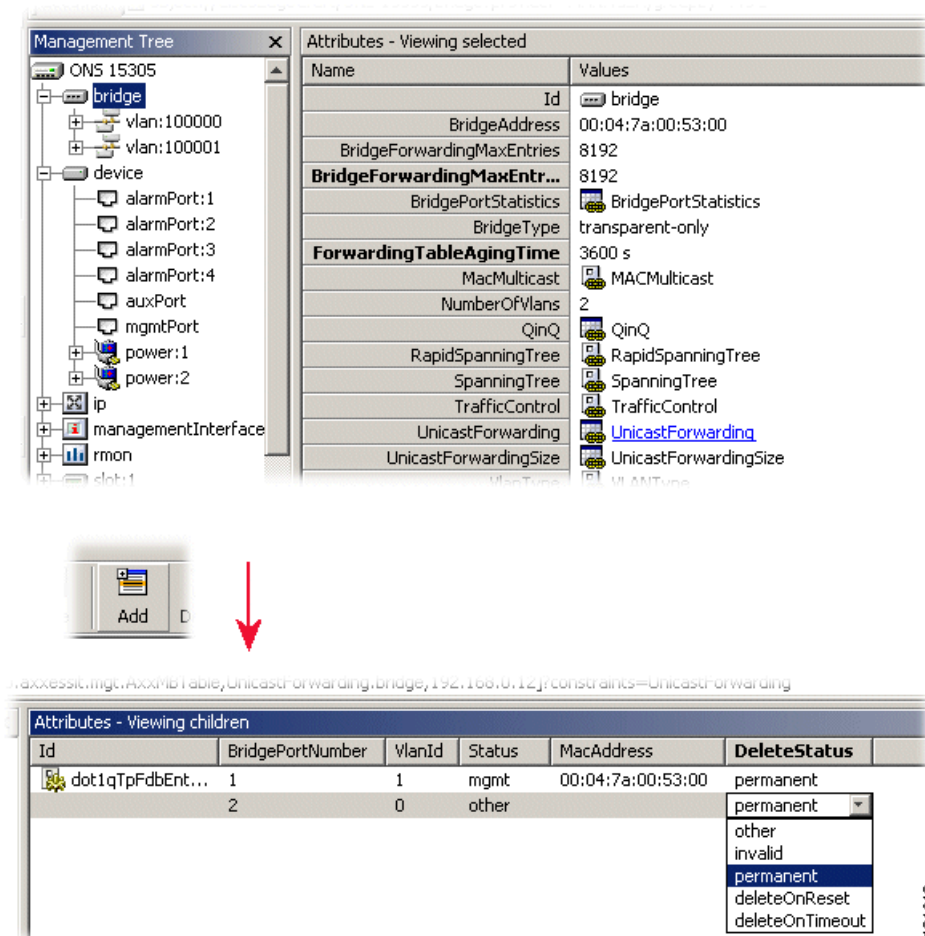
Troubleshooting and FAQ, see [Chapter 9, “Troubleshooting and FAQ.”](#) This chapter contains a few tips, and gives answers to a number of Frequently Asked Questions.

7.1.1 Examples

7.1.1.1 Configuration of Static Unicast Forwarding Information

Configure an entry in the MAC unicast forwarding table, [Figure 7-1](#).

-
- Step 1** Click on the ONS 15305 managed object, and then the **Bridge** managed object in the topology browser.
- Step 2** Double-click on **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.

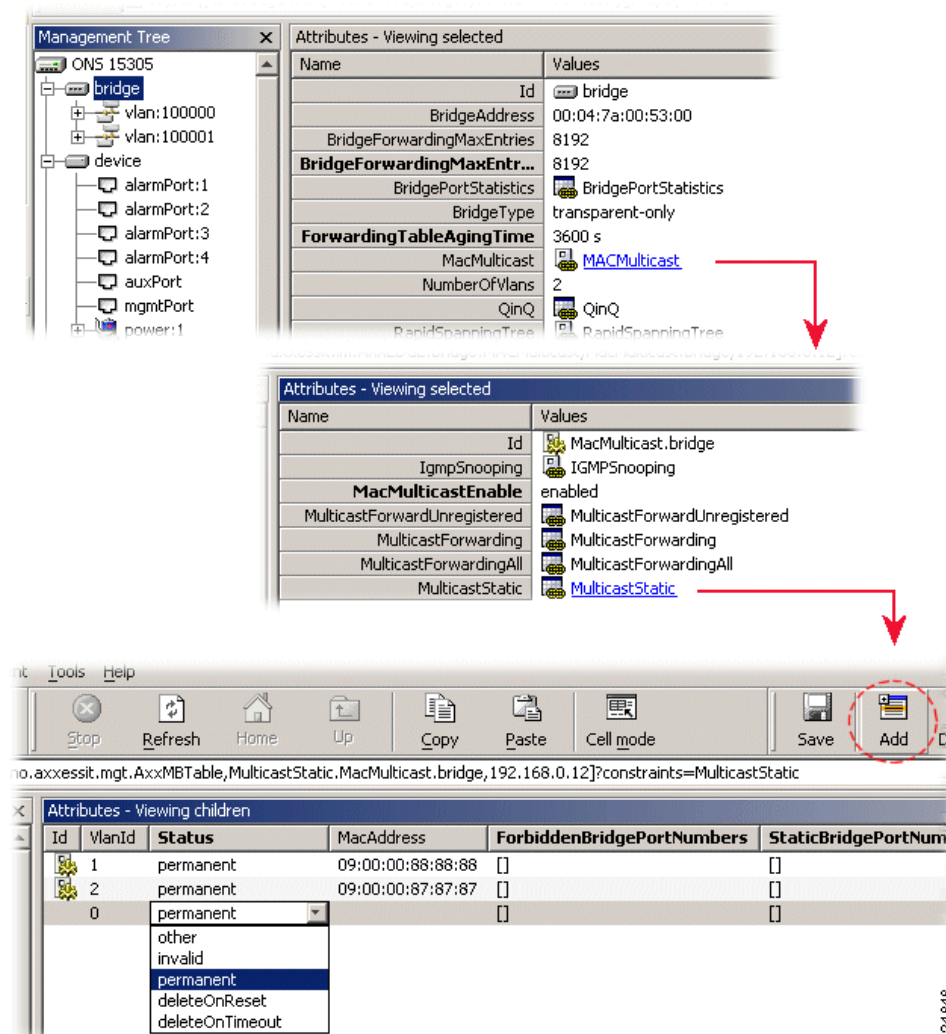
Step 5 Click **Save** on the toolbar.

7.1.2 Configuration of Static Multicast Forwarding Information

Please see [Question 5, page 9-2](#) before you start Configure an entry in the MAC multicast forwarding table, [Figure 7-2](#).

- Step 1** Click on the ONS 15305 managed object, and then the **Bridge** managed object in the topology browser.
- Step 2** Double-click on **MACMulticast**, then on **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 [Chapter 9, “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 [Chapter 9, “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 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.

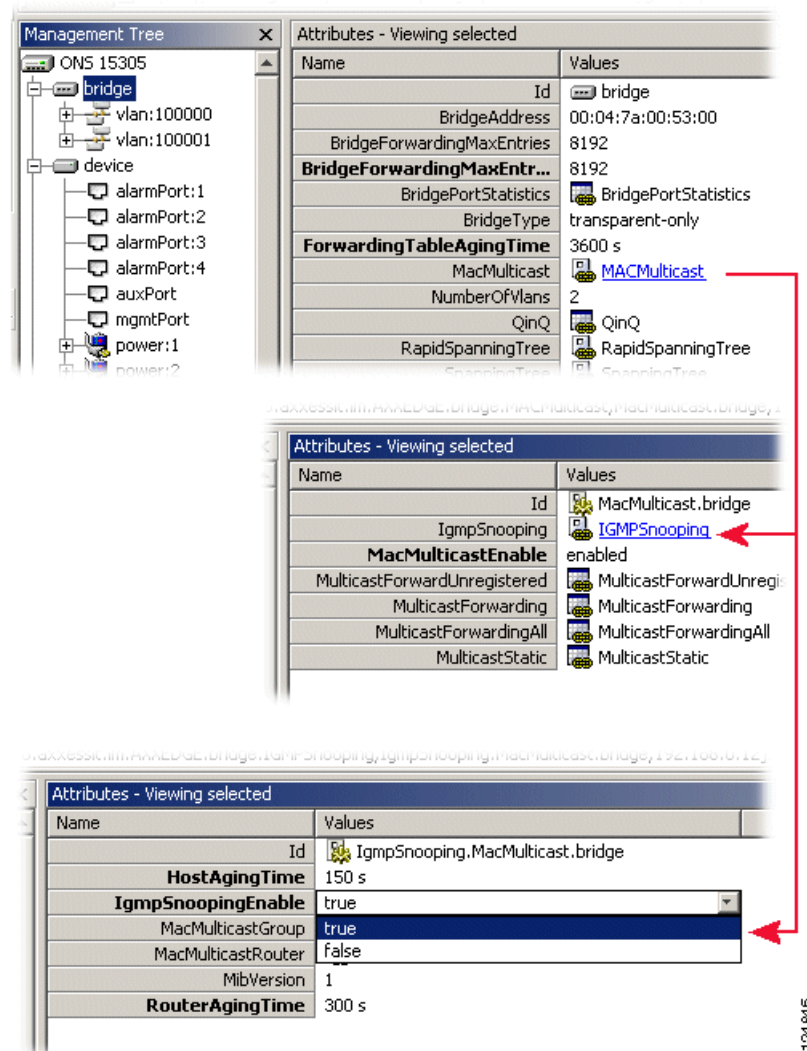
7.1.3.1 Enabling IGMP Snooping

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



124846

7.2 Miscellaneous

This section describes STP, RSTP, MAC Multicast and Traffic control.

7.2.1 Spanning Tree Protocol (STP) Configuration

The STP allows layer 2 devices to discover a subset of the topology that is loop-free, but still with a path between every pairs of LANs.

STP is compatible with the RSTP. See [7.2.2 Rapid Spanning Tree Protocol \(RSTP\) Configuration, page 7-6](#)

The network element can run either one single STP algorithm for the whole device (per Device type), or one STP algorithm per VLAN (per VLAN 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.

7.2.1.1 Configuring the STP Algorithm per Device

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 forward Delay, hello Time, max Age, 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 Rapid Spanning Tree Protocol (RSTP) Configuration

The original STP uses rather 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 ONS 15302 and ONS 15305 support only a partial RSTP implementation which offers the same type of service as e.g. PortFast on Cisco equipment, as it 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 ONS 15302 or ONS 15305 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 ONS 15302 and ONS 15305.

7.2.2.1 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**.
-

7.2.3 MAC Multicast

Multicast is a method of sending one packet to multiple destinations. Multicasting is used for applications such as video conferencing, 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 ONS 15302 and ONS 15305 support 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, and that the use of these tables are only necessary for performance tuning.

7.2.3.1 Enabling MAC Multicast Control Tables

The internal resources of the ONS 15302 and ONS 15305 used for the multicast tables are shared with the VLAN tables. The total of VLAN entries and multicast groups registered are 4000, and both types of entries occupy the same amount of resources. Hence, to enable the Multicast feature, ensure that the maximum amount of VLANs is less than 4000 according to how many multicast groups anticipated. For most applications 4000 VLANs are well above what will be used, and in these cases one can safely reserve a good chunk of entries for multicast traffic.

Configuring MAC Multicast

Multicast menu has the following menu options:

- IGMPSnooping

- MacMulticastEnable
- MulticastForwardUnregistered.
- MulticastForwarding.
- MulticastForwardingAll.
- MulticastStatic

The parameter MacMulticastEnable is for enabling/disabling of the MAC Multicast control tables.

7.2.3.2 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.

7.2.3.2.1 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.

7.2.3.2.2 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.

7.2.3.2.3 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.

7.2.4 Traffic Control

The Traffic Control menu has the following menu options:

- PortPriority
- PriorityGroup
- TrafficClass

7.2.4.1 PortPriority

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.

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.

7.2.4.2 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 theoretical 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).

7.2.4.3 TrafficClass

Classification of Ethernet frames are done according to the information in the TrafficClass table. The device use four queues for differentiating traffic, and as 802.1p defines eight different priorities, the priorities 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).

7.3 Manage VLAN

The purpose of this section is to guide you through management of 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).

7.3.1 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 ONS 15305 which can be assigned to a VLAN, is limited to 64. The maximum number of Ethernet-ports per slot is 16. Also see [Troubleshooting and FAQ, Question 7, page 9-3](#).

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.

7.3.1.1 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.

Example:

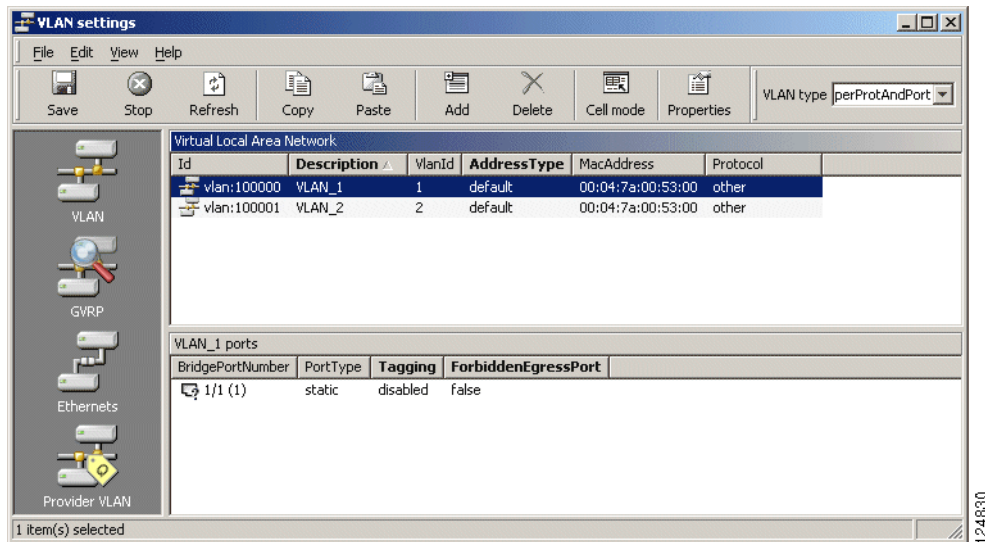
If a port is member of two VLANs with the VIDs of 10 and 20, and the port receives frames tagged according to VID 10, 20 and 30, only the frames with VID 10 and 20 will be accepted and forwarded. The frames with VID 30 will be discarded.

It is absolutely 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.

7.4 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



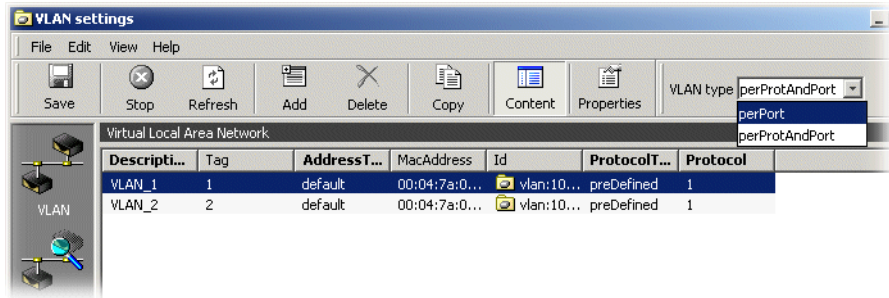
The following examples show how a VLAN per port, and a VLAN per port and protocol can be created and provisioned by using the custom GUI. The VLAN custom GUI can be opened either by clicking on VLAN Setting under the Bridge menu on the Cisco Edge Craft desktop, or by right-clicking on Bridge M.O. in the topology browser, and then selecting VLAN Setting.

7.4.1 Configuration Of A New VLAN Per Port

Create a new VLAN per port.

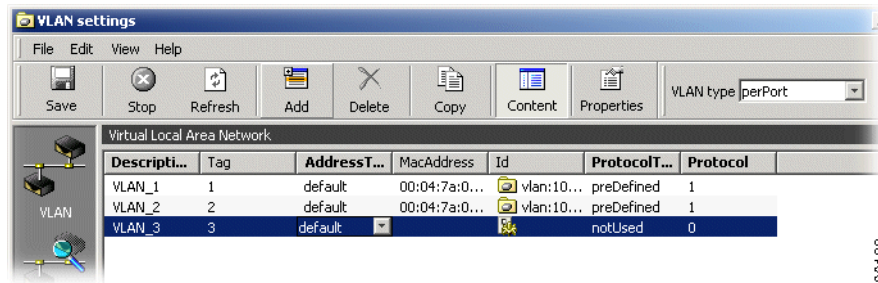
- Step 1** Verify that the VLAN type on the top right corner of the GUI is set to perPort, [Figure 7-5](#). If not, set **VLAN type** to **perPort**, and click **Yes** when asked if the network element should be rebooted.

Figure 7-5 VLAN Settings



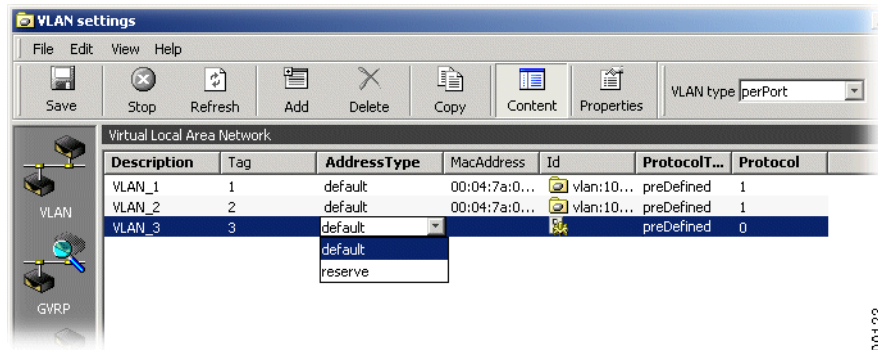
Step 2 Click **Add** in the GUI, [Figure 7-6](#).

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



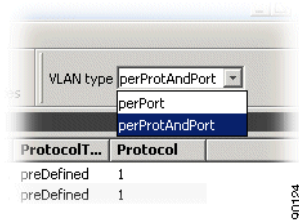
Step 4 Click **Save**.

7.4.2 Configuration Of A New VLAN Per Protocol And Per Port

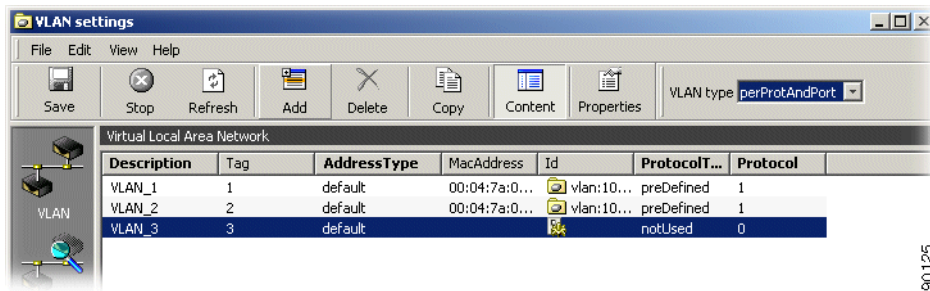
Create a new VLAN per protocol and per port.

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.

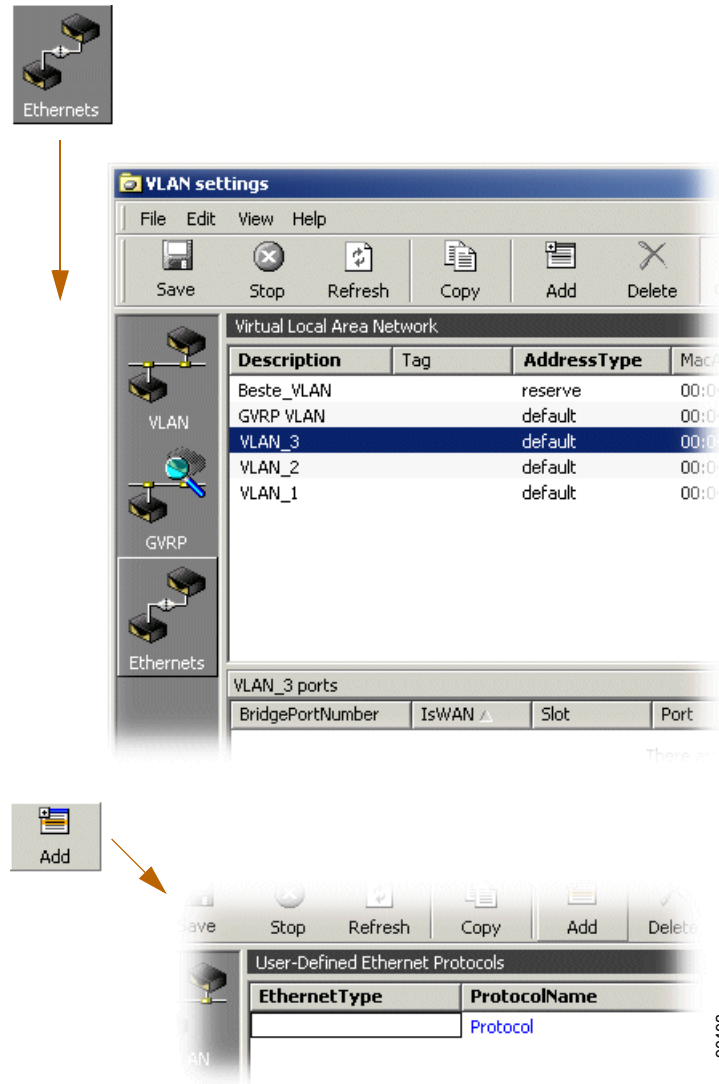
7.4.3 Configuration of an Ethernet User Defined Protocol

How to configure an ethernet user defined protocol:

7.4.3.1 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.

7.4.3.2 Use One Of The 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

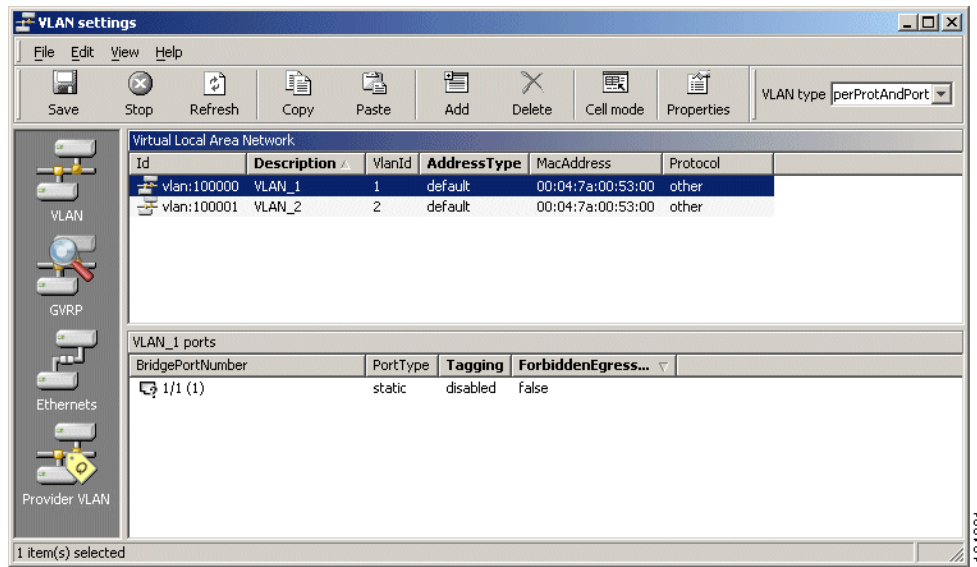
Step 3 Edit the description, tag, and/or addressType attributes if required.

Step 4 Click **Save**.

7.4.4 Configuration of VLAN Port Members

Add port members to an existing VLAN

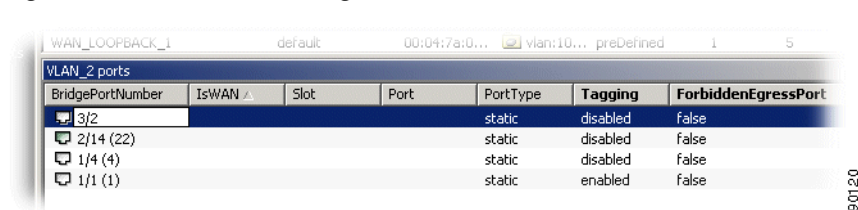
Step 1 Select the VLAN to which ports will be added. The VLAN is highlighted in the virtual local area network window (top window in [Figure 7-11](#)). The list of ports already members of the VLAN is displayed in the VLAN ports window (bottom window in [Figure 7-11](#)).

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.

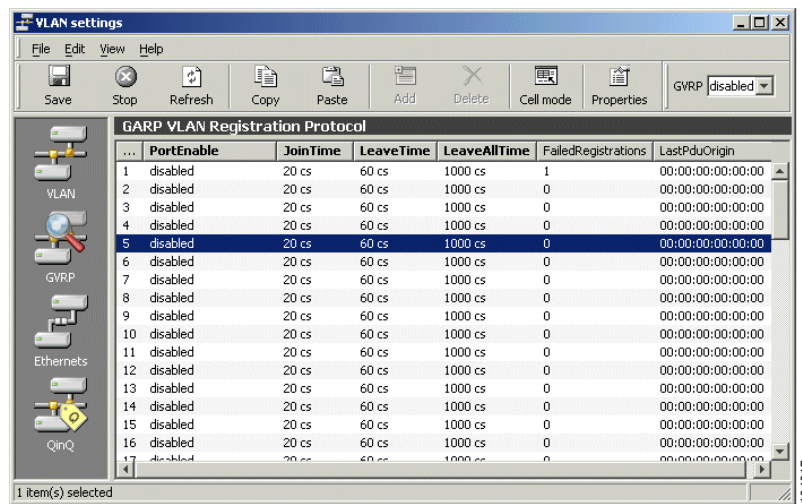
Figure 7-12 Edit the Bridge Port Number

- Step 5** Edit the tagging and forbiddenEgressPort attributes if required.
- Step 6** Click **Save**.

7.4.5 GVRP

GARP VLAN registration protocol (GVRP).

- Step 1** Click **GVRP** in the Content pane, [Figure 7-13](#).

Figure 7-13 GVRP Attributes

The following attributes are modifiable:

- PortEnable

Set to enabled or disabled.

- JointTime

Set value in centiseconds.

- LeaveTime

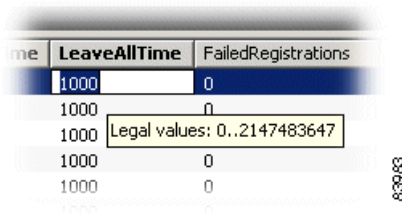
Set value in centiseconds.

- LeaveAllTime

Set value in centiseconds.

7.4.5.1 Legal time values

Click in desired 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

7.4.6 Provider VLAN (IEEE 802.1Q, Q in Q)

7.4.6.1 Overview

The 802.1Q Tunneling is part of the Layer 2 switching capabilities of the Cisco ONS 15300 SDH product line. The desired functionality enables the operator to tunnel separate customer traffic, containing 802.1Q tagged (VLAN tagged) Ethernet frames, through a second layer of VLANs. This allows the operator to be oblivious to the customers VLAN schemes, and focus on managing only one VLAN per customer through the network. At the same time, the different customers on a shared device can use whatever VLAN IDs they choose without the risk of interfering with each others VLAN schemes.

7.4.6.2 Definitions

- Tunnel Port

By tunnel port we mean a LAN port that is configured to offer 802.1Q-tunneling support. A tunnel port is always connected to the end customer, and the input traffic to a tunnel port is always 802.1Q tagged traffic.

The different customer VLANs existing in the traffic to a tunnel port shall be preserved when the traffic is carried across the network.

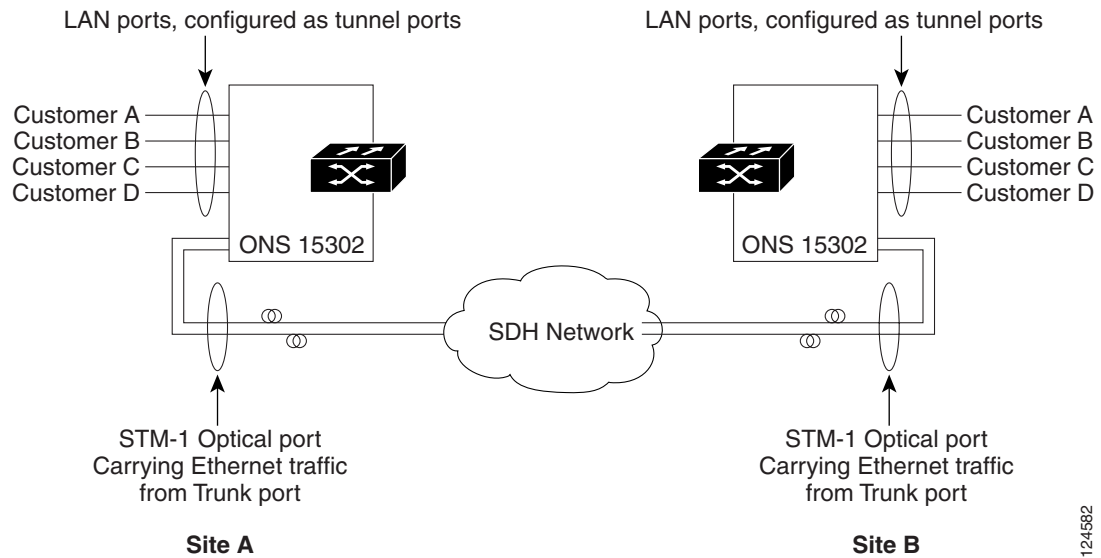
- Trunk Port

By trunk port we mean a LAN port that is configured to operate as an interswitch link/port, able of carrying double-tagged traffic. A trunk port is always connected to another trunk port on a different switch. Switching shall be performed between trunk ports and tunnels ports and between different trunk ports.

7.4.6.3 Applications - examples

Application 1

Application 1 is two ONS 15302 connected back to back over an SDH network as shown in Figure 7-15, carrying Ethernet traffic from different customers using double tagging (802.1Q tunnelling).

Figure 7-15 Application Example 1

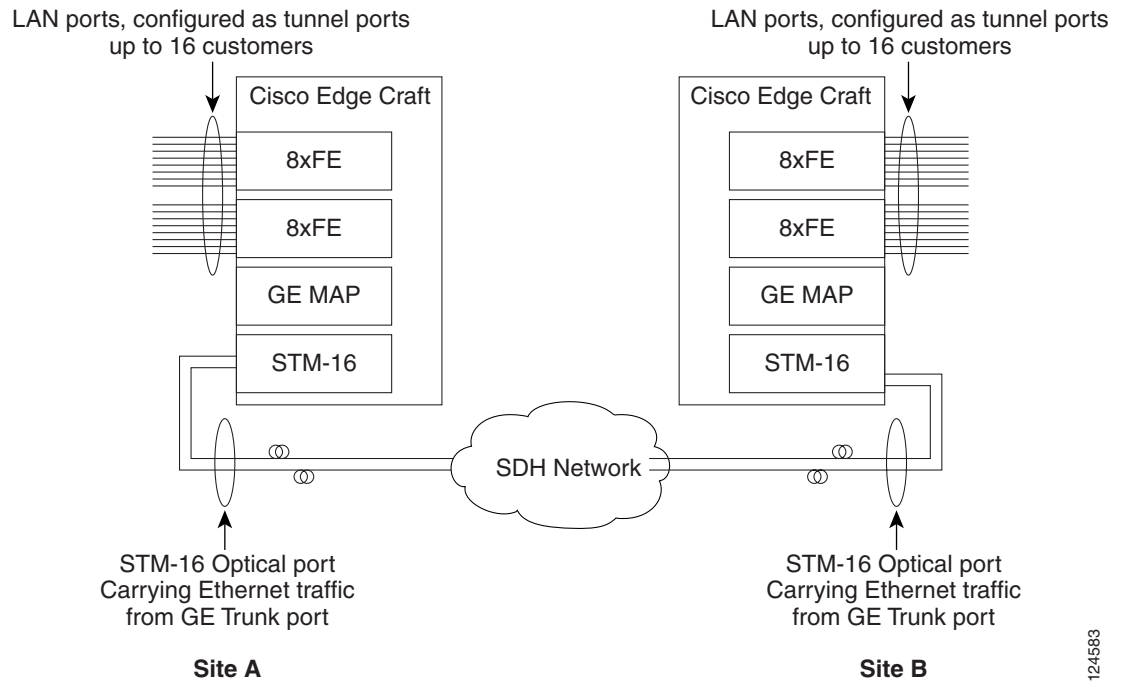
In this application both the tunnel ports and the trunk port is on the same switch.

124582

Application 2

Application two is two ONS 15305 connected back to back over an SDH network as shown in Figure 7-16, carrying Ethernet traffic from different customers using double tagging (802.1Q tunnelling). This application is equal to application 1 except that the number of tunnel ports is increased and the trunk port is a GE port, which requires an STM-4 or STM-16 optical interface.

Figure 7-16 Application Example 2



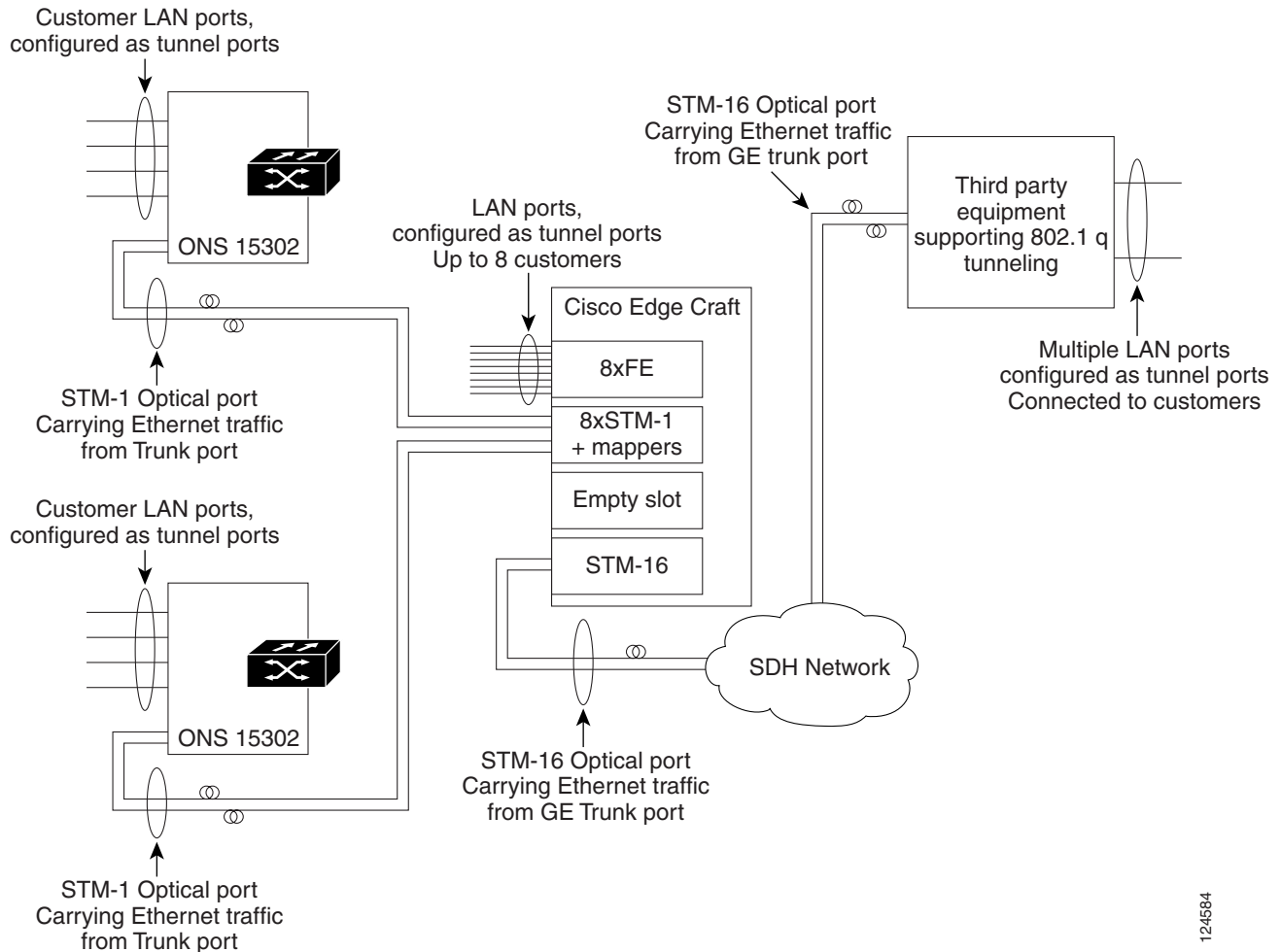
The customer tunnel ports are FE ports, while the trunk port mapped into the SDH traffic is a GE port. In this application the tunnel ports and the trunk ports reside on different switches.

124583

Application 3

In application 3, shown in Figure 7-17 below, the ONS 15305 has the same trunk port towards the network as in application 2, but 8 of the tunnel ports towards the customers are removed and replaced of 8 STM-1 ports connected to ONS 15302 devices (for simplicity only two ports and two ONS 15302 devices are shown). Each of the 8 STM-1 ports is connected to a switch via a mapper circuit. The LAN ports are configured as trunk ports, making them able to talk to the trunk ports on the ONS 15302s. This application also includes switching between trunk ports.

Figure 7-17 Application Example 3



124584

7.4.7 Provider VLAN

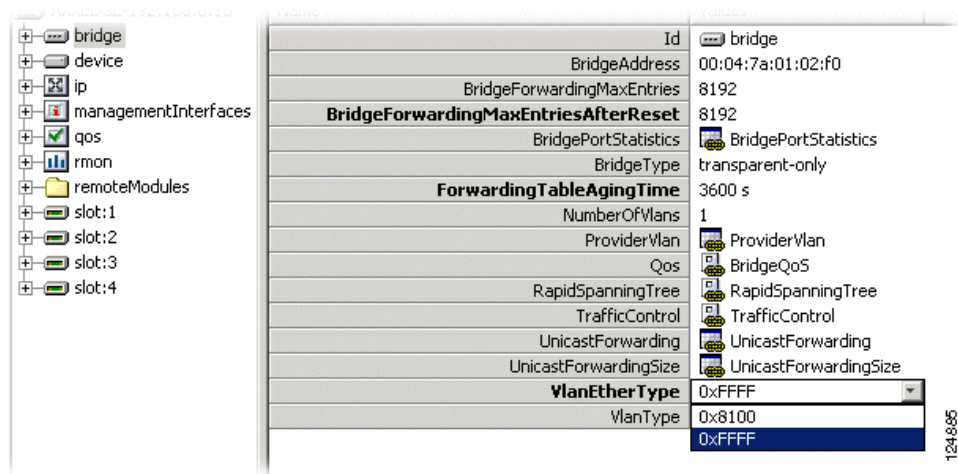
7.4.7.1 Setting up Provider VLAN - ONS 15305

Depending on network element and module version, the Provider VLAN features is implemented on two different levels:

- Switch/Bridge or
- Module/Port policer (new in ONS 15305 R2.0 and ONS 15302 R2.0) The new LAN/WAN modules implements QinQ in Policers allowing for individual setup pr. port. The older modules require a common QinQ setup on the switch.

Step 1 Select **bridge > VlanEtherType** in the Management Tree.

Figure 7-18 **VlanEtherType**



Step 2 Using the pulldown menu set **VlanEtherType**
Set **0xFFFF** for configuration in Switch. This setting completes the QinQ configuration for old modules
Set **0x8100** for configuration through Policer (new modules only). Continue configuration as described in [7.4.7.1 Setting up Provider VLAN - ONS 15305, page 7-22](#).

Step 3 Click **Save**.



Note

VlanEtherType set to 0x8100, is only applicable to the new E100-WAN-8 and GigE-WAN-2 modules introduced for ONS 15305 R2.0 and WAN MODULE+ for ONS 15302 R2.0. These modules support QinQ configuration on per port basis.

7.4.7.2 Setting up Provider VLAN - ONS 15305 with FE/GE+SMAP modules

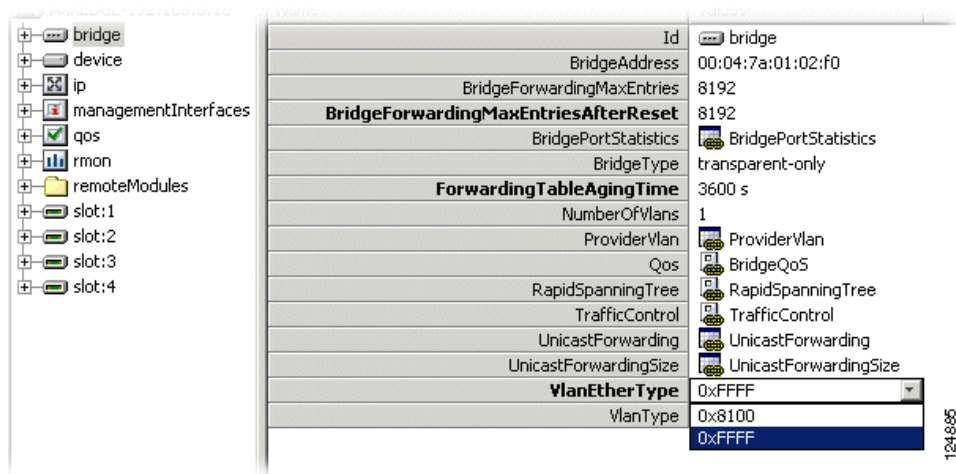


Note

The following description is only applicable for the following modules introduced in ONS 15305 R2.0; GigE-2-LC, GigE-WAN-2 and the E100-WAN-8 module.

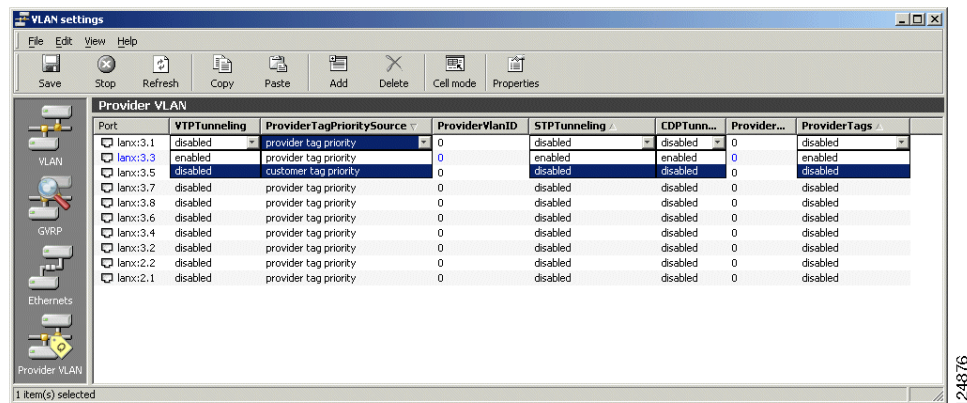
Step 1 Select **bridge > VlanEtherType** in the Management Tree.

Figure 7-19 VlanEtherType



- Step 2** Using the pulldown menu verify that **VlanEtherType** is set to **0x8100**.
- Step 3** Click the **Provider VLAN** button in the **Content** pane in VLAN settings window. Available ports with Provider VLAN available, are displayed:

Figure 7-20 Provider VLAN



7.4.7.3 ProtocolTunneling

Enabling the ProtocolTunneling attribute makes the port transparent to other Layer 2 protocols, such as RSTP.

As an example, If a Service Provider VLAN manages his own Spanning Tree, the Network Owner may need to exempt the port used by the Service Provider from the Network Owners own spanning trees to prohibit the two spanning tree protocols from interfering with each other.

7.4.7.4 ProviderTagPrioritySource

Ethernet packages in a VLAN is allocated a priority that controls the packets flow through the network switches. When entering Service Provider VLAN traffic into a Network Owner VLAN, this attribute controls if the Network Owner VLAN shall inherit the Service Provider VLAN priority settings, or assigns his own priority settings.

taginframe forces the Network Owner VLAN to inherit the Service Provider priority.

qtagregister assigns a Network Owner custom priority to his VLAN traffic. The priority is read from a local data register.

7.4.7.5 VLANProviderID

This attribute identifies the Service Provider VLAN that uses the highlighted LAN/WAN port.

7.4.7.6 ProviderTagPriority

This attribute sets the custom priority value (0.7) that is used when the ProviderTagPrioritySource is set to "qtagregister".

7.4.7.7 ProviderTags

This attribute enables or disables QinQ (Provider VLAN) support on the selected port.

- Step 4** Set Provider VLAN attributes for desired ports and click **Save**.
- Step 5** Repeat for other network elements that are part of the desired application. (Select **File>Reconnect** to access the other NE's)

7.4.7.8 Setting up Provider VLAN - ONS 15302



Note

This procedure is only applicable to ONS 15302 R 2.0 equipped with the new WAN module, supported in this release.

- Step 1** Select Bridge>**Bridgemode** in the Management Tree.

- Step 2** Set Bridgemode = **provider**

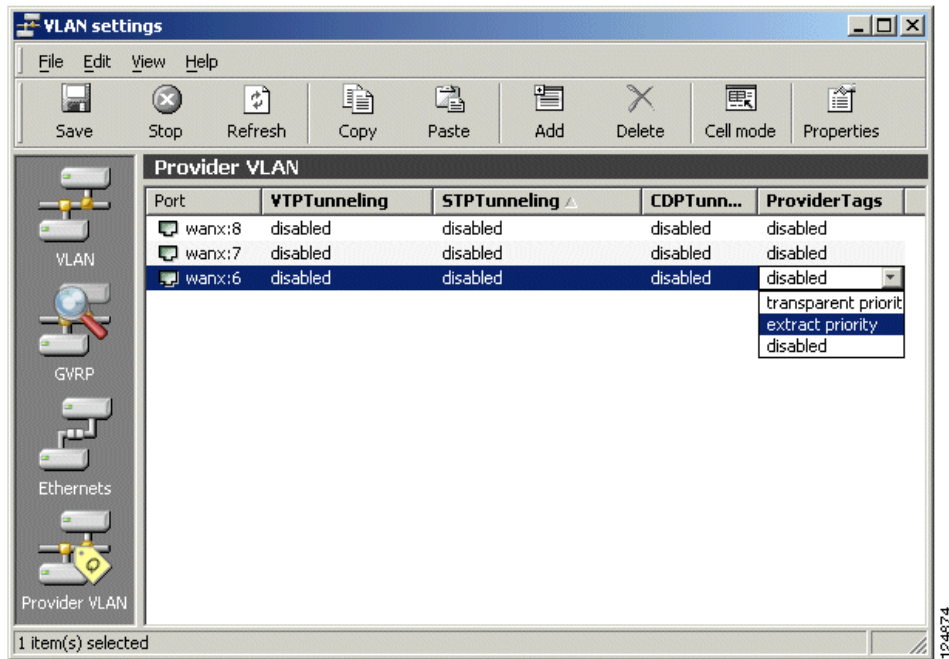
The switch will now operate with a proprietary VLAN Ethertype; 0xFFFF.

Using a VLAN with one LAN port and one WAN port, where the LAN port is untagged and the WAN Port is tagged, the switch will enter an additional VLAN tag. This tag is identified by the type 0xFFFF and has priority as set in Bridge>TrafficControl>PortPriority (default priority for this port). The tag has VLAN ID as indicated in the VLAN Table.

The Provider Tag configuration allows the Mapper in the FPGA to switch the proprietary 0xFFFF to 0x8100, enabling these frames to be switched by other 3rd party switches.

- Step 1** Click the **Provider VLAN** button in the **Content** pane in VLAN setting window.
- Step 2** Select **ProviderTags** setting;
disabled,
transparent priority: use the default port priority
or **extract priority**: inherit priority from the customer traffic.

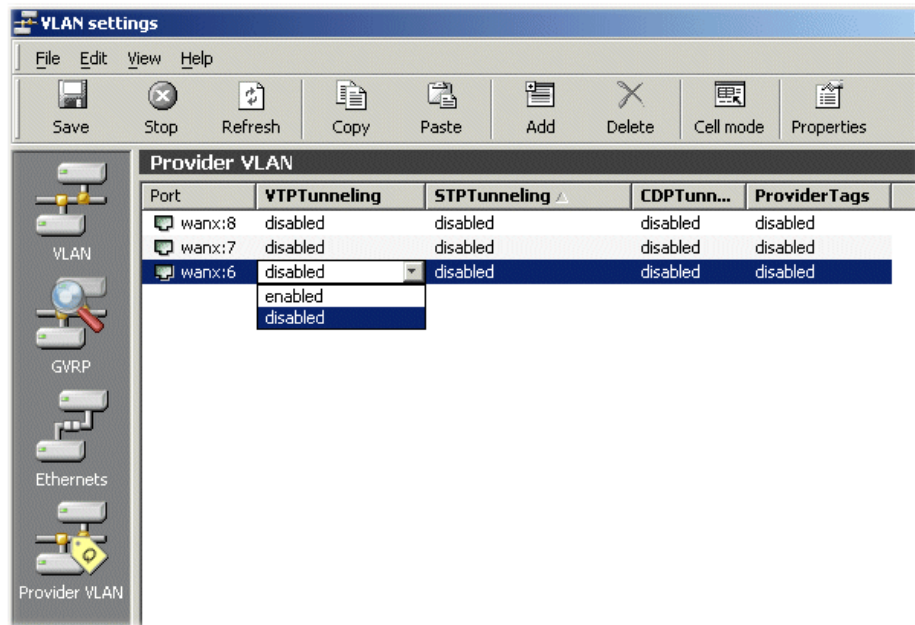
Figure 7-21 *Provider Tags Setting*



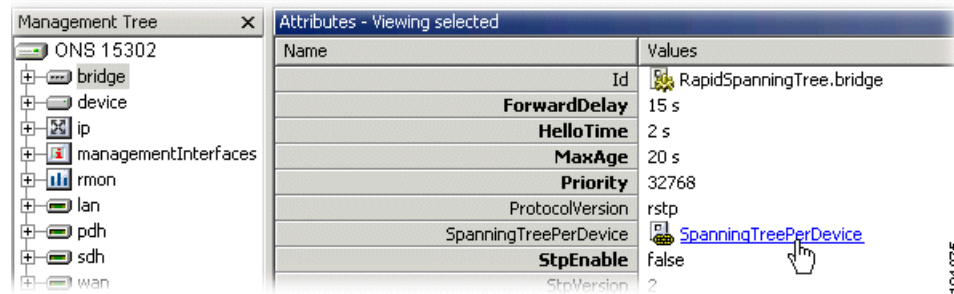
- Step 3** Click **Save**.
- Step 4** Repeat for other network elements that are part of the desired application. (Select **File>Reconnect** to access the other NE's).

7.4.7.9 Enabling Protocol Tunneling

ProtocolTunneling is default set to NA (due to STP enabled).

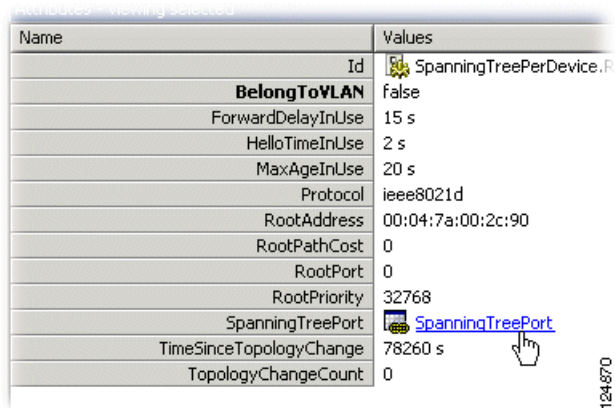
Figure 7-22 Protocol Tunneling

To enable ProtocolTunneling please follow these steps:

Figure 7-23 SpanningTreePerDevice

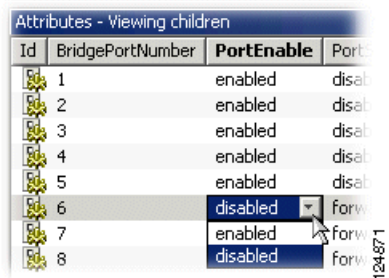
Step 1 In the Management Tree select **bridge > SpanningTreePerDevice**.

Step 2 Select **SpanningTreePort**.

Figure 7-24 *SpanningTreePort.*


Name	Values
Id	SpanningTreePerDevice.R
BelongToVLAN	false
ForwardDelayInUse	15 s
HelloTimeInUse	2 s
MaxAgeInUse	20 s
Protocol	ieee8021d
RootAddress	00:04:7a:00:2c:90
RootPathCost	0
RootPort	0
RootPriority	32768
SpanningTreePort	SpanningTreePort
TimeSinceTopologyChange	78260 s
TopologyChangeCount	0

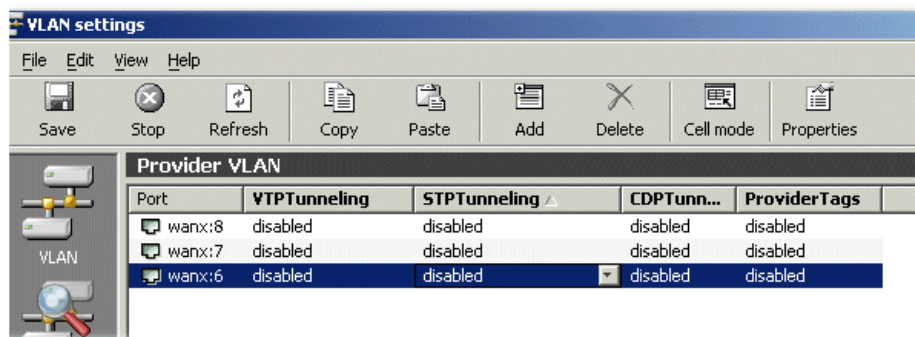
Step 3 Select desired Port and set **PortEnable** attribute to **disabled**.

Figure 7-25 *PortEnable*


Id	BridgePortNumber	PortEnable	Port
1		enabled	disab
2		enabled	disab
3		enabled	disab
4		enabled	disab
5		enabled	disab
6		disabled	forw
7		enabled	forw
8		disabled	forw

Step 4 Return to VLAN Settings and continue the Provider VLAN settings.

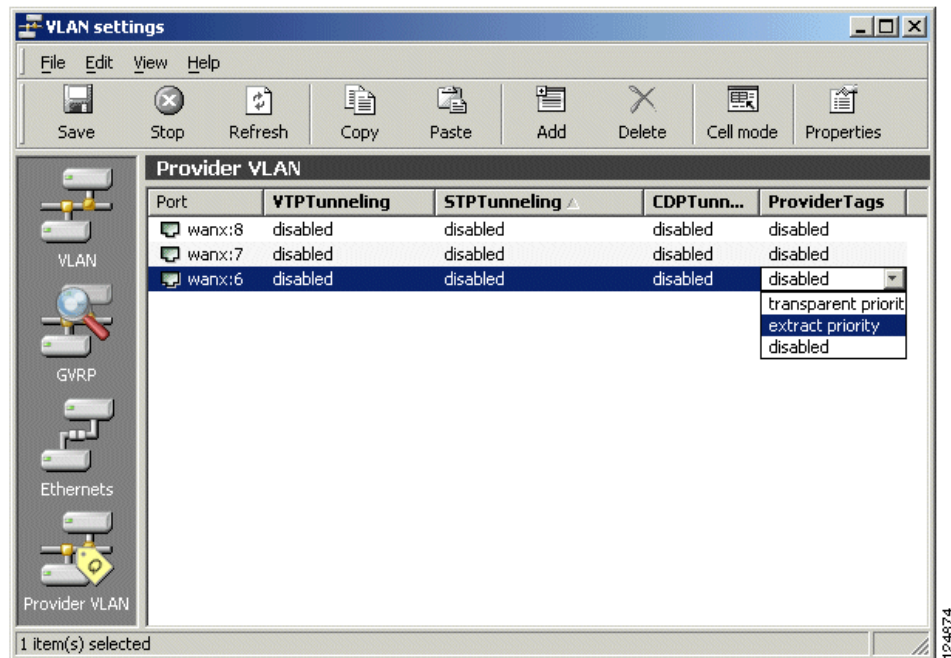
Step 5 Set **ProtocolTunneling** to **enabled**.

Figure 7-26 *Protocol Tunneling*


VLAN settings				
File Edit View Help				
Save Stop Refresh Copy Paste Add Delete Cell mode Properties				
Provider VLAN				
Port	VTPTunneling	STPTunneling	CDPTunn...	ProviderTags
wanx:8	disabled	disabled	disabled	disabled
wanx:7	disabled	disabled	disabled	disabled
wanx:6	disabled	disabled	disabled	disabled

Step 6 Set to desired value:
disabled, transparent priority or extract priority

Figure 7-27 ProviderTags



<\$chapnum>.0.1 QinQ

The following section focus on QinQ settings for ONS 15305 Release 1.1 and ONS 15302 Release 1.0.

This implementation is using the value 0xFFFF as Ethertype for the Provider VLAN. Hence, Provider VLAN tagged traffic will not be recognized as VLAN tagged traffic according to 802.1Q (as the later implementation does) if sent through third party VLAN aware switches.

For these network element releases, the QinQ implementation is different than described in “Provider VLAN (IEEE 802.1Q, Q in Q)” on page -19.

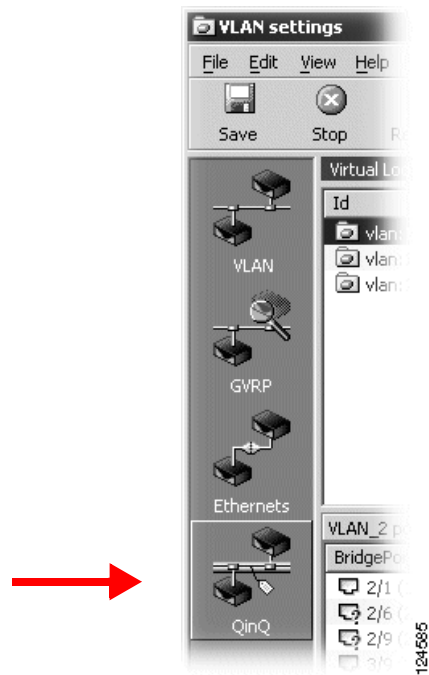
For ONS 15305 the following QinQ settings are available (depending on selected module type); **available ports, disable and enable.**

For ONS 15302: **disable or enable.**

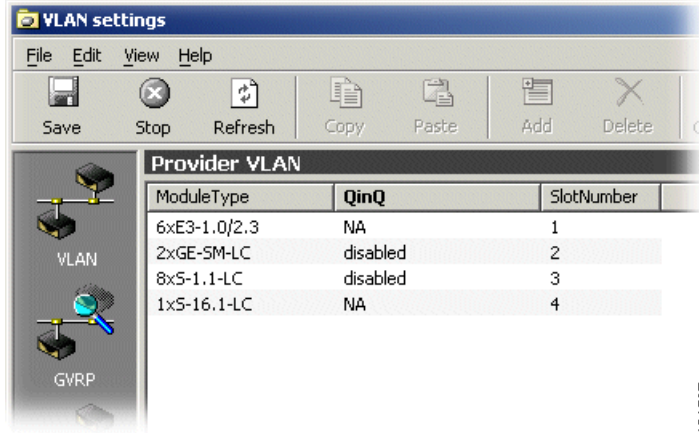
7.4.7.10 Setting up Q in Q - ONS 15305

Step 1 Click the **QinQ** button in the **Content pane** in VLAN setting window.

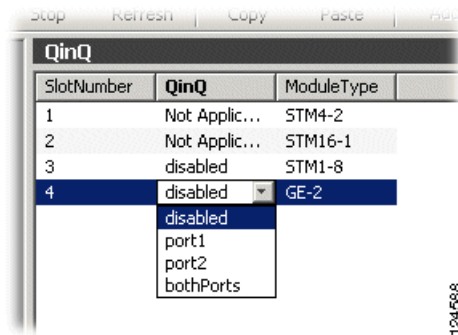
7.4.7 Provider VLAN



Available modules types with Q in Q available, are displayed:



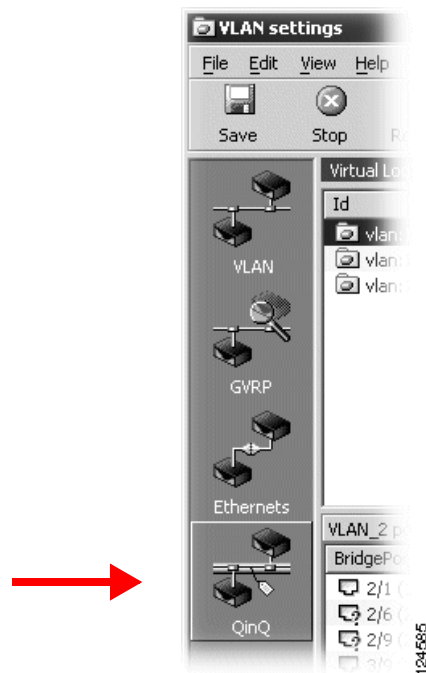
- Step 2** Click desired **module type**, in this example GigE-2-LC, and select Q in Q. Available choices in the pull-down menu (depending on selected module type) are; available ports, disable and enable.



- Step 3** Select port/enable (depending on module type) and click save.
- Step 4** Repeat for other network elements that are part of the desired Q in Q application. (Select **File>Reconnect** to access the other NE's).

7.4.7.11 Setting up Q in Q - ONS 15302

- Step 1** Click the **Qinq** button in the **Content pane** in VLAN setting window.



- Step 2** Select **Qinq**. Available choices in the pull-down menu; disable or enable.
- Step 3** Select enable and click save.
- Repeat for other network elements that are part of the desired Q in Q application. (Select **File>Reconnect** to access the other NE's)

7.5 Examples

These examples describe how to configure an IP Interface, Static route, Default route and RIP filter.

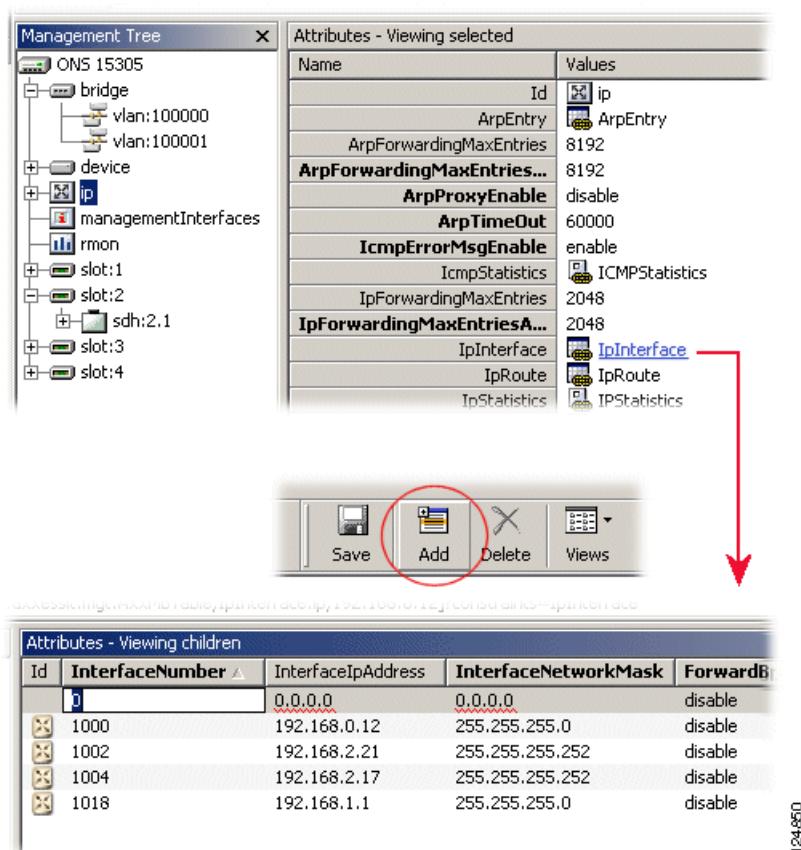
7.5.1 Configure an IP Interface

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).

Configure an IP interface with an IP address, [Figure 7-28](#).

- 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 7-28 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.

7.5.2 Configure 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.



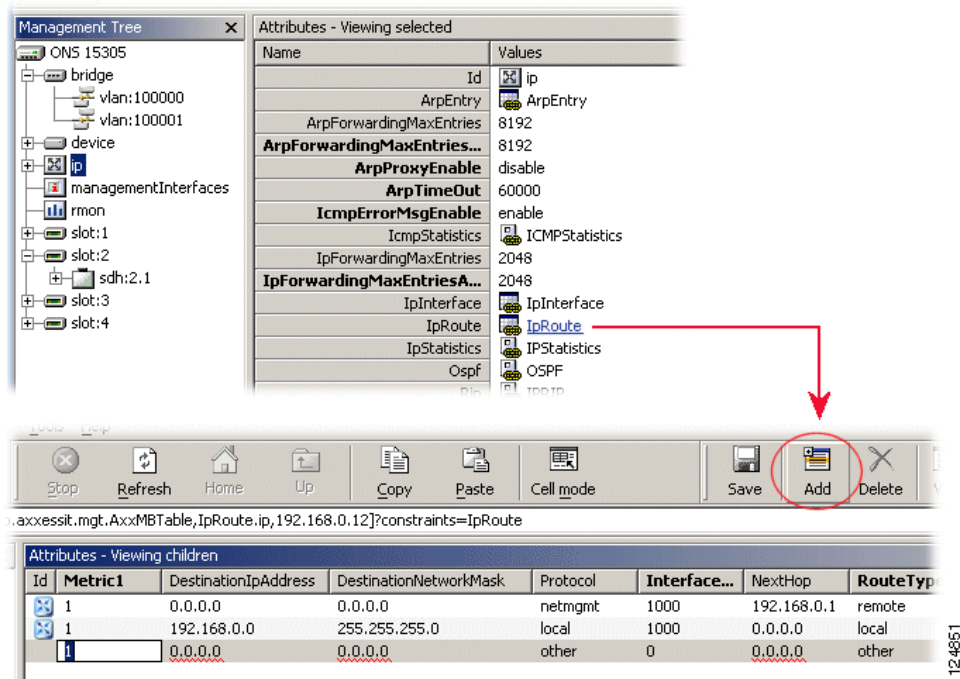
Note

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.

7.5.2.1 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 7-29](#).
- Step 2** Double click on the **ipRoute** attribute in the attributes window.
- Step 3** Click **Add** on the toolbar.

Figure 7-29 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.



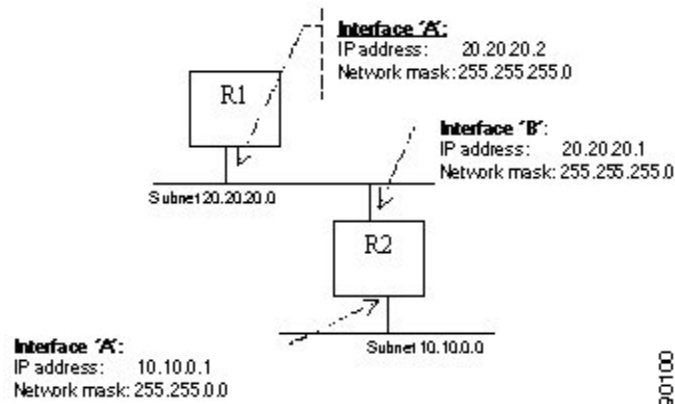
Note The value x set to the destinationNetworkMask attribute will be rejected by the network element if the bitwise logical-and of x with the value of the destinationIpAddress attribute is not equal to the value of the destinationIpAddress attribute.

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.

Example

To define a static route to the subnet 10.10.0.0 in router R1, [Figure 7-30](#).

Figure 7-30 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
-

7.5.2.2 Configure 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.

Example

To create a default route on router R1 using router R2 as default gateway, [Figure 7-30](#).

-
- Step 1** Set destinationIpAddress: 0.0.0.0

- Step 2** Set destinationNetworkMask: 0.0.0.0
 - Step 3** Set nextHop: 20.20.20.1
 - Step 4** Set interfaceNumber: ifIndex associated with interface 'A'.
 - Step 5** Set routeType: Remote
 - Step 6** Set metric: 1
-

7.5.3 Configure 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.

7.5.3.1 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.
-

Examples

To define a RIP global filter which 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.

7.6 Miscellaneous

This section describes OSPF and DHCP.

7.6.1 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.
-

7.6.1.1 Supported OSPF Areas: Transit and Stub Areas

Three OSPF 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-area and default routes, that means it is not possible to configure an area as a totally-stub area.

7.6.1.2 Configuring an OSPF Area

To configure a new OSPF area follow this Steps:

-
- 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.

7.6.1.3 Configuring an OSPF Interface

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, [7.6.1.2 Configuring an OSPF Area, page 7-38](#).
 - 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**.
-

7.6.1.4 Enabling OSPF on the Network Element

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**.
-

7.6.2 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, “[7.6.2.1 Configure the Range of IP Addresses for the DHCP Server](#)” section on page 7-39. 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, “[7.6.2.2 Configure the DHCP Server for Manual Allocation](#)” section on page 7-39.

7.6.2.1 Configure the Range of IP Addresses for the DHCP Server

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.

7.6.2.2 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

8.1 Introduction

This chapter describes the presentation of Performance Management (PM) data as they occur on the network element. The PM data available on the network element:

- G.826 performance data for the SDH paths and section termination points.
 - G.826 on Multiplex Section (MS), Regeneration Section (RS), Virtual Containers (VC).
 - Non-intrusive monitors on AU's and TUs cross- connected through the network element.
- Values of the various counters.
- RMON.

PM data can be monitored from the Management Tree. You can read the registered PM data on the network element, get it presented in performance management data tables. The file can be read, copied and/or edited in any tool, for instance MS Excel. It is possible to clear all PM data on the network element, see “Logs (Alarm Logs, Performance Data Logs)” on page -32.

8.1.1 Definitions

According to G.826 PM data, the following definitions are used:

- Errored second (ES)
 - A one second period with one or more errored blocks or at least one defect.
- Severely errored second (SES)
 - A one second period which contains $\geq 30\%$ errored blocks or at least one defect
- Background block error (BBE)
 - An errored block not occurring as a part of an SES
- Unavailable seconds (UAS)
 - A period of unavailable time begins at the onset of ten consecutive SES events. These ten seconds are considered to be part of unavailable time. A new period of available time begins at the onset of 10 consecutive non-SES events. These ten seconds are considered to be part of available time. UAS is the number of second of unavailable time.

This section describes:

- “Present G.826 PM data”
- “View Counters”

8.1.2 Present G.826 PM data

G.826 PM data is available in the network elements under management.

8.1.2.1 Background

The network elements have limited memory for historical data storage, and the oldest data will be removed in favour of new, current data registered to the network element¹.

G.826 specifies the accumulated performance data for 15 minutes and 24 hours periods. The incomplete data for the current 15 minutes period is also available. This is updated continuously on the network element. PM data is stored in time series measurement periods (for instance such as the last 15 minutes and the last 24 hours period) on the network element.

From Management Tree, you can select G.826 PM data for the following managed objects:

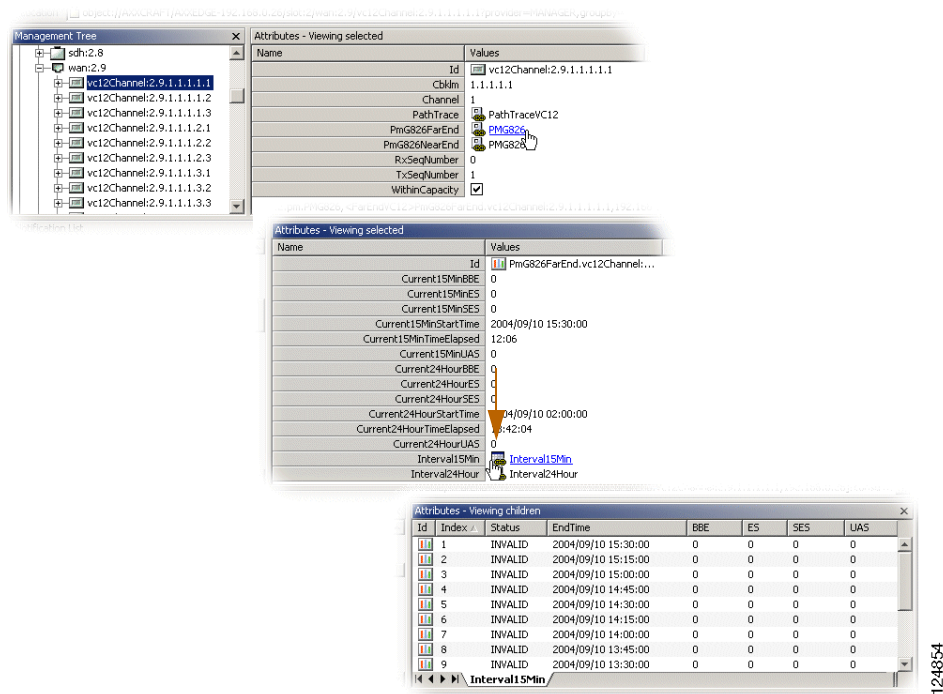
Table 8-1 *Managed Objects*

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

- None- intrusive monitors on AU's and TUs

Near End and Far End data apply to all managed object, except for the RS.

1. Time periods and interval may vary between the different network element types.

Figure 8-1 View PM - Example

With near end and far end data for all managed object except the RS. The 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 “[5.4.7 Monitoring PDH Port VC-n Performance](#)” section on page 5-12 and “[5.15.10 Monitoring WAN Port Performance](#)” section on page 5-66.

8.1.3 View Counters

From the Management Tree you can view all managed objects that are monitored objects, for instance:

- LAN ports
- WAN ports
- Bridge
- IP
- IPM
- IPX

8.1.4 Criteria for Counting Valid-data

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

8.2 Manage RMON

This section describes management of RMON (Remote Network Monitoring) within a network of Cisco network elements.

RMON is an IETF standard (RFC 2819) for monitoring the status of a network by activating probes/monitors at targeted ports in the network, and using RMON clients to collect and present the status information.

8.2.1 About Rmon Measurements In Cisco Network Elements

With Cisco RMON Management, the user can set up local monitoring devices (probes) at selected locations in the managed network. The RMON monitors perform data acquisition and local storage.

An RMON monitor can be set up to accumulate information (perform diagnostics and collect statistics) in local PM buffer, and to log PM associated events or to generate RMON traps to the management system. To collect information, the management system can either poll the monitors regularly or be notified by monitor notifications (SNMP traps), triggered by exception conditions.

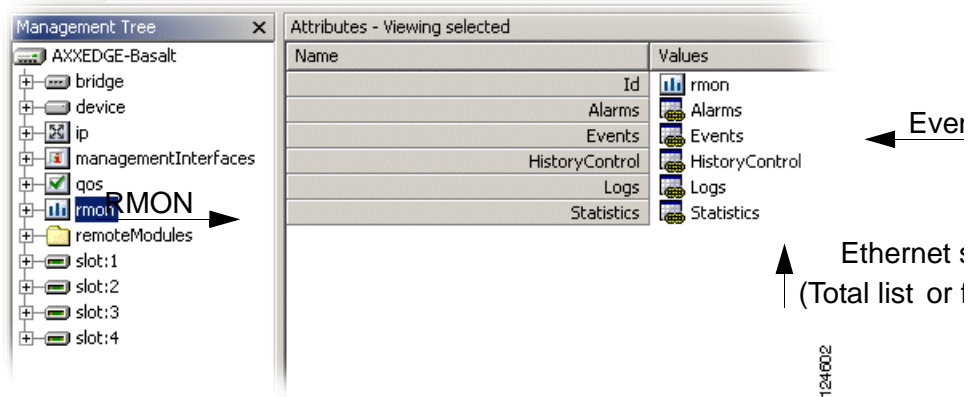
8.2.2 RMON Overview

Manage time series measurements on local area networks (LANs) and interconnecting E1/E3 lines from a central site with RMON. RMON uses monitoring probes to acquire and store measurements. Remote monitoring according to RMON needs management, and has to be set up specifically.

With RMON management you create RMON monitors, configuring measurement sessions, alarm conditions, logging and alarm generation, and acquire RMON data views.

- **Events** is used to define event types generated from the device.
- **Alarms** is used to set up alarm thresholds for RMON monitoring.
- **History Control** is used to set up the periodic sampling of information from the network element ports, and to configure RMON probes/ monitors.
- **Logs** is used to log selected events from RMON Events.
- **Statistics** contains statistics on each monitored ethernet interface on the network element.

Figure 8-2 RMON - GUI overview



The following sub- sections explain how to create, configure and inspect RMON monitor(s):

- “Create RMON History Monitor(s)”.
- “Create RMON Event Monitor”.
- “View RMON Data”.

8.2.3 Create RMON Event Monitor

This section describes how to create an RMON Event Monitor as follows:

- “Define RMON Event Types”.
- “Configure an RMON Event Monitor”
 - “Define A Monitor Source”
 - “Define detection criteria”

8.2.3.1 Define RMON Event Types

Set RMON event types prior to configuring RMON Event Monitors. Events are defined as entries in the **RMON Event Table**. You can choose between the following alternatives:

- Generate log entries (to **RMON Logs**)
- Generate RMON traps (to **Event Trace**, Notification List)
- A **combination** of Log entry and RMON traps (as illustrated in the following sections)

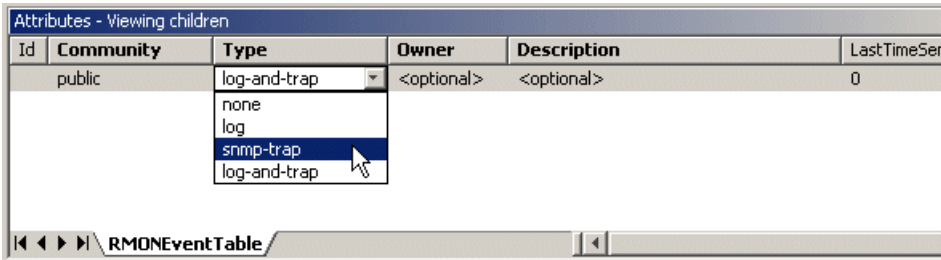
- Step 1

Add a new event to **RMON Event Table**.
- Step 2

Select event **Type** (here: Log entry and SNMP trap).
- Step 3

Enter **Community** string for communication with intended trap recipient.

Figure 8-3 RMON Events-GUI example



- Step 4

Enter an **Owner** (optional).
- Step 5

Enter a **Description** (optional).
- Step 6

Repeat the procedure for as many event definitions as desired.
- Step 7

Save event definition.


Note

The event Id is used in configuring RMON event monitors.

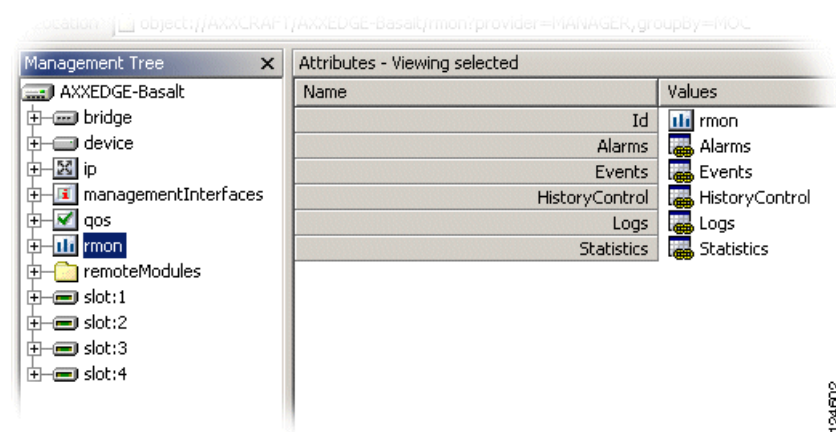
8.2.4 Configure an RMON Event Monitor

You configure RMON Event Monitor by defining the conditions for event generation from RMON Alarms. If editing an existing monitor, you select the desired table entry.

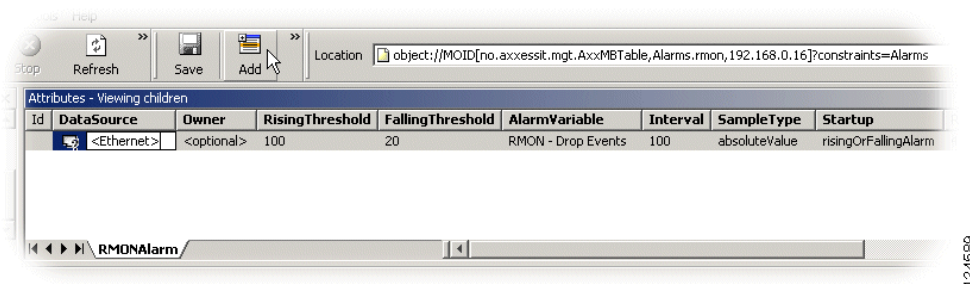
8.2.4.1 Define A Monitor Source

- Step 1

Select **Alarms** from RMON attributes.

Figure 8-4 Select RMON Alarms

Step 2 Add a new monitor entry to RMON Alarm table.

Figure 8-5 Add Monitor Entry

Step 3 Specify a LAN/ WAN port as **DataSource** for desired ethernet interface instance (Port if-index or BridgePortNumber.)

Step 4 Enter an **Owner** for monitor administration (optional).

Step 5 Select the port status to be used in detecting the alarm situation from **AlarmVariable** pull- down list.
Define detection criteria

Step 6 Set **Interval** for the periodic check for alarm conditions.

Step 7 Choose absolute values or delta values from **Sample Type** if the monitor checks alarm conditions (difference between last and current sample).

Step 8 Set the desired alarm **Startup** conditions:

This attribute defines the initial behavior of the monitor:

Alarms are generated if the monitor is in an alarm situation (below falling threshold or above rising threshold) at startup.

Alarm Rising Threshold (integer - number of occurrences).

The monitor triggers an event when the counter value rises above this level.

Alarm Falling Threshold (integer - number of occurrences).

The monitor triggers an event when the counter value sinks below this level.

Rising Event cross-reference.

A cross reference to the Event Table that identifies the event that is triggered when the monitor registers a rising threshold violation.

Falling Event cross-reference.
 A cross reference to the Event Table that identifies the event that is triggered when the monitor registers a falling threshold violation.

- Step 9

Save RMON event monitor configuration.

The network elements RMON monitor can start generating alarm events for selected ethernet interface.

8.2.5 Create RMON History Monitor(s)

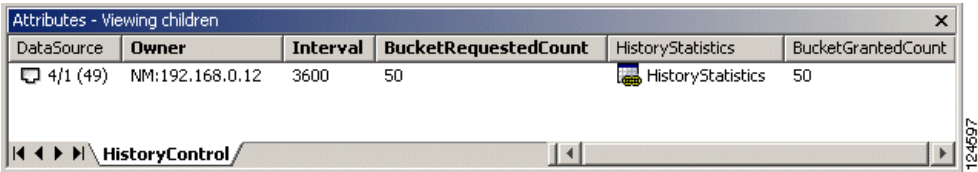
Sampling interval is as defined by the user. Sampling duration is as granted by the network element. Each sample contains the full set of RMON counter data associated with the data source.

An RMON historical monitor maintains both a 'current' and a 'historical' list of statistical data. History Statistics contains the periodical samples from one specific Ethernet interface instance.

- Step 1

Add a monitor for time series measurements in RMON History Control.

Figure 8-6 RMON History Monitor- example



- Step 2

Specify a LAN/ WAN port as **DataSource** for desired ethernet interface instance (Port if-index or BridgePortNumber.)
- Step 3

Enter an **Owner** (optional).
- Step 4

Set polling parameters for each data sampling:
Poll **interval** in seconds, or poll duration as number of polls in **BucketRequestedCount**.
- Step 5

Save RMON monitor configuration.
The network element starts monitoring historical data.
- Step 6

Inspect the poll duration of the RMON monitor from **BucketGrantedCount**.



Note

The monitored data is based on free-running sets of counters. RMON has no support for detecting counter overflow.

8.3 View RMON Data

RMON data is available for inspection in several RMON tables within the network element:

- **RMON Statistics** present statistics for each monitored ethernet interface. See “Inspection Of Current Statistical Data” on page -9.
- **RMON History Statistics** present time series of statistics measurements. See “Inspection of History Statistics Per Port” on page -10.
- **RMON Logs** contain logged events from each monitored interface. See “View logged events” on page -10.
- **RMON Traps** are presented in **CiscoEdgeCraft Event Trace** view. This information is not stored on the network element. See “Notification” on page -19.

You can manage several RMON Monitors in the network element at any time.

8.3.1 View Statistical Data

This section describes the following:

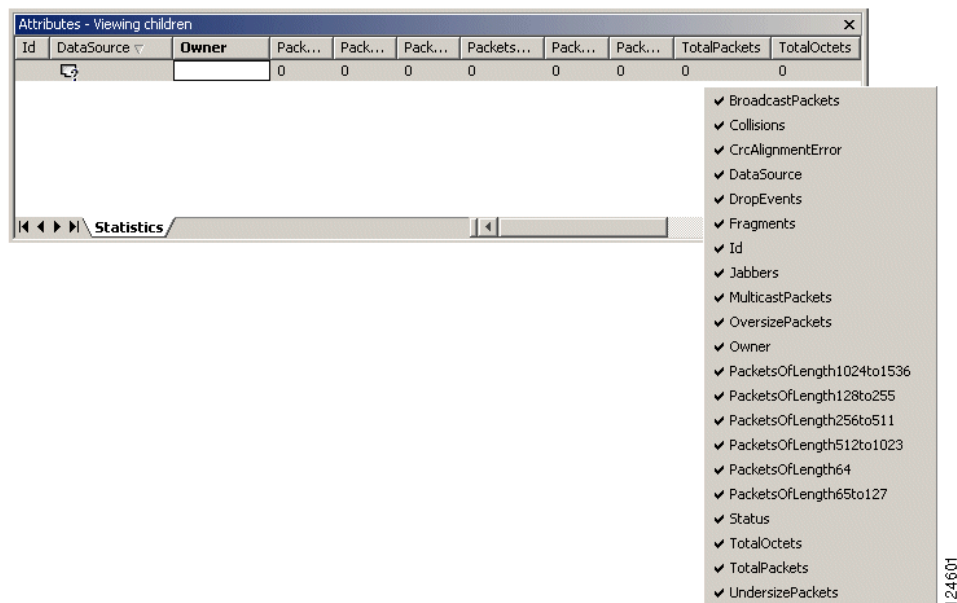
- “Inspection Of Current Statistical Data”.
- “Inspection of History Statistics Per Port”.

Presented RMON data can be printed to file.

8.3.1.1 Inspection Of Current Statistical Data

- Step 1** Press **RMON** in Management Tree.
- Step 2** Select **Statistics** from RMON attributes.

Figure 8-7 RMON Statistics- GUI overview



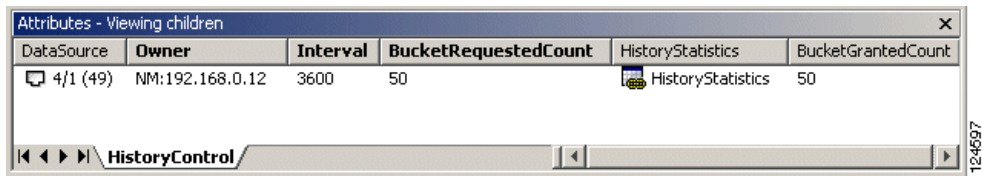
The current statistical information of all monitored interfaces for all monitored ports will be presented.

Step 3 Customize visible columns from right- click menu (optional).

8.3.1.2 Inspection of History Statistics Per Port

Step 1 Select **History Control** from RMON attributes. RMON statistical time series table view for all history monitors and to all the ports is presented.

Figure 8-8 Select History Control



Step 2 Select the **RMON history monitor** for LAN/ WAN interface you want to inspect.

Step 3 Press **History Statistics** link to view the RMON statistical time series for that specific port.

Figure 8-9 RMON History statistics - example

Attributes - Viewing children									
Id	Fragments	Broadcast...	MulticastP...	Utilization	DropEvents	Undersize...	CrcAlignm...	IntervalSt	
etherHistoryEntry:1.72	465976	0	0	0	6144	0	131336450	25921294	
etherHistoryEntry:1.73	0	0	0	0	34156028	0	131336450	26281294	
etherHistoryEntry:1.74	597026	0	0	0	34155608	0	3767104	26641294	
etherHistoryEntry:1.75	34155504	0	0	2004	34155448	0	36866	27001294	
etherHistoryEntry:1.76	0	1	34155496	0	34155472	0	1	27361294	
etherHistoryEntry:1.77	0	0	3862684	2	0	0	3863068	27721294	
etherHistoryEntry:1.78	34155780	0	0	521	0	0	5034680	28081294	
etherHistoryEntry:1.79	0	8704	1	0	36866	34155624	33587184	28441294	
etherHistoryEntry:1.80	0	3818928	0	0	36866	0	33587112	28801294	
etherHistoryEntry:1.81	0	3818928	0	0	36866	0	33587112	29161294	
etherHistoryEntry:1.82	0	3818928	0	0	36866	0	33587112	29521294	
etherHistoryEntry:1.83	0	3818928	0	0	36866	0	33587112	29881294	
etherHistoryEntry:1.84	0	3818928	0	0	36866	0	33587112	30241294	
etherHistoryEntry:1.85	0	3818928	3818928	0	36866	3	36866	30601294	
etherHistoryEntry:1.86	0	3818928	3818928	0	36866	3	36866	30961294	

8.3.2 View logged events

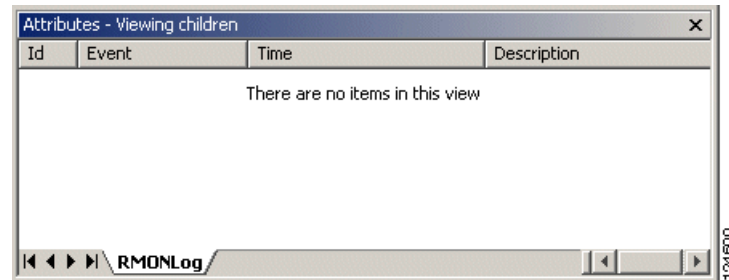
How to view logged events:

8.3.2.1 Inspection of the Event Log

If the event monitor is configured to log events locally, you can inspect this in the RMON Logs.

Step 1 Select **Logs** from RMON attributes.

All events logged by all monitors within the selected network node will be presented.

Figure 8-10 RMON Logs-view

8.3.2.2 Inspection of the Event Log

Inspect events filtered for a specific LAN/ WAN port.

-
- Step 1** Select desired RMON monitor from **RMON Alarms**.
- Step 2** Open **RMON Event** logs from **Rising Event** and/ or **Falling events**.

Figure 8-11 Alarm monitor- example

DataSource	Startup	RisingEventIndex	RisingEvent	FallingEventIndex	FallingEvent	Value
1/1 (1)	risingOrFallingAlarm	4	RMONEvent	4	RMONEvent	0

A filtered table view of the Event Log will be presented, containing all events associated by the selected monitor. All logged events are presented with timestamp and description fields.

Figure 8-12 RMON Event log to alarm monitor-view

Name	Id	Community	Description	LastTimeSent	Owner	Type
RisingEvent.alarmEntry:4						

8.3.2.3 Delete RMON Monitor

-
- Step 1** Select desired **monitor** (Alarms or History) in the relevant RMON table.

Step 2 Press **Delete**.

RMON monitor (and any RMON event definitions) is removed in from the network element.

RMON data presentation is closed on your desktop. When deleting RMON monitors, the associated log table entries (History Statistics, Event Log entries) are removed automatically.



Troubleshooting and FAQ

Question one handles troubleshooting and FAQ from [Chapter 4, “General Management”](#).

Question two to four handle troubleshooting and FAQ from [Chapter 5, “Traffic Port Management”](#).

Question six to eleven handle troubleshooting and FAQ from [Chapter 7, “Layer 2 Configuration”](#).

Question 1

- Q.** How can I 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 9-1 VLAN calculation

$$(\text{max number multicast entries}) = 4000 - (\text{max number VLANs})$$

89199

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.

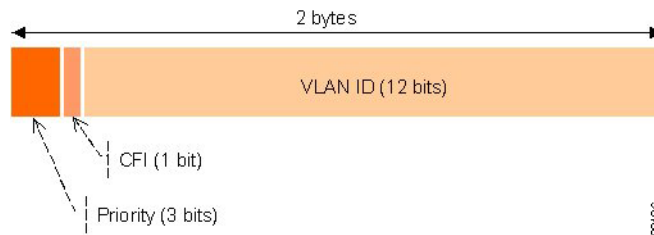
Question 8

- 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 9-2](#).



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 9-2 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:

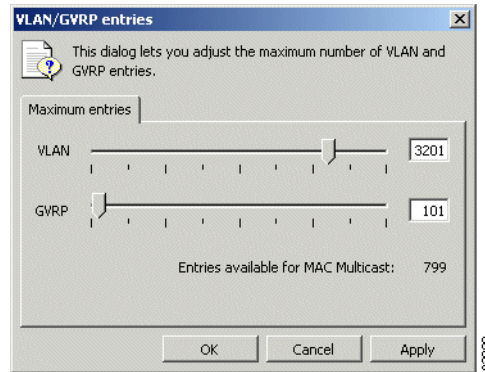
The number of all static VLANs both currently configured and expected to be configured.

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.

Increasing 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

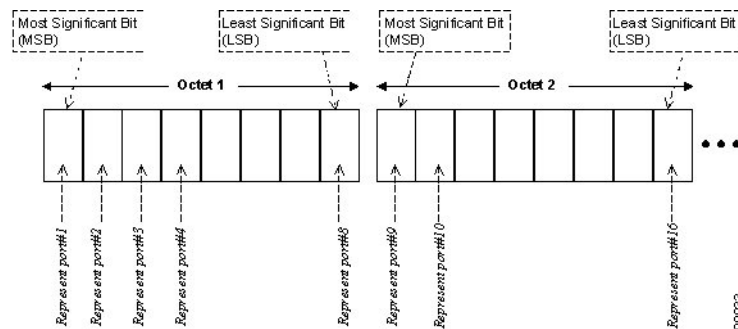
-
- Step 1** Click **Properties** in the VLAN Settings window.
- Step 2** The appearing dialog allows you to adjust the maximum number of VLAN and GVRP entries.

Figure 9-3 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 9-4](#). 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 9-4 Definition of a set of ports through an octet string

[Table 9-1](#) presents two examples of octet strings and their corresponding sets of ports.

Table 9-1 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 9-5](#).

Figure 9-5 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 9-2](#).

Table 9-2 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



GLOSSARY

A

ADM	Add/drop multiplexer
AIS	Alarm indication signal
APS	Automatic protection switching
ARP	address resolution protocol
ASBR	Autonomous system border router
AU-x	Administrator Unit - x

B

BBE	Background block error
BER	Bit error rate

C

CBKLM	Addressing schema for data container
CFI	Canonical format indicator
CPE	Customer premises environment
CTP	Connection termination port
CTS	Clear to send

D

DNU	Do not use
DEG	Degraded signal effect
DCC	Data communications channel

DCN Data communications network

DHCP Dynamic host control protocol

E

EMS Element management system

ETS European Telecommunications Standard

ETSI European Telecommunications Standards Institute

ES Errored seconds

F

FCC Federal Communications Commission

G

GARP Generic attribute registration protocol

GUI Graphical user interface

GW Gateway

GVRP Generic attribute registration protocol VLAN registration protocol

H

HTML Hypertext markup language

I

IANA Internet assigned numbers authorit

ID Identifier

IEC International Electrotechnical Commission

IEEE Institute of Electrical and Electronics Engineers

IF-DN-0101-R1 Network and service forum (NSIE) standard for IP over DCC

IGMP	Internet group management protocol
IP	Internet Protocol
IPX	Internetwork packet exchange protocol
IS	Intermediate system
ISDN	Integrated services digital network
ISO	International standard organization
ITU	International Telecommunications Union
ITU-T	International Telecommunications Union, Telecommunication standards sector

L

L1 IS	Layer 1 intermediate system
L2 IS	Layer 2 intermediate system
LAP-D	Link access procedure on the D channel
LAN	Local area network
LED	Light emitting diode
LLC	Logical link control layer
LL2/LL3	Local loop 2/3
Log4j	Tool for logging from jakarta.apache.org
Los	Loss of signal

M

MAC	Medium access
Mbps	Megabits per second
MHz	Megahertz
MIB	Management information base
MO	Managed Objects
MS	Multiplex section
MSP	Multiplex section protection

N

NC	not connected
NE	Network element
NET	Network
NMS	Network management system
NSAP	Network Service Access Point
NSSA	Not-so-stubby areas

O

ONS	Optical networking system
ONCLI	Optical networking system command line interface
OSPF	open shortest path first

P

PC	Personal Computer
PDH	Plesiochronous digital hierarchy (ITU-T Rec. G.702)
PIM	Protocol independent multicast
PIM-DM	Protocol independent multicast - Dense mode
PM	Performance monitoring
PPP	Point-to -point protocol
PRC	Primary reference clock

Q

QL	Quality Level
QLM	Quality Level minimum

R

RFC	Request for comments
RIP	Routing information protocol
RJ-45	Registered jack #45 (8-pin)
RS Layer	Regenerator section layer
RSTP	Rapid spanning tree protocol
RMON	Remote monitoring
Rx	Receive

S

SAP	Server advertisement protocol
SASE	Stand alone synchronization equipment
SEC	SDH equipment clock
SES	Severely errored second
SDH	Synchronous digital hierarchy
SNAP	Subnetwork access protocol
SNC	Sub-network connection
SNC/I	Sub-network connection inherent monitoring
SNC/N	Sub-network connection on-intrusive monitoring
SNMP	Simple network management protocol
SNTP	Simple network timing protocol
SSU	Synchronisation supply units
SSM	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
-----------	---------------