

NetHorizon User's Guide

For software version ZMS 3.2

Aug 2017

Document Part Number: 830-00741-63

DASAN Zhone Solutions, Inc
7195 Oakport Street
Oakland, CA 94621
USA
510.777.7000
www.dasanzhone.com
info@dasanzhone.com

**COPYRIGHT C2000-2017 DASAN Zhone Solutions, Inc. and its licensors.
All rights reserved.**

This publication is protected by copyright law. No part of this publication may be copied or distributed, transmitted, transcribed, stored in a retrieval system, or translated into any human or computer language in any form or by any means, electronic, mechanical, magnetic, manual or otherwise, or disclosed to third parties without the express written permission from DASAN Zhone Solutions, Inc.

Bitstorm, EtherXtend, EZ Touch, IMACS, MALC, MXK, Raptor, SLMS, Z-Edge, Zhone, ZMS, zNID and the Zhone logo are trademarks of DASAN Zhone Solutions, Inc.

DASAN Zhone Solutions makes no representation or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability, non infringement, or fitness for a particular purpose.

Further, DASAN Zhone Solutions reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation of DASAN Zhone Solutions to notify any person of such revision or changes.

ABOUT THIS GUIDE

Zhone Management System (ZMS™) is the network management system that provides service-to-subscriber management for Zhone™ local loop network elements, including Broadband Access Node (BAN™), Multi-Access Line Concentrator (MALC™), Raptor, Sechtor™ 100A, Z-Edge™, MXK™.

NetHorizon™ is the application that operators use to navigate, monitor, and manage objects in their ZMS networks.

Audience

This guide is written for the operator who runs NetHorizon to manage ZMS objects and subscribers. As a reader of this guide, you should be familiar with basic networking components such as network devices, cards, physical ports, logical interfaces, and permanent virtual circuits (PVCs). You should also be familiar with network management tasks such as configuring network components, managing subscribers, managing network faults, and monitoring network performance.

Document organization

This guide contains the following information:

Read	To learn about
Chapter 1 Getting Started	Basic tasks such as navigating the system and accessing information about network objects.
Chapter 2 Provisioning Devices with NetHorizon	Using NetHorizon to configure network objects.

Style and notation conventions

The following conventions are used in this document to alert users to information that is instructional, warns of potential damage to system

equipment or data, and warns of potential injury or death. Carefully read and follow the instructions included in this document.



Caution: A caution alerts users to conditions or actions that could damage equipment or data.



Note: A note provides important supplemental or amplified information.



Tip: A tip provides additional information that enables users to more readily complete their tasks.



WARNING! A warning alerts users to conditions or actions that could lead to injury or death.



WARNING! A warning with this icon alerts users to conditions or actions that could lead to injury caused by a laser.

Typographical conventions

The following typographical styles are used in this guide to represent specific types of information.

Bold	Used for names of buttons, dialog boxes, icons, menus, profiles when placed in body text, and property pages (or sheets). Also used for commands, options, parameters in body text, and user input in body text.
Fixed	Used in code examples for computer output, file names, path names, and the contents of online files or directories.
Fixed Bold	Used in code examples for text typed by users.
<i>Fixed Bold Italic</i>	Used in code examples for variable text typed by users.
<i>Italic</i>	Used for book titles, chapter titles, file path names, notes in body text requiring special attention, section titles, emphasized terms, and variables.
PLAIN UPPER CASE	Used for environment variables.
Command Syntax	Brackets [] indicate optional syntax. Vertical bar indicates the OR symbol.

Related documentation

Refer to the following publications for additional information:

OSS Gateway User's Guide describes how to install, configure, and use the OSS gateway application.

OSS Gateway Reference Guide describes the OSS Gateway configuration, performance, and notification attributes.

OSS Gateway Release Notes contains the most current product information and requirements.

MALC Hardware Installation Guide describes how to install the Multi-Access Line Concentrator.

MALC Configuration Guide describes how to provision the Multi-Access Line Concentrator.

MALC Release Notes contain the most current product information and requirements.

MXK Hardware Installation Guide describes how to install the MXK.

MXK Configuration Guide describes how to provision the MXK.

MXK Release Notes contain the most current product information and requirements.

Raptor XP Hardware Installation and Configuration Guide describes how to install and configure the Raptor XP.

Raptor XP Release Notes contains the most current product information and requirements.

Raptor Hardware Installation and Configuration Guide describes how to install and configure the Raptor.

Raptor Release Notes contains the most current product information and requirements.

ZMS Administrator's Guide describes how to configure the ZMS system, including the ZMS client application, and describes how to administer user accounts.

ZMS Release Notes contains the most current ZMS product information and requirements.

ZMS Installation Guide describes how to install the various components of the ZMS system.

Contacting Global Service and Support

If your product is under warranty (typically one year from date of purchase) or you have a valid service contract, you can contact Global Service and Support (GSS) for questions about this or other Zhone products, or for Technical Support or Hardware Repairs.

Before contacting GSS, make sure you have the following information:

- Zhone product you are using
- System configuration
- Software version running on the system
- Description of the issue
- Your contact information

If your product is not under warranty or you do not have a valid service contract, please contact GSS or your local sales representative to get a quote on a service plan. You can view the options on our web site at

<http://www.zhone.com/support/services/warranty>.

Technical support

The Technical Assistance Center (TAC) is available with experienced support engineers who can handle questions, assist with service requests, and help troubleshoot systems.

Hours of operation	Monday - Friday, 8 a.m. to 5 p.m, Pacific (excluding U.S. holidays)
Telephone (North America)	877-ZHONE20 (877-946-6320)
Telephone (International)	510-777-7133
E-mail	support@zhone.com
The Web is also available 24 x 7 to submit and track Service Requests (SR's)	www.zhone.com/support

If you purchased the product from an authorized dealer, distributor, Value Added Reseller (VAR), or third party, contact that supplier for technical assistance and warranty support.

Hardware repair

If the product malfunctions, all repairs must be authorized by Zhone with a Return Merchandise Authorization (RMA) and performed by the manufacturer or a Zhone-authorized agent. It is the responsibility of users requiring service to report the need for repair to GSS as follows:

- Complete the RMA Request form (<http://www.zhone.com/account/sr/submit.cgi>) or contact Zhone Support via phone or email:
Hours of operation: Monday Friday, 6:30am-5:00pm (Pacific Time)
E-mail: support@zhone.com (preferred)
Phone: 877-946-6320 or 510-777-7133, prompt #3, #2
- Provide the part numbers and serial numbers of the products to be repaired.
- All product lines ship with a minimum one year standard warranty (may vary by contract).
- Zhone will verify the warranty and provide the customer with a repair quote for anything that is not under warranty. Zhone requires a purchase order or credit card for out of warranty fees.

CONTENTS

About This Guide	3
Audience	3
Document organization	3
Style and notation conventions	3
Typographical conventions	4
Related documentation	5
Contacting Global Service and Support	6
Technical support.....	6
Hardware repair	7
Chapter 1 Getting Started	25
Introduction	25
About your NetHorizon account	26
Logging into NetHorizon	26
Viewing information about your NetHorizon account.....	27
Creating operator accounts.....	28
Logging in as a newly created operator.....	29
Navigating the system	30
Tree display.....	30
Graphical display	31
Equipment display: viewing card status	33
Map display: zooming in and out of views	34
Navigating through objects in the graphical display	35
To reposition objects in your map display:	35
Navigating through views	35
Navigating a tree	36
Navigating a graphical display	36
Launching multiple display windows	36
Launching multiple display windows:	36
Using the message console window	37
Updating your display.....	38
Updates following adds and deletes	38
Updates following action parameter changes.....	38
Updates following synchronization.....	38
Updating an object and its children	39

Updating the entire display	39
Using the menu bar	39
Using the toolbar	45
Changing your NetHorizon password	46
To change your NetHorizon password:	46
Accessing online Help	46
 Chapter 2 Provisioning Devices with NetHorizon	 49
Basics	50
Adding maps and changing the default ZMS map	50
Adding a region or subregion	53
Navigating regions and subregions	54
Modifying a region or subregion	54
Deleting a region or subregion	55
Adding a device	55
Autodiscovering devices	56
Deleting a device	57
Managing a device	58
Finding a device	58
Moving a device to a different region or subregion	58
Finding an object	59
Finding a port by its serial number	61
Locating a device in the network using its MAC address	61
Adding topology links to ZMS maps	61
Using the message console window	62
Selecting templates	62
ZMS Web Client Launch	63
Chassis procedures	63
Templates	63
Device	63
Management	64
Services	64
Software images	64
SNMP configuration	64
Adding an SNMP community name	64
Deleting an SNMP community name	65
Adding an SNMP access list	66
Configuring a trap forwarding address	66
Adding a trap forwarding address	67
Viewing a trap forwarding addresses	67
Deleting a trap forwarding address	68
Device configuration	68
Downloading files to a single or multiple devices	70
Downloading a software image to a single or multiple devices	71
Performing hitless software upgrades	74
Backing up configurations	75

Performing immediate configuration backup on a single device	75
Setting backup device configurations.....	76
Flashing the software image	77
Upgrading a device using ZMS	78
Editing a configuration.....	79
Rebooting a device	80
Restoring a configuration	80
Performing immediate synchronization with a single device	81
Performing scheduled synchronization with a single device or multiple devices.....	82
Configuring device identity	82
Configuring device administration settings.....	82
Configuring MXK user privilege management.....	83
Configuring MXK users in bulk	83
View the MXK users of selected devices.....	83
Add a MXK user to selected device(s).....	84
Modify a MXK user of a selected device.....	84
Change the password for the MXK users have same username on different devices	84
Delete the MXK users from devices	84
Configuring shelf inventory manager.....	85
Enabling or disabling secure mode on device	85
Configuring port access security	85
Configuring device alarm level settings (alarm suppression)	87
Configuring ZMS connectivity settings	87
Configuring device community names.....	87
Configuring device access lists	88
Configuring device trap configuration settings	88
RADIUS Configuration	88
Configuring user authentication method	89
Configuring RADIUS client profiles	90
Configuring RADIUS index.....	91
Configuring device location settings.....	92
Configuring voice DSP settings	92
Configuring DSCP to COS (802.1p)	93
Viewing or Modifying DSCP to CoS mapping.....	93
Assigning DSCP to COS mapping to MXK	93
Assigning DSCP to COS mapping to an Unified Service Provisioning CPE	94
Configuring device video source settings	95
Configuring device system clock settings.....	95
Configuring device NTP configuration settings.....	95
Configuring device bulk statistics configuration settings	95
Configuring device global STP parameters.....	96
Configuring GigaMux 1600/3200 device settings	97
Configuring CPE device settings	98
Adding CPE.....	99
Adding CPE by CPE manager.....	100
Adding CPE with a static IP address.....	100
Initializing a CPE	101
Initializing a CPE	101
Downloading file to a CPE	101

Downloading file to EtherXtend 30xx/31xx and SkyZhone	101
Downloading file to EtherXtend 33xx/34xx that with an IP address	102
Downloading file to EtherXtend 33xx/34xx that are managed by CPE manager 102	
Downloading software to a CPE	103
Downloading software to EtherXtend 30xx/31xx and SkyZhone	103
Downloading software to EtherXtend 33xx/34xx that with an IP address	103
Downloading software to EtherXtend 33xx/34xx that are managed by CPE manag- er	104
Activating software on a CPE	105
Activating software on a CPE	105
Upgrading software on a CPE	105
Upgrading software on a CPE	105
Executing configure script on a CPE	105
Executing configure script on a CPE	106
Backing up database on a CPE	106
Backing up database on a CPE	106
Restoring database on a CPE	106
Restoring database on a CPE	106
Synchronizing alarms on a CPE	107
Telnetting a CPE	107
Launching CPE WebUI on a CPE	107
Launching secured CPE WebUI on a CPE	107
CPE Manager Enhancements - Bulk Operations	107
Downloading file to CPEs	108
Downloading software to CPEs	108
Activating software on CPEs	108
Upgrading software on CPEs	109
Executing script on CPEs	109
Backing up CPE databases on CPEs	110
Automatic Web Cut-through to ZMS	110
Configuring EZ Touch Provisioning™ CPEs	110
EZ Touch Provisioning™ Overview	111
Adding EZ Touch CPE by CPE Manager	113
Adding download servers for CPE Configuration Manager	115
Creating CPE Configuration Manager	116
Adding CPE Configuration Manager Member to CPE Configuration Manager Group	118
Viewing CPE Configuration Manager Member runtime details	119
Configuring Malc XP device settings	119
Configuring Raptor XP device settings	120
Configuring MXK device settings	120
Configuring 1U MX-150 device settings	120
Configuring 1U MX-160, MX-161, MX-162 device settings	121
Configuring 1U MX-180, MX-280 device settings	121
Configuring 1U MX-260, MX-261, MX-262 device settings	121
Configuring 1U MXP-150 device settings	122
Configuring 1U MXP-160, MXP-260 device settings	122
Configuring 1U MXP-180, MXP-280 device settings	123
Configuring 1U MXK-194, MXK-198 device settings	123

Secure Shell (SSH).....	124
Configurable Temperature Alarm Severity and Ranges	124
Create vdsl-vect-config.....	125
View vdsl-vect-config attributes	125
Viewing the vdsl-vect-config attributes	125
vdsl-vect-config profile configuration.....	129
Card configuration	130
Adding a single card.....	131
Adding multiple cards	132
Enabling a card.....	133
Adding redundant MALC, MXK and Raptor cards	133
Modifying redundant MALC, MXK, or Raptor cards	134
Modifying card configurations.....	135
Rebooting a single card	136
Viewing card state	136
Setting the card default image	137
Deleting a card.....	138
Deleting a software image.....	138
Configuring a clock source.....	139
Viewing clock source status	140
Shelf monitoring.....	140
Network Time Protocol	141
Changing VCL rates	141
Creating an ATM VPI profile	143
Modifying a card's ATM bandwidth settings	144
Modifying GigaMux 1600/3200 card configurations	145
Modifying EFM SHDSL card configurations	145
Port status	146
Configuring port status.....	146
Port configuration	147
Physical port templates	148
Creating DSL port templates.....	149
Creating DSL alarm profile templates.....	149
Creating HDSL2 config profile templates.....	150
Creating SDSL port templates.....	150
Creating SHDSL port templates.....	151
Creating ADSL port templates.....	151
Creating ADSL Alarm templates	152
Creating ADSL Configuration templates	152
Creating POTS physical templates.....	153
Creating POTS FXS config templates.....	154
Creating EBS physical templates	154
Creating ISDN Bri physical port templates.....	155
Creating ISDN Bri alarm profile templates.....	155
Creating ISDN Bri Ulc configuration templates	156
Creating T1 physical templates	156
Creating E1 physical port templates.....	157
Creating T1 ATM physical port templates.....	157
Creating E1 ATM physical port templates.....	158

Creating VDSL physical port templates.....	158
Creating VDSL alarm profile templates.....	159
Creating VDSL configuration profile templates	159
Applying physical port templates to a port	160
Changing administration status of ports	160
Subscriber ID/ Port description.....	161
Modifying description field.....	161
Configuring ULC card physical ports	162
Configuring Uplink-OC3C/STM1-ATM/IP card physical ports	162
Configuring OC12 Uplink card physical ports.....	162
Configuring BPON OLT card physical ports.....	162
Configuring BPON ONT/ONU.....	163
Configuring 4-wire SHDSL card physical ports	163
Configuring ADSL card physical port	163
Modifying ADSL Port Configuration	163
Modifying ADSL2+ Phy-R™ parameters	167
Modifying ADSL2+ Cabinet mode.....	169
Configuring VDSL card physical ports	171
Configuring VDSL physical ports.....	171
Enabling G.INP	171
Configuring T1/E1 physical ports	178
Configuring G.SHDSL physical ports.....	179
Viewing EtherXtender Performance Statistics.....	180
Configuring Malc XP/ Raptor XP physical ports.....	180
Configuring Link aggregation and LACP.....	181
Link Aggregation	181
Link Aggregation Control Protocol (LACP).....	182
Prepare the uplink card for link aggregation	182
Changing the LACP aggregation mode.....	183
Creating a link aggregation group on a uplink card	183
Creating a link aggregation group on a Active Ethernet card	184
Deleting a link aggregated group	184
Link resiliency	185
Configuring interfaces for link aggregation	185
Bridge configurations	185
Interface configurations.....	185
Ethernet redundancy	186
Configuring Ethernet line redundancy	187
Removing a redundant Ethernet port.....	187
Disable standby transmit on Standby AE ports.....	188
Switchover from active to standby Ethernet port.....	188
Ethernet redundancy configuration limitations	188
Concurrent uplinks on the MXK 2.2.x.....	189
Settable alarm severity for Ethernet ports.....	190
Changing the alarm severity level for one Ethernet port.....	190
Bond groups.....	190
EFM, N2N bond groups	190
Adding an EFM/N2N bond group.....	190
Gbond bond group.....	192
Adding a Gbond group.....	194

Adding bridge on a Gbond group.....	195
Multiple Links for PPP (MLPPP) bond group.....	196
Creating MLPPP bond groups.....	196
Deleting bond groups	197
Offering an IP address to the far end IAD using host add	198
Offering an IP address to the far end using interface add	199
Configuring RPR ports.....	200
Configuring GigaMux ports	201
Configuring Talk Battery Disconnect on the POTS port	201
SFP/XFP Information	202
Viewing SFP/XFP Info	202
GPON configuration	202
Configure GPON OLT ports.....	203
Modifying GPON OLT ports	203
Configure GPON ONU/ONT	203
.....	203
Configure GPON type B redundancy	204
Configuring GPON line redundancy.....	205
Removing a redundant OLT port	205
Switchover from active to standby GPON OLT port.....	205
GPON redundancy configuration limitations.....	206
Activate ONT/ONUs by assigning serial number	207
Activating ONT/ONUs.....	207
Viewing unassigned serial numbers on the MxK	207
Change ONT/ONU serial number format (Hexa-decimal or Decimal).....	208
Display ONT/ONU MAC address	208
Received Signal Strength Indication (RSSI) and Digital Diagnostic Monitoring (DDM)	
209	
Viewing the received power on an OLT from an ONT/ONU.....	209
Viewing the transmit parameters on an OLT	209
GPON High and Low Receive Power Threshold Alarms	210
Configuring GPON high and low received power threshold alarms.....	211
Configure GPON ONT/ONU GEM Ports	211
Configuring GEM port general settings	212
Modifying GEM port upstream bandwidths and traffic class settings when activat-	
ing ONT/ONU (MALC only)	213
Modifying the alloc-ID profile on the static GEM port (MALC only).....	213
Creating a dynamic GEM port with a GEM traffic profile (Smart OMCI on MXK	
only).....	214
Bandwidth allocation	216
Configure GPON traffic profile	216
Creating a GPON Traffic Profile.....	216
Dynamic Bandwidth Allocation (DBA)	217
Configuring DBA in the GPON traffic profile.....	218
Viewing the bandwidth allocation on a GPON physical port	219
Viewing the allocation Ids information on a GPON physical port	219
Connection Admission Control (CAC) validation during creation of bridge/host on	
the ONT/ONU GEM port	219
Enable ONT/ONU web interface.....	220

Enabling ONT/ONU web interface	220
View SFP presence	220
Viewing SFP presence.....	220
Rogue ONU detection and rogue ONU alarms.....	221
Configuring ONU Detection	222
GPON OMCI configuration	223
OMCI file (MALC only)	223
Downloading an OMCI file.....	224
Associating the OMCI file when activating the ONT/ONU	224
Associating the OMCI file with an activated ONT/ONU	225
Smart OMCI - OMCI profiles (MXK only)	225
Configure Smart OMCI on ONU	225
Creating ME profile.....	225
Creating Generic profiles	226
Creating Specific profiles on OLT level	227
Creating Specific profiles on ONU level	228
Activating ONT/ONU with OMCI profiles	229
Import and export OMCI profile file.....	230
Importing and exporting ME profile file.....	230
Importing and exporting Generic profile file	231
Importing and exporting Specific profile file.....	231
Manage ONT/ONU with OMCI (MXK, MXK 194/198 only).....	232
Viewing or changing trap reporting status on ONT/ONU	233
Retrieving alarm information on ONT/ONU	234
Viewing the ONT/ONU specific OMCI alarms.....	234
Viewing OMCI alarms on the ONT/ONU subscriber ports.....	234
Viewing OMCI status on ONT/ONU.....	234
Configuring subscriber ports on ONT/ONU	235
Re-syncing changes to a single ONT/ONU	236
Re-syncing changes to ONT/ONUs	236
Applying changes to a single ONT/ONU (Smart OMCI Only).....	236
Applying changes to multiple ONT/ONUs (Smart OMCI Only)	237
Rebooting a single ONT/ONU	237
Rebooting multiple ONT/ONUs	237
Performing immediate upgrade on a single ONT/ONU.....	237
Performing immediate/scheduled upgrade on multiple ONT/ONUs	239
Viewing or deleting scheduled ONT upgrades	241
Performing auto upgrade on an ONT/ONU	241
Viewing ONT/ONU upgrade status on an OLT.....	242
Enabling upstream multicast video support	243
OMCI Statistics (MXK, MXK 194/198 only)	243
Unified Service Provisioning - CPE profiles (MXK, MXK 194/198 only) ...	244
Dynamic OMCI	244
Provision MXK upstream services.....	245
Create service related GPON additions.....	245
Provision Dynamic OMCI GPON with internal ME profile.....	245
Specifying internal ME profile for the ONU.....	246
Provision per subscriber downstream MXK bridges and CPE connections with Dy- namic bridging	246

Creating CPE traffic management profiles	247
Creating MXK bridge and CPE connections for different services	249
Deleting a MXK bridge and associated CPE connections	251
Provision services with CPE Profiles	251
Creating CPE video access control (optional).....	253
Creating CPE video profile and associate it with a CPE video access control list (optional).....	254
Creating a CPE IP server profile (i.e. CPE IP common profile)	255
Creating CPE VoIP server profiles	257
Creating CPE SIP dial plans for a SIP VoIP server (optional)	259
Creating CPE VoIP features profile for SIP or SIP PLAR	259
Creating CPE VoIP media profile	260
Creating a CPE PWE common profile	261
Creating CPE Ethernet subscriber profile (optional)	262
Creating CPE VoIP subscriber profile and associate it with a VoIP server, a VoIP features profile, and a media profile	264
Creating a CPE IP profile and associate it with a CPE IP server profile	265
Creating PWE service on ONU CES ports and associate it with a CPE PWE profile 266	
Creating RF service on ONU RF ports	268
Activate ONT/ONU in Dynamic OMCI	269
Activating ONT/ONU in Dynamic OMCI.....	269
Residential Gateway (RG) Features Provisioning	270
RG modes in RG provisioning.....	271
OMCI GPON zNID with RG features installation for Triple services	272
Associating a GPON traffic profile to the ONU	273
Specifying internal ME profile for the ONU.....	273
Creating uplink/downlink MXK bridges, and CPE connections in RG-brouted mode for data service.....	273
Activating the ONU.....	275
Creating uplink/downlink MXK bridges, and CPE connections in RG-bridged mode for Video service.....	275
Creating uplink/downlink MXK bridges, and CPE connections in RG-bridged mode for Voice service	276
Creating IP Common profile for Voice service (Optional).....	277
Creating uplink/downlink MXK bridges, and CPE connections in RG-brouted mode.....	278
Creating CPE WLAN subscriber profile and associate it with a CPE WLAN com- mon profile or CPE WLAN common advance profile (optional)	279
Creating CPE WLAN common profile (optional)	280
Creating CPE WLAN common advance profile (optional)	282
CPE System Level Default Settings	286
Configuring CPE system common profile	286
Applying a CPE system common profile to a CPE.....	288
Static Configuration on the WAN side interfaces (without DHCP)	288
Assigning a Static IP address to the WAN side interface on the zNID.....	288
Static configuration on the LAN side interfaces with a new DHCP server ...	290
Assigning a Static IP address to the LAN side interface on the ONU	290
Configuration of Static Routes	291
Adding a Static Route to the ONU	291

Configuration of Firewall	293
Enabling or disabling firewall	293
Configuring firewall access.....	293
Configuring port forwarding	295
Configuration of DHCP server.....	297
Creating a new DHCP server for the LAN interface.....	297
Configuration of TR-069.....	298
Configuring TR-069 client settings on the ONU	298
Configuration of PPPoE username and password.....	298
Specifying a PPPoE username and password.....	298
CPE Management Templates.....	299
Adding a user-defined CPE management template.....	300
Selecting a CPE system template	301
Post Configuration in USP.....	301
Appending post script file to the ME Profile	301
Removing post configuration script file from the ME profile.....	302
CPE LLDP-MED configurations.....	302
GPON ONT Inventory Tool	304
Generating GPON reports with the GPON ONT Inventory Tool	304
Voice configuration.....	304
Voice configuration templates	306
Creating AAL2 to V5.2 (PSTN) voice configuration templates	306
Creating AAL2 to V5.2 (ISDN) voice configuration templates	307
Creating AAL2 to GR-303 voice configuration templates	308
Creating AAL2 ELCP to V5.2 (ISDN) configuration templates	309
Creating AAL2 ELCP to V5.2 (POTS) configuration templates.....	310
Creating ISDN to AAL2 configuration templates.....	310
Creating ISDN to V5.2 configuration templates.....	311
Creating POTS to GR-303 configuration templates.....	312
Creating POTS to V5.2 configuration templates	313
Creating POTS to AAL2 configuration templates.....	314
Creating POTS to DS1 configuration templates	314
Creating EBS to GR-303 configuration templates	315
Manage voice connections.....	316
POTS to AAL2 voice connections	316
Adding POTS to AAL2 voice connections	317
Adding POTS to AAL2 voice connections using the wizard (Z-Edge)	317
Adding POTS to AAL2 voice connections using the wizard (MALC)	318
Ringling POTS phone.....	319
POTS to DS1 voice connections	320
Adding POTS to DS1 voice connections	320
POTS to V5.2 voice connections	320
Adding POTS to V5.2 voice connections	321
Adding POTS to V5.2 voice connections using the wizard.....	321
POTS to VOIP voice connections	322
Adding POTS to VOIP voice connections.....	322
POTS to GR303 voice connections.....	325
Configuring VOIP settings for POTS to GR303 voice connections.....	326
Adding POTS to GR303 voice connections.....	326

Adding POTS to GR-303 voice connections using the wizard	327
POTS (RT) to GR-303 (COT) voice connections	328
Adding POTS (RT) to GR-303 (COT) voice connections	329
POTS to GR303 ESA voice connections	330
Configuring VOIP settings for POTS to GR303 ESA voice connections	330
Adding POTS to GR303 ESA voice connections	331
Adding POTS to GR-303 ESA voice connections using the wizard	332
ISDN to AAL2 voice connections.....	333
Adding ISDN to AAL2 voice connections.....	333
ISDN to V5.2 voice connections	334
Adding ISDN to V5.2 voice connections	335
ISDN SIG to VOIP voice connections	335
Adding ISDN SIG to VOIP voice connections	336
ISDN to VOIP voice connections	336
Adding ISDN to VOIP voice connections	336
VOIP (SIP PLAR) to GR303 voice connections (Voice Gateway)	337
Adding VOIP to GR303 voice connections	338
VOIP (SIP PLAR) to V5.2 voice connections (Voice Gateway).....	339
Adding VOIP to V5.2 voice connections	339
AAL2 to GR303 voice connections (Voice Gateway).....	340
Adding AAL2 to GR303 voice connections	340
AAL2 to V5.2 voice connections (Voice Gateway).....	341
Adding AAL2 to V5.2 voice connections	341
AAL2 ELCP to V5.2 voice connections (Voice Gateway).....	342
Adding AAL2 ELCP to V5.2 voice connections	342
EBS to GR303 voice connections	343
Adding EBS to GR303 voice connections	344
Adding EBS to GR-303 voice connections using the wizard	344
EBS to VOIP voice connections	345
Adding EBS to VOIP voice connections	345
Manage voice gateway AAL2 subscribers	346
Adding voice gateway AAL2 subscribers.....	347
Creating an ATM AAL2 VCL	349
Manage VOIP connections	350
Configuring VOIP system parameters	350
Configuring VOIP server parameters.....	351
Configuring malicious caller lists.....	353
Configuring hunt groups	354
Configuring SIP dial plans	355
Configuring voicegateway	356
Configuring ISDN signaling profiles	357
Configuring ESA voice connections	359
Data configuration.....	360
Data templates.....	361
Creating ATM traffic descriptor configuration templates.....	361
Creating ATM cross connect configuration templates.....	362
Adding an ATM cross connect.....	363
Adding ATM cross connect on MALC, and Raptor using the wizard.....	364
Adding ATM cross connect on MALC, and Raptor (advanced mode).....	366

Adding an ATM cross connect (VP switched connection)	369
Modifying an ATM cross connection traffic descriptor.....	370
Deleting an ATM cross connect.....	371
Creating an ATM VCL for data	372
Creating an ATM VPL	373
Adding an ATM cross connect (CES).....	374
Adding an ATM Circuit Emulation Service (CES) cross connect using the wizard 376	
Modifying CES.....	378
Optical cross connection (GigaMux only).....	379
Adding an optical cross connect.....	380
Modifying an optical cross connection	381
Deleting an optical cross connect.....	381
IP configuration.....	382
DHCP	382
DHCP relay	382
Specifying DHCP server in DHCP relay mode.....	383
Setting up a DHCP server	384
Modifying DHCP defaults.....	386
Adding network-based routes.....	386
Adding host-based routes	387
Adding IP interfaces	391
Modifying the IP routing domain and adding static routes	392
Adding IP interfaces (Z-Edge only)	394
Configuring NAT (Z-edge only)	395
Configuring PAT bindings	396
Configuring IPSLA.....	397
Configuring IPSLA statistics path.....	397
Configuring CoS action.....	399
Configuring CoS map.....	400
Viewing the Real time IPSLA statistics	400
Viewing the historical IPSLA statistics.....	401
Configuring IP on a bridge	402
Bridge configuration.....	403
Overview	404
Asymmetrical and symmetrical bridges	404
Untagged, tagged, and double tagged bridges.....	406
Bridge filtering	406
VLAN/SLAN Translation	407
Multicast VLAN Registration (MVR) for video configuration	407
Configuring bridging.....	408
Modifying bridging logicals.....	410
Configuring bridge paths.....	415
Bridge filter groups and members.....	418
Access Control List	419
Rate Limit Discard	419
Color Aware Rate Limit Discard.....	420
Bridge Storm Detect.....	421
Destination Mac Swap Dynamic.....	422

Destination Mac Swap Static	422
Dhcp Relay	423
DscpToCos	424
Forbid Oui	424
Insert Option 82.....	424
Insert PPPoE Vendor Tag.....	425
VLAN Encapsulation	428
Configuring bridge filter groups and members	431
Viewing Bridge IGMP tables.....	436
Bridge template.....	437
Adding a bridge template	437
External DHCP subnet template	437
Adding a DHCP subnet template	437
Packet rule member template.....	438
Adding a packet rule group member template	438
Packet rule group template.....	438
Adding a packet rule group template	439
IGMP Snooping with Proxy Reporting.....	439
Enabling IGMP snooping with proxy reporting and custom IP address.....	440
IGMP DSCP.....	442
IGMP DSCP overview	442
Default IGMP IP address and Custom IGMP IP address.....	443
Configuring IGMP DSCP and IGMP proxy reporting and IGMP IP address.....	443
ADSL fall-back Mode for VDSL 2 card.....	444
ADSL2+ fallback in PTM mode	444
ADSL2+ fallback in ATM mode	444
Secure DHCP, Secure IP without DHCP.....	444
Case 1: Configuring secure DHCP.....	445
Case 2: Configuring secure static MAC + IP	445
Case 3: Configuring secure static MAC.....	446
Case 4: Configuring secure static IP	446
Multiple Spanning Tree Protocol (MSTP).....	447
MSTP overview	447
MSTP instances	447
MSTP port role.....	447
MSTP port state.....	448
Plan the VLAN mapping for MSTP.....	449
Configuring MXKs for MSTP	449
Configure MSTP uplinks on two MXKs in a MSTP network for load balancing	
451	
Configuring the stp-params 0 profile on the first MXK.....	451
Configuring the mstp-instance profile on the first MXK.....	451
Configuring the uplink(s) on the first MXK	451
Configuring the stp-params 0 profile on the second MXK	452
Configuring the mstp-instance profile on the second MXK	452
Configuring the uplink(s) on the second MXK.....	453
Configuring redundant MSTP uplinks	454
Configuring MSTP uplinks for load balancing	454
IPV6 bridges	454

Multicast control list configuration	455
Configuring multicast control lists	455
Adding an ATM VCL to multicast map.....	456
Redundancy overview	457
Automatic protection switching (MALC and Raptor only)	458
Configuring APS	458
Administration procedures	459
Managing Users.....	459
Logging out of NetHorizhon	459
Changing your NetHorizhon password	460
Locating the version number of the NetHorizhon application	460
Changing your NetHorizhon preferences	460
Displaying objects in group.....	460
Configuring audio alarm notification	461
Finding ATM VCLs and cross connects	461
Pinging ATM VCL endpoints	462
Viewing alarm history	462
Viewing the audit log	463
Viewing the task log.....	463
Printing or exporting log entries.....	464
Printing or exporting configuration data	465
Filtering alarms.....	465
Adding notes to alarms.....	466
Displaying Inventory Manager.....	466
Updating Display from Database	467
Telnetting/ SSH to ZMS server	467
Running diagnostics	467
TAC Metallic Line Tests	467
Metallic loop testing.....	468
View line state before testing	469
Viewing the line state for a POTS port	469
MTAC-FC / MTAC-RING card line testing.....	469
To perform metallic tests on MTAC/RING-FC card or MTAC-RING card:	469
MTAC-ENH card internal line testing	470
To perform MTAC/RING-ENH card internal line tests:	470
Single-End Loop Test (SELT).....	472
Running SELT.....	472
Dual-End Loop Test (DELT).....	473
Running DELT	473
T1 BERT	474
BER Testing for T1 EFM.....	474
Running a BER test	474
802.3ah Ethernet OAM loopback	475
Configuring Ethernet OAM loopback.....	475
Traps	476
Viewing traps	477
Viewing trap details.....	478
Alarms	479

Alarm manager overview	480
Viewing all alarms on the network.....	480
Viewing all alarms for a particular object.....	482
Viewing alarm history.....	482
Viewing alarm details.....	482
Acknowledging alarms.....	483
Clearing alarms.....	483
Forwarding alarms.....	484
Assigning alarms	486
Identifying objects with alarms	486
Receiving mail notification of alarms	488
Configuring external alarms.....	488
Index.....	491

1

GETTING STARTED

This chapter describes basic NetHorizon operations. It includes the following sections:

- [Introduction, page 25](#)
- [About your NetHorizon account, page 26](#)
- [Logging into NetHorizon, page 26](#)
- [Creating operator accounts, page 28](#)
- [Navigating the system, page 30](#)
- [Using the menu bar, page 39](#)
- [Using the toolbar, page 45](#)
- [Changing your NetHorizon password, page 46](#)
- [Accessing online Help, page 46](#)

Introduction

NetHorizon™ is a Java application that operators use to navigate, monitor, and manage *objects* in their Zhone Management System (ZMS™) networks. Objects are networking components such as network devices, cards, physical ports, logical interfaces, and permanent virtual circuits (PVCs).

The ZMS administrator determines the specific operations that are offered to operators. If the ZMS administrator provides full ZMS permissions, operators can perform the following types of operations from the NetHorizon application:

- **Monitor objects** — View and monitor the status of network elements.
- **Provision resources** — Make configuration changes to network elements and provision subscribers and end-to-end services within the Zhone™ environment.
- **Manage faults** — View traps and alarms from network elements and configure alarm forwarding to destination addresses, as needed.
- **Monitor performance data** — Track real-time and interval network performance statistics.
- **Run diagnostics tests** — Run diagnostics on cards.

About your NetHorizhon account

Your ZMS administrator sets up the specifics of your NetHorizhon account:

- Your NetHorizhon user name and password.
- Your user permissions, ranging from modify and delete permission to view-only permission for ZMS objects.

Logging into NetHorizhon

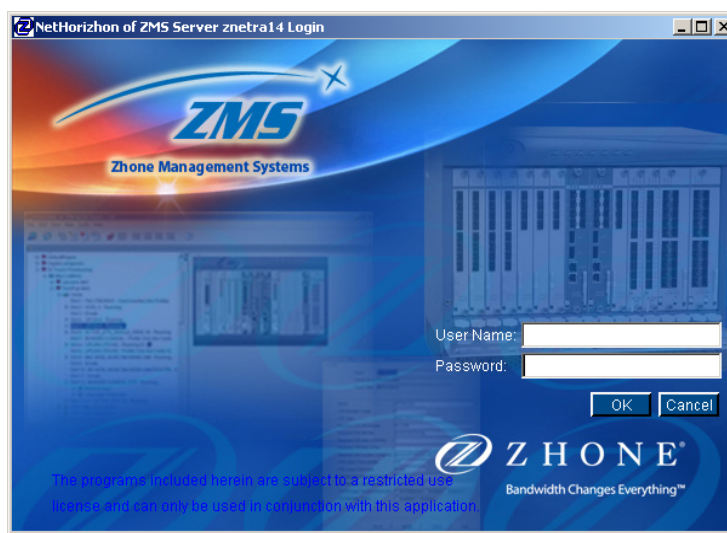
Before you can log in to NetHorizhon, you need a user name and password from your administrator.

- 1 Open Windows Explorer and change to the ZMS directory.
- 2 Double-click the *load_zms.cmd* file.

The installation program installs the NetHorizhon application in the ZMS directory. The process may take several minutes, depending on your network connection. After the application has been installed on your local machine, the NetHorizhon Login dialog box appears.



WARNING! Zhone recommends a maximum of 30 clients running at the same time in order to prevent ZMS server performance degradation



- 3 Enter the administrator user name and password in the **NetHorizhon Login** box (user name **admin** and the password **zhone**).
- 4 Click **OK**.

The NetHorizhon application starts, displaying the **User Administration** window. (see [Figure 1](#))

For instructions on how to change your password, see [Changing your NetHorizhon password, page 46](#).

Viewing information about your NetHorizon account

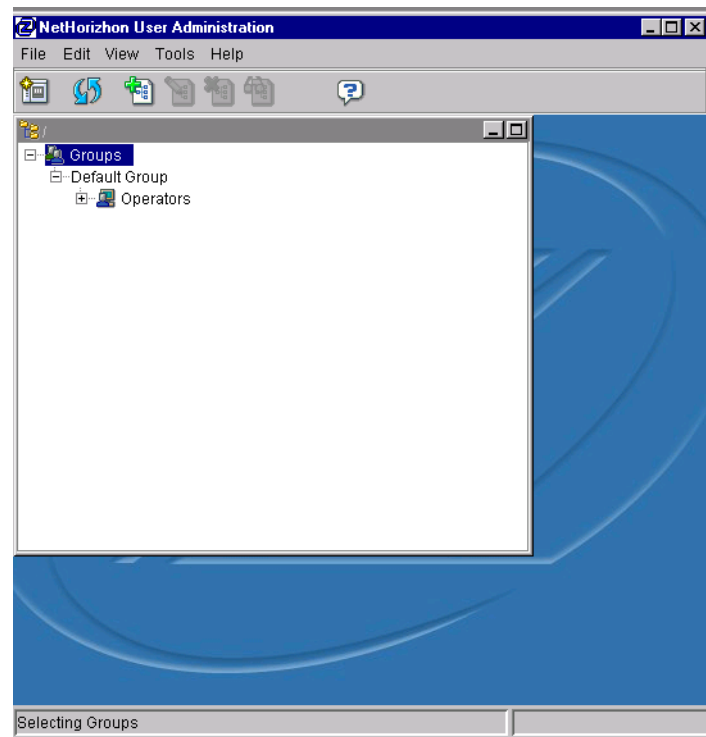
- 1 Click **View > My Account Info** from the menu bar.

NetHorizon displays the **Operator Configuration** dialog box, listing your account name, status, and assigned permissions.

- 2 When you have finished viewing information about your account, click **Close**.

If you attempt to log in to NetHorizon four consecutive times, but fail (because you supplied the wrong user name or password), the administration manager automatically deactivates your NetHorizon account. You cannot log in to NetHorizon until your ZMS administrator reactivates your account.

Figure 1: NetHorizon User Administration window



The **User Administration** dialog box is made up of these components:

- Menu bar containing commands you can issue (see [Table 2 on page 39](#)).
- Toolbar containing icons that represent commands you can issue (see [Table 3 on page 45](#)).
- Tree display listing Groups, Default Group, and Operators.
- Status bar for selection messages.



Note: If you log in as **admin**, NetHorizon displays the User Administration dialog box. You must create operator accounts to view device objects in the tree display and the graphical display (see [Creating operator accounts on page 28](#).)

Creating operator accounts

When you create an operator account, you specify the user name and password and assign user permissions.

Once you activate the account, the operator can download, install, and run the NetHorizon client application. The operator permissions define what actions the operator can perform in NetHorizon (see the online help for more information).

- 1 Use any of the following methods to create an operator account:

Menu bar: Click **Tools > Configure Users**.

Toolbar: Click the **Create and Administer User Accounts** icon.

NetHorizon displays the **User Administration** dialog box, listing existing users in your group.

- 2 Right click the operators container and click **Add**.

NetHorizon display the **Operator Configuration** dialog box.

- 3 Complete the parameters in the **Operator Configuration** dialog box:

Name—Enter the user name. Use only alphanumeric characters and the underscore (_) character. (Do not use blank characters.)

Password—Enter a unique password for the user. Use a minimum of four characters consisting of alphanumeric characters and the underscore (_). (Do not use blank characters.)

Confirm Password—Re-enter the password for the user.

Account Status—To activate the operator, choose **Active** from the drop-down list. To deactivate the operator, choose **Inactive** from the drop-down list.

(Be sure to record the user name and password, so you can provide it to the operator.)

Permissions—Assign permissions for the user:

- **View Objects in All Groups**—Mark the checkbox to allow the user to view objects that belong to any group. Unmark the checkbox to restrict the user from viewing objects that are not in the user's group. (If this permission is **Disabled** for your account, you cannot set it for other operators.)
- **Region and Subregion Configuration**—Choose **Write** to permit the user to add, modify, and delete regions and subregions in the user's group. Choose **Read** to permit the user to only view configuration settings for regions and subregions in the user's group.
- **Equipment Provisioning**—Choose **Write** to permit the user to add, modify, and delete equipment (devices, cards, physical ports, and so on) in the user's group. Choose **Read** to permit the user to only view configuration settings and performance data for equipment in the user's group.

- **Subscriber Provisioning**—Choose **Write** to permit the user to add, modify, and delete customers, subscribers, and voice and data connections in the user's group. Choose **Read** to permit the user to only view configuration settings for customers, subscribers, and voice and data connections in the user's group.
- **Trap/Alarms Administration**—Choose **Write** to permit the user to view traps and alarms and acknowledge, assign to troubleshooter, and close alarms of objects in the user's group. Choose **Read** to permit the user to only view traps and alarms of objects in the user's group.
- **Diagnostics Administration**—Mark the checkbox to allow the user to run diagnostics tests on cards in the user's group. Unmark the checkbox to restrict the user from running diagnostics tests.

4 Click Add.

The operator inherits the user administrator's group ID. The operator can manage objects only in that group. If the operator has **View Objects in All Groups** permission, the operator can view objects in other groups.

5 Click Close.

The newly created operator will appear under **Operators** in the tree display.



Note: Refer to the *ZMS Administrator's Guide* for more information on viewing, modifying, and deleting an operator account.

Logging in as a newly created operator

You must exit NetHorizon and then log in as the newly created operator to add, manage, and view devices.

1 Exit NetHorizon:

Menu bar: Click **File > Exit**

or click the close button icon in the upper right corner of the window

2 Re-start NetHorizon by double-clicking the *load_zms.cmd* file in the appropriate ZMS directory.

The NetHorizon Login dialog box appears.

3 Enter the user name and password of the newly created operator in the **NetHorizon Login box.**

4 Click OK.

The NetHorizon application starts, displaying the **Top Level** window. This view has a graphical display which displays ZMS objects and their physical and geographical details.

Navigating the system

You navigate through the system by expanding *container* objects to view their object *instances* (objects whose type is that of the container). Containers are like folders and instances are like the files contained within them. Instances can contain other objects.

You can select an object using either the tree display or the graphical display and then act on that object (for example, view it, modify it, or delete it). Depending on the method you use, selecting an object in the tree display can update both the tree display and the graphical display (and vice versa).

Tree display

In the tree display, the expansion icon indicates which objects contain other objects:

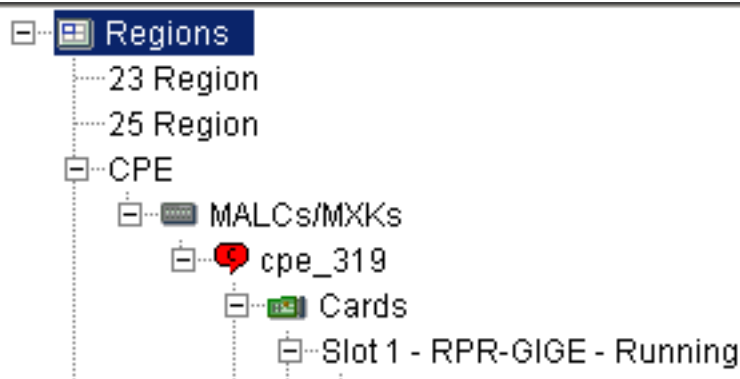
- If the expansion icon is the plus sign (+), the object is closed.

Figure 2: Expansion icon is the plus sign



- If the expansion icon is the minus sign (–), the object is open, and the names of all its contained objects are listed below it.

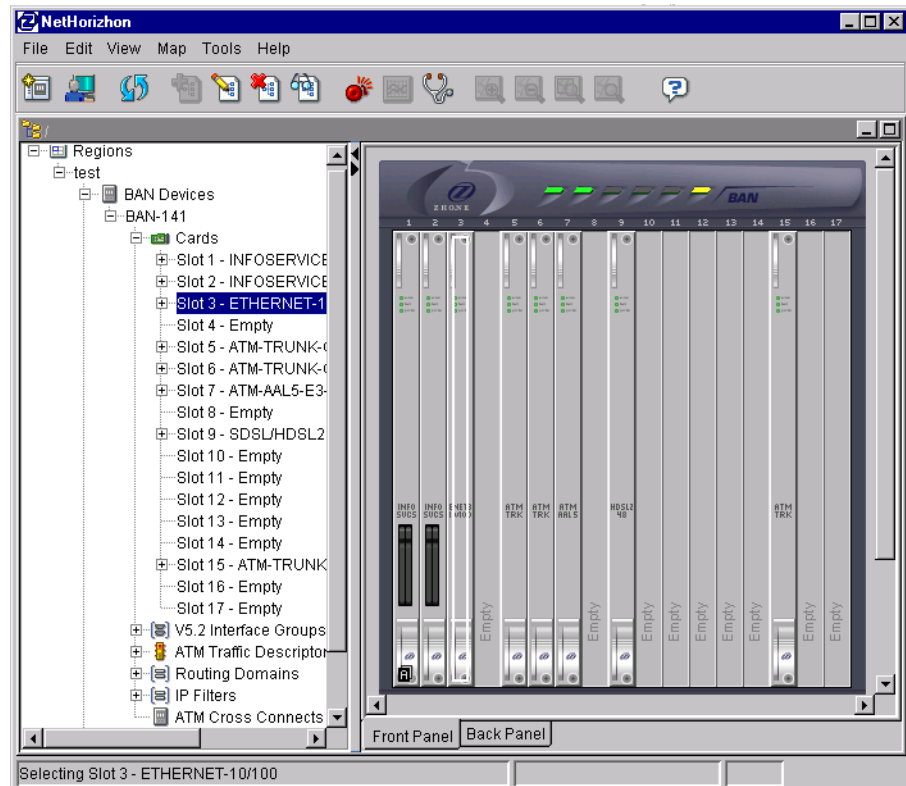
Figure 3: Expansion icon is the minus sign



You navigate through objects in the tree much like you navigate through folders and files listed in a file management program (see [Figure 4](#)):

- Click the expansion icons to open and close objects in the tree display.
- Single-click an object to select it in both the tree display and the graphical display.
- Double-click an object to open or close it in both the graphical display and the tree display.

Figure 4: Navigating the tree

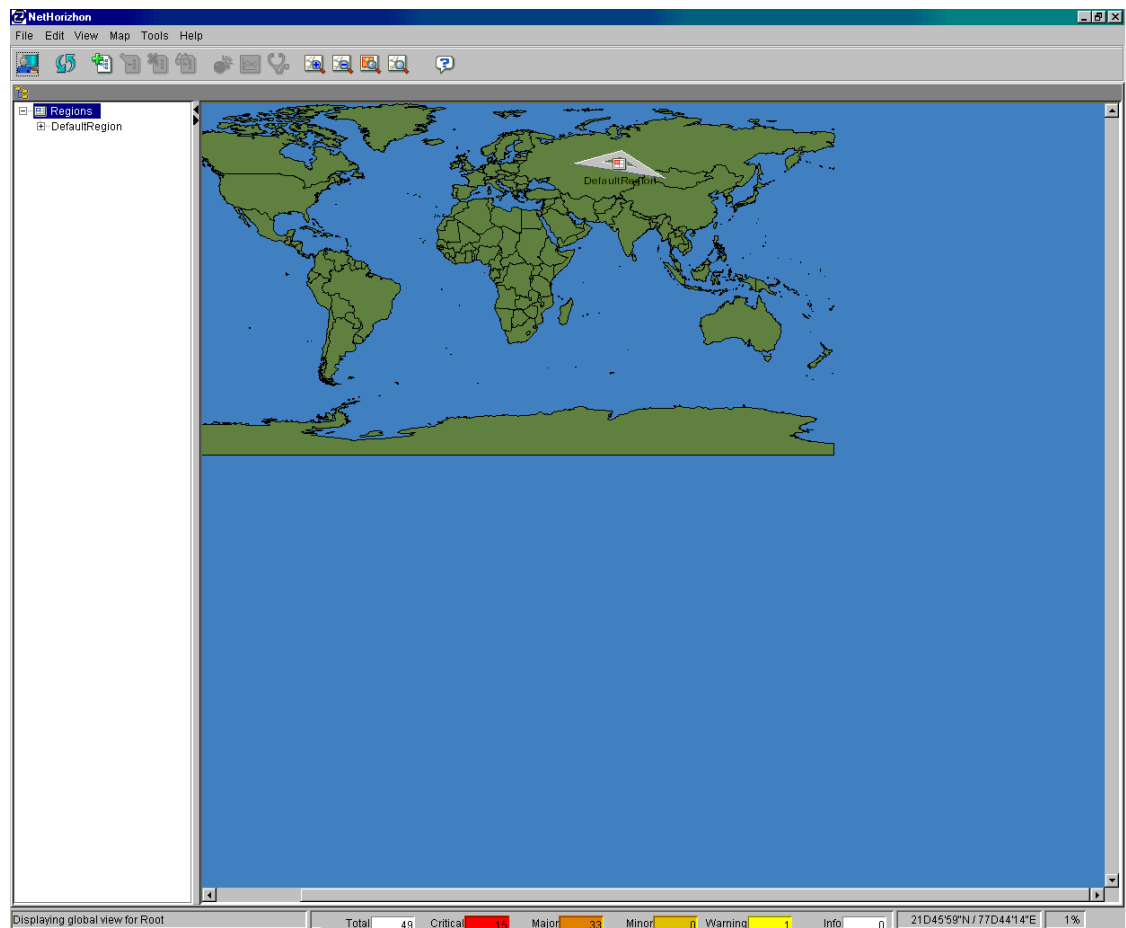


Graphical display

In the graphical display, objects are displayed graphically:

- Equipment displays show the physical details of an individual object (including front and back panels) (see [Figure 4](#)).
- Map displays show the geographical location of network objects and the total number of alarms and the severity of each is shown in the status bar of the ZMS main screen (see [Figure 5](#)).

Figure 5: Graphical display showing geographic location of an object



The following sections describe how to use the graphical display.

Equipment display: viewing card status

NetHorizon dynamically updates the equipment display with current card status information. Any time a card's status changes, your display informs you with the following changes:

Adds (or removes) a status icon to the card—The card status icon identifies the current state of the card:

Table 1: Card status icons

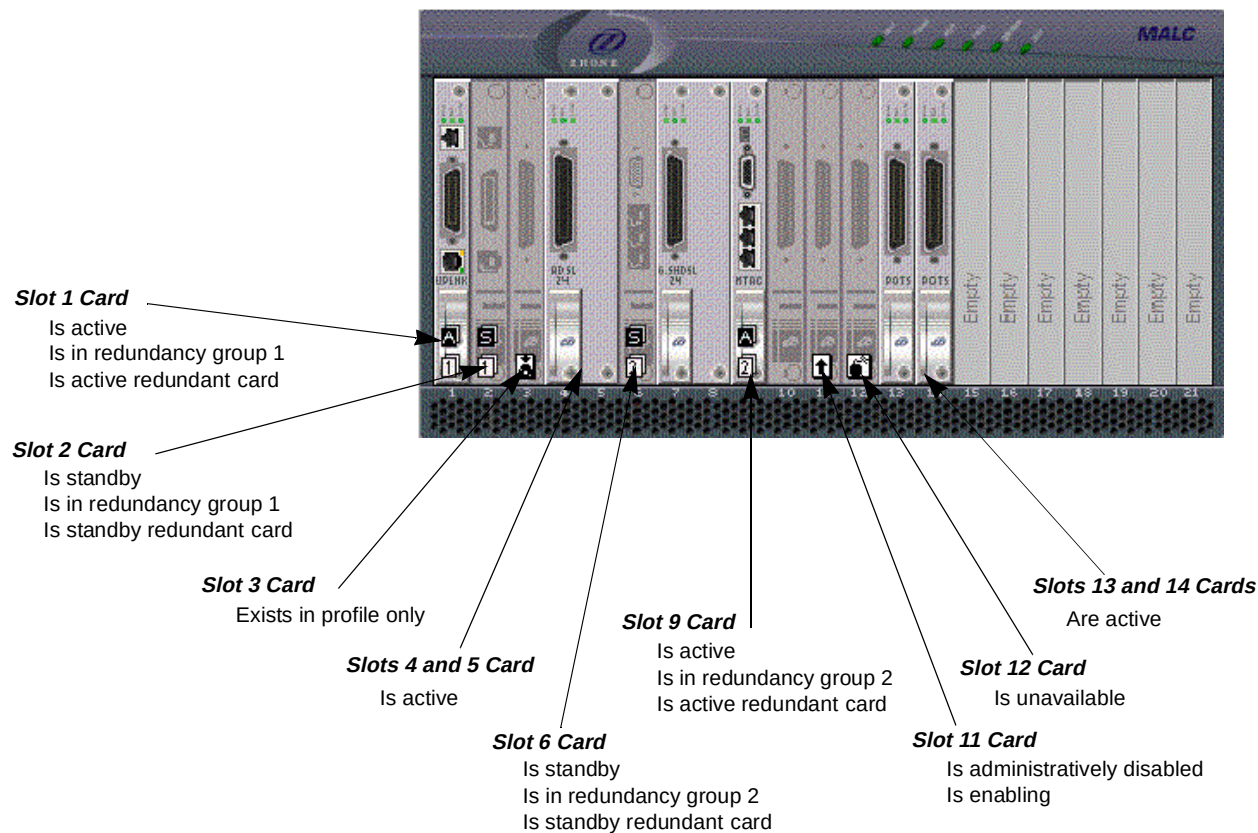
Icon	Status
	Enabling Card is enabling.
	Unavailable Card is unavailable.
	Profile Only Card exists in profile only.
	Redundancy Group Member Card is a member of a redundancy group. All members of a group display the same group number. (Icon shown in both tree display and graphical display.)
	Redundant, Active Card is redundant and is the active redundant card. (Icon shown in both tree display and graphical display.)
	Redundant, Standby Card is redundant and is the standby redundant card. (Icon shown in both tree display and graphical display.)

Updates the card graphic—If the card is dimmed, its current state is one of the following:

- Card exists in profile only.
- Card is administratively disabled.
- Card is unavailable.
- Card is in standby mode.

Figure 6 shows the graphical display, identifying status of the cards in a device.

Figure 6: Graphic display with card status indicators



Map display: zooming in and out of views

To zoom in and zoom out of your view of the map:

Toolbar icon



- **Zoom In** increases magnification of your map.
- **Zoom Out** decreases magnification of your map.
- **Zoom to Designated Area** sets your map to a specific area.
Using the cursor, point and drag diagonally to draw a selection border around the area. NetHorizon magnifies your view to the specified area of the map.
- **Zoom to Default** sets your map to the default magnification.

Menu bar

- **Map > Zoom > In** increases magnification of your map.
- **Map > Zoom > Out** decreases magnification of your map.
- **Map > Zoom > Default** sets your map to the default magnification.
- **Map > Zoom > Designated Area** sets your map to a specific area. Using the cursor, point and drag diagonally to draw a selection border around the area. NetHorizon magnifies your view to the specified area of the map.

Navigating through objects in the graphical display

To navigate through objects in the graphical display:

- Single-click an object to select it in both the graphical display and the tree display.
- Double-click the object to view the instance objects in both the graphical display and the tree display.

To reposition objects in your map display:

- 1 Display the global, regional, subregional, or access map that contains the objects you want to reposition.
- 2 Use any of the following methods to reposition the object instances in your display:

Menu bar: Click **Map > Reposition Objects**.

Pop-up menu: Right-click the map and click **Reposition Objects**.

NetHorizon displays the **Reposition** dialog box.

- 3 To increase magnification of your map, click **Zoom In**.

To decrease magnification of your map, click **Zoom Out**.

To set your map to a specific area, click **Zoom to Designated Area**. Using the cursor, point and drag diagonally to draw a selection border around the area. NetHorizon magnifies your map to the specified area.

- 4 To reposition an object, click the object and drag and drop it to the location you want.
- 5 To save your changes, click **OK** or **Apply**.

NetHorizon updates your view with the new object positions.

Navigating through views

When you first start NetHorizon, the top-level NetHorizon window displays the global view to which you have access. The global view shows one or more regions containing Zhone device(s).

As you navigate the system to access a particular object, your view becomes more detailed. For example:

Navigating a tree

- 1 From a global view, click the expansion icon on the region to list all its regions.
- 2 Click the expansion icon on a region to list all its subregions and managed devices. Your view is now a regional view.
- 3 From a regional view of subregions and devices, click the expansion icon on a subregion to view all its subregions and devices.

Click the expansion icon on a subregion to view all its nested subregions. Subregions can contain up to three levels of nested subregions. Your view is now a subregional view.

Click the expansion icon on a device to view all its cards. Your view is now a chassis view.
- 4 From a chassis view of cards, click the expansion icon on a card to view all its ports. Your view is now a card view.

Navigating a graphical display

- 1 From a global view, expand a region or subregion (using any of the methods described in [Navigating through objects in the graphical display on page 35](#)) to view its managed devices. Your view is now a regional view or subregional.
- 2 From a regional or subregional view of devices, expand a device to view its cards. Your view is now a chassis view.
- 3 From a chassis view of cards, expand a card to view all its ports. Your view is now a card view.



Note: From a regional or subregional view of devices, you can expand a device to view attached access devices. To do so, right-click a device and click **Expand Attached IADs**. Your view is now an access view.

Launching multiple display windows

NetHorizon allows you to have multiple display windows (viewports) open at a time. This feature is useful for simultaneously displaying details of different objects in the network. For example, you can have one viewport open, displaying details on a device. At the same time, you can have a second viewport open, displaying details on a particular card on that device.

Launching multiple display windows:

- 1 From any view, select an object to display in a separate window.



- 2 Click **File > New** (or click the **New** icon).

NetHorizon displays the object in a new viewport, showing the object as the root of the tree display.

- 3 Move the display windows where you want for viewing.

To arrange the viewports side-by-side for simultaneous viewing of each object, click **View > Layout > Tile**.

To arrange the viewports in an overlapping series, click **View > Layout > Cascade**.

- 4 To close a second viewport, click the close button icon in the upper right corner of the window.

NetHorizon closes the second window and returns you to the original display window.

Using the message console window

NetHorizon allows you to view important system messages (such as errors) that are generated by NetHorizon. For example, you can have a viewport open, displaying details on a device. At the same time, you can have the message console open, displaying any errors that occur as you configure objects on that device.

To view system messages, click **View > Console** from the menu bar.

NetHorizon displays the **Console** dialog box, listing messages generated during your current NetHorizon session.

Figure 7: Console dialog box



To clear the Console dialog box and start displaying new messages, click **File > Edit > Clear** (or click the **Clear** icon).

To close the **Console** dialog box, click **File > Close** from the **Console** dialog box (or click the close button icon in the upper right corner of the window).

Updating your display

Updates following adds and deletes

NetHorizon dynamically updates its display with current information from the ZMS database. As objects are added or deleted by you or other operators, your display updates to reflect those changes.

Updates following action parameter changes

Action parameters configure particular settings related to those at the Local Exchange (LE) or Integrated Digital Terminal (IDT). When an operator changes the value of an action parameter, ZMS sends the change to the Zhone device, which then sends the change to the connected LE or IDT. Until the parameter change is successful at the LE or IDT, the V5.2 or GR-303 interface group is in a transitional state. During the transition, activity occurs between the Zhone device and the LE or IDT. NetHorizon warns you and other operators against modifying some parameters on the device until the action change has been made at the LE or IDT.



Note: If you do change action parameters or other associated parameters before notification has been received from the device and/or the switch at the LE or IDT, you may render the object in an inconsistent state.

Once the action change is successful at the LE or IDT, NetHorizon displays a message informing you that the action parameters and other associated parameter values have changed. Your display updates to reflect those changes.

Examples of action parameters are **Admin Status** of a GR-303 interface group, **Check ID** and **Block Type** of a V5.2 link, and **Port Alignment Request** and **Request Provisioning Variant** of a V5.2 interface group. Action parameters are labeled with the **Action** icon.



Updates following synchronization

When other operators perform a **Synchronize with Device**, NetHorizon displays a message informing you that the device has changed:

- To update your display with the latest information, click **Update**.
- To leave your display unchanged, click **Cancel**. NetHorizon labels the device with the refresh icon in the tree display.

ban_80_210 

Anytime you want to update your display, select the device and click **Update Display from Database** (using any of the methods described in [Updating an object and its children](#)).

Updating an object and its children

You can manually update your display with current information from the database. You can update a selected object and its children (if any).

Use any of the following methods to select the object and update your display:

Menu bar: Select the object and click **Edit > Update Display from Database**.



Toolbar: Select the object and click the **Update Display from Database** icon.

Pop-up menu: Right-click the object and click **Update Display from Database**.

NetHorizon updates the selected object and all its children in your display with current information from the ZMS database.

If NetHorizon cannot update the selected object (for example, because the object or its parent was deleted by another operator and is no longer in the ZMS database), NetHorizon prompts you whether you want the object (or, in some cases, the parent object) removed from your display.

Updating the entire display

You can manually update your entire display with current information from the database.

To update your entire display, click **View > Update Entire Display**.

NetHorizon updates the entire display with current information from the ZMS database.

Using the menu bar

Table 2 lists the menu options in NetHorizon.



Note: The actual menu options provided to the operator depend on the user permissions defined by the ZMS administrator. If an operator does not have permissions to a particular function, menu options that support that function are hidden.

Table 2: NetHorizon menu options

Menu	Option	Use this option to
File	Exit	Log out of NetHorizon.
Edit	Add	Add an object.
	Modify	Modify an object.
	Delete	Delete an object.

Table 2: NetHorizon menu options (Continued)

Menu	Option	Use this option to
	View	View configuration data for the selected object.
	Add Sub Region	Add a sub region.
	View Alarms	View alarms for an object.
	Synchronize Alarms	Synchronize alarms
	Equipment Provisioning Device Configuration Synchronize with Device	Synchronize device and ZMS databases for a device.
	Equipment Provisioning Device Configuration Reboot Device	Reboot the selected device.
	Equipment Provisioning Device Configuration Download Software Image	Download a software image to be loaded for operation by cards of a particular type.
	Equipment Provisioning Device Configuration Delete Software Image	Delete a software image no longer used by cards of a particular type.
	Equipment Provisioning Device Configuration Set Card Default Image	Load the default software image for operation by cards of a particular type.
	Equipment Provisioning Device Configuration Manage ATM Connections	Configure ATM PVC cross connections.
	Equipment Provisioning Device Configuration Modify VCL Rates	Change the allowable VCL rates for rt-VBR or rt-VBR traffic.
	Equipment Provisioning Device Configuration Point to Point Protocol	Configure point-to-point protocol.
	Equipment Provisioning Device Configuration Manage Voice Subscribers	Assign subscribers to voice ports.
	Equipment Provisioning Device Configuration Manage IP	Configure IP services.
	Equipment Provisioning Device Configuration Manage Bridging	Configure bridging.
	Equipment Provisioning Device Configuration View Shelf Status	Obtain general information about the device.

Table 2: NetHorizon menu options (Continued)

Menu	Option	Use this option to
	Equipment Provisioning Device Configuration Backup Device Configuration	Back up configuration data on a device.
	Equipment Provisioning Device Configuration Restore Device Configuration	Restore configuration data on a device.
	Equipment Provisioning Device Configuration Edit Configurations	Modify an existing configuration file to use as the basis for configuring another device.
	Equipment Provisioning Card Configuration Configure Cards	Add and modify cards on a device.
	Equipment Provisioning Card Configuration View Card States	View the status on a device.
	Equipment Provisioning Card Configuration Reboot Card	Reboot an individual card.
	Equipment Provisioning Card Configuration Enable Card	Enable a card that was previously disabled.
	Equipment Provisioning Card Configuration Disable Card	Disable a card.
	Equipment Provisioning Card Configuration Flash Software Image	Initialize the flash memory on a BAN, MALC or Raptor.
	Equipment Provisioning Card Configuration Bulk Statistics	Configure the statistics to store on the device.
	Equipment Provisioning Port Configuration Modify Alarm Profile	Configure DSL alarm templates.
	Equipment Provisioning Port Configuration Modify Config Profile	Configure ADSL configuration templates.
	Equipment Provisioning Port Configuration Modify HDSL2 Config Profile	Configure HDSL2 configuration templates.

Table 2: NetHorizon menu options (Continued)

Menu	Option	Use this option to
	Equipment Provisioning Port Configuration Modify SDSL Config Profile	Configure SDSL configuration templates.
	Equipment Provisioning Port Configuration Modify SHDSL Config Profile	Configure SHDSL configuration templates.
	Equipment Provisioning Port Configuration Modify Voice FXS Config	Configure FXS configuration templates.
	Equipment Provisioning Port Configuration Modify ULC Configuration	Configure ULC configuration templates.
	Update Display from Database	Update the selected object and all its children in your display with current information from the ZMS database.

Table 2: NetHorizon menu options (Continued)

Menu	Option	Use this option to
View	My Account Info	View information about your operator account, such as status and assigned permissions.
	Faults View Traps	View traps on the network.
	Faults View Alarms	View alarms on the network.
	Faults View Alarm History	View all alarms on the device, even those that have been cleared.
	Faults Manage Trap Configuration	Add, modify, or delete trap destinations.
	Faults View Trap History	View the traps received by ZMS.
	Faults View Trap Forward History	View the traps ZMS has forwarded.
	Faults View Alarm Forward History	View the alarms ZMS has forwarded.
	Statistics	View statistics for an object.
	View Voice System Statistics	View voice statistics for an object.
	Tests Diagnostics	Run card diagnostics tests and view results.
	Tests OAM F5 Loopback Ping	Run OAM F5 loopback and view results.
	Tests OAM F4 Loopback Ping	Run OAM F4 loopback and view results.
	Windows	Switch between application windows.
	Console	View message console for the NetHorizon session.
	Update Entire Display	Update your entire display with current information from the ZMS database.

Table 2: NetHorizon menu options (Continued)

Menu	Option	Use this option to
Map	Reposition Objects	Reposition objects in your map display.
	Zoom In	Increase map magnification.
	Zoom Out	Decrease map magnification.
	Zoom Region	Set map to a specific regional area. Using the cursor, point and drag diagonally to draw a selection border around the area. NetHorizon magnifies your view to the specified area of the map.
	Zoom Subregion	Set map to a specific subregional area. Using the cursor, point and drag diagonally to draw a selection border around the area. NetHorizon magnifies your view to the specified area of the map.
	Zoom Normal	Set map to the default magnification.
Tools	Change My Password	Change your password.
	Configure Users	Configure users and grant permissions.
	Manage Active Users	Users with administrative access can view user data, logout and de-active other users.
	Preferences	Change user preferences.
	Auto Discovery	Discover and add devices for management automatically.
	Find Component	Find VCLs and cross connects.
	Configure Templates	Creates configuration templates.
	Download Software Image	Download software images to multiple devices on the network.
	Backup Device Configuration	Enables immediate and scheduled configuration backups on single and multiple devices.
	Find VCLs/VC Cross Connects	Find ATM VCLs or cross connections in a region, subregion, or a device.
	Find Objects	Find object(s) in a region, subregion, or a device.
	Telnet to ZMS Server	Establish a telnet session to the ZMS server.
	Audit Log Viewer	View the configuration requests received by the ZMS server.
	Task Log Viewer	View the task logs received by the ZMS server. The task could be Auto Discovery, Device, Backup, ConfigSync, Download Image, or All.

Table 2: NetHorizon menu options (Continued)

Menu	Option	Use this option to
Help	Topics	Launches online Help.
	About NetHorizon	View NetHorizon version number and copyright information.

Using the toolbar

Table 3 lists the toolbar options in NetHorizon.

Table 3: NetHorizon toolbar options

	Option	Use this option to
	New	Launch a new display window.
	Create and Administer User Accounts	Configure users and grant permissions.
	Update Display from Database	Update the selected object and all its children in your display with current information from the ZMS database.
	Add	Add an object.
	Modify	Modify an object.
	Delete	Delete an object.
	View	View configuration data for an object.
	Faults	View traps on the network.
	Statistics	View statistics for an object.
	Diagnostics	Run card diagnostics and view results.
	Zoom In	Increase map magnification.

Table 3: NetHorizon toolbar options (Continued)

Option	Use this option to
 Zoom Out	Decrease map magnification.
 Zoom Designated Area	Set map to a specific area. Using the cursor, point and drag diagonally to draw a selection border around the area. NetHorizon magnifies your view to the specified area of the map.
 Zoom Default	Set map to the default magnification.
 Help	View online Help.

Changing your NetHorizon password

Initially the ZMS administrator defines your NetHorizon password.

To change your NetHorizon password:

- 1 Click **Tools > Change My Password** from the menu bar.
NetHorizon displays the **Change Password** dialog box.
- 2 Enter your current password in the **Current Password** box.
- 3 Enter a new password in the **New Password** and the **Confirm Password** boxes. Follow the password rules which shown in the **Password Rules** box.
- 4 Click **OK**.

Accessing online Help

The NetHorizon application provides online Help.

You can access online Help in several ways:

Menu bar: Click **Help > Topics**.

NetHorizon displays Help in a separate window, showing the top-level help topic for NetHorizon.



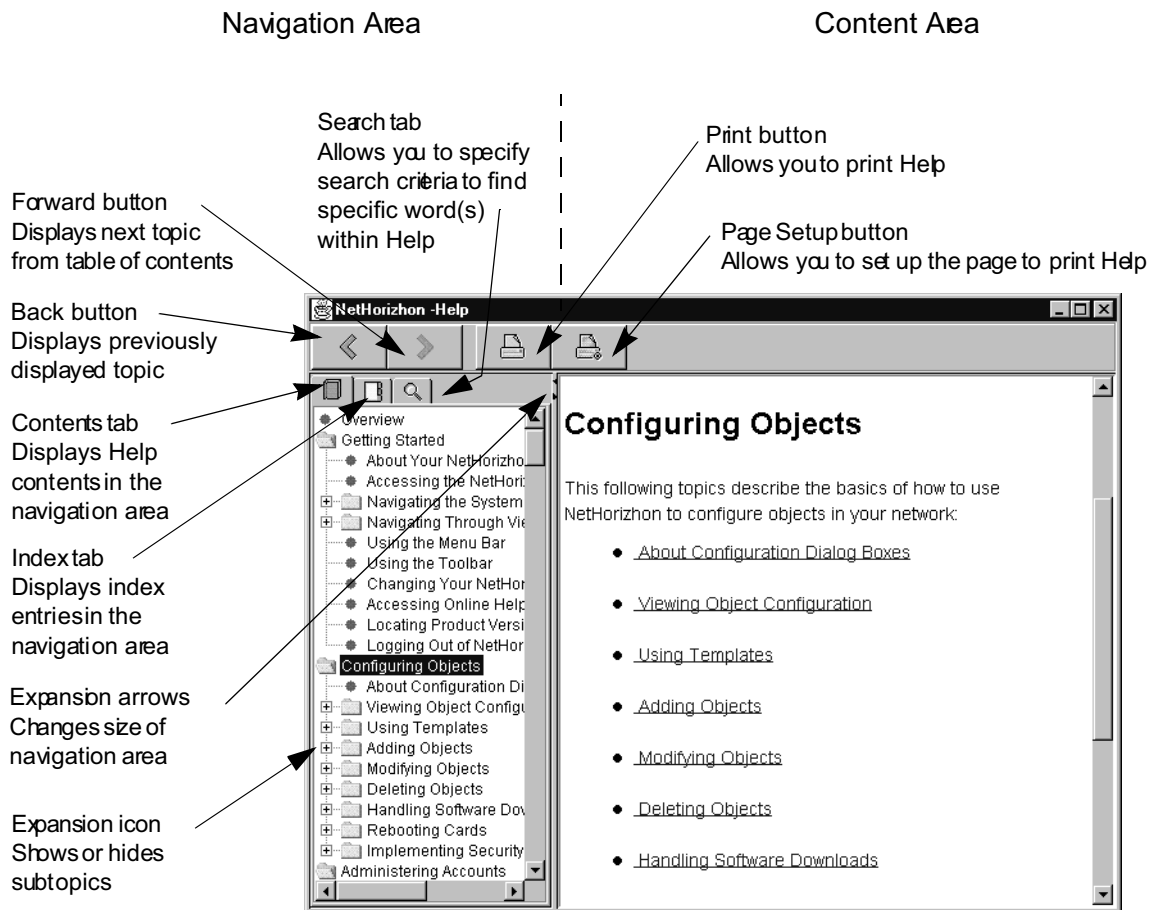
Toolbar: Click the **Help** icon.

NetHorizon displays Help in a separate window, showing the top-level help topic for NetHorizon.

Dialog box: Click **Help** from any dialog box.

NetHorizon displays Help in a separate window, showing the help topic for the particular dialog box (see [Figure 8](#)).

Figure 8: Sample Help window



NetHorizon Help windows have two panes:

Navigation pane—The left-hand navigation pane allows you to select and move to specific topics of Help. This pane includes the following tabs:

- **Contents tab** displays the table of contents in the left pane with an expansion icon to list subtopics. Click on an entry to display that topic in the content pane.
- **Index tab** displays the index entries in the left pane. Click on an index entry to display the referenced topic in the content pane.
- **Search tab** displays the **Find** box and search results. Enter search criteria to search for specific word(s) within Help. Files containing the words are listed below the **Find** box. Click on the file name to display the file in the content pane. The words in the file that match the search are highlighted in blue.

- **Back and Forward buttons** sequentially display information. Click **Forward** to display the next topic of the table of contents in the content pane. Click **Back** to display the previously topic in the content pane.
- **Print button** allows you to print Help information, one topic at a time.
- **Page Setup button** allows you to set printer paper and page formatting options.

Content pane—The right-hand pane displays the help information for a topic.

2

PROVISIONING DEVICES WITH NETHORIZHON

This chapter describes how to provision your device using NetHorizon. It includes the following topics:

Basics

Chassis procedures

SNMP configuration

Device configuration

Card configuration

Port status

Port configuration

SFP/XFP Information

GPON configuration

GPON OMCI configuration

GPON ONT Inventory Tool

Voice configuration

Data configuration

IP configuration

Bridge configuration

Multicast control list configuration

Redundancy overview

Automatic protection switching (MALC and Raptor only)

Administration procedures

Running diagnostics

Traps

Alarms

Basics

Topics:

[Adding maps and changing the default ZMS map](#)
[Adding a region or subregion](#)
[Navigating regions and subregions](#)
[Modifying a region or subregion](#)
[Deleting a region or subregion](#)
[Adding a device](#)
[Autodiscovering devices](#)
[Deleting a device](#)
[Managing a device](#)
[Finding a device](#)
[Moving a device to a different region or subregion](#)
[Finding an object](#)
[Finding a port by its serial number](#)
[Locating a device in the network using its MAC address](#)
[Adding topology links to ZMS maps](#)
[Using the message console window](#)
[Selecting templates](#)

Adding maps and changing the default ZMS map

You can change the default ZMS map. This is the map that displays when NetHorizon starts up.



Note: Custom maps apply only for new regions or subregions created on those maps. The devices or objects created in the DefaultRegion are always shown on the default map (the world map).

ZMS also enables you to add new maps to the NetHorizon client. You can change the default map from a world map to any map loaded on the server as well as select a different map as the background for new regions or subregions.

Use the following guidelines when installing maps:

- Maps can be in any of the following formats: .ivl, .gif, .jpg, .jpeg, .jif

When specifying map images, the file extensions need to be lower case, for example .gif, .jpeg, or .jif. Upper case file extensions are not supported.

- The image size should be approximately 1050x850 pixels in order to maintain good resolution.

To change the default maps:

- 1 Telnet to the ZMS server as *root* user.
- 2 Change to the */zms/lib* directory on the ZMS server:
`cd /zms/lib`
- 3 Copy the *zmsclasses.jar* file, save a backup file in the current directory:
`cp zmsclasses.jar zmsclasses.jar.original`
- 4 Copy the *zmsimages.jar* file, save a backup file in the current directory:
`cp zmsimages.jar zmsimages.jar.original`
- 5 Create two new temporary directories on the ZMS server:
`mkdir temp1 temp2`
- 6 Change to the *temp1* directory on the ZMS server:
`cd temp1`
- 7 Extract the contents of *zmsclasses.jar* file:
`jar xf ../zmsclasses.jar`
- 8 Change to the properties directory on the ZMS server:
`cd com/zhone/zms/properties`
- 9 Open the editor of the *NetHorizhon.properties* file:
`vi NetHorizhon.properties`
- 10 If you want to change the background map for the regions or sub-regions, change the **Region_Map** variable in the *NetHorizhon.properties* file.
Search **Region_Map** variable in the file:
`/Region_Map`
- 11 Add a new map name to the **Region_Map** variable:
`Region_Maps=world.ivl,north
america.ivl,europe.ivl,usa.ivl,blank.jpg,newworldmap.j
pg`
- 12 If you want to change the global map, change the **Global_Map** variable in the *NetHorizhon.properties* file.
Search **Global_Map** variable in the file:
`/Global_Map`

- 13** Modify the “**Global_Map=world.ivl**” in the *NetHorizon.properties* file to the new custom map, for example, “**Global_Map=newworldmap.jpg**”.

- 14** Save the change.

```
:wq
```

- 15** Change to the *temp2* directory on the ZMS server:

```
cd /zms/lib/temp2
```

- 16** Extract the contents of *zmsimages.jar* file:

```
jar xf ../zmsimages.jar
```

- 17** Change to the *maps* directory on the ZMS server:

```
cd com/zhone/zms/cz/resources/graphics/maps
```

- 18** Copy your new map file (“*newworldmap.jpg*”) from the base directory to the current directory.

```
cp <BaseDir>/newworldmap.jpg .
```

- 19** Change to the *temp1* directory on the ZMS server:

```
cd /zms/lib/temp1
```

- 20** Create the *zmsclasses.jar* file in the current directory:

```
jar cf ../zmsclasses.jar com
```

- 21** Change to the *temp2* directory on the ZMS server:

```
cd /zms/lib/temp2
```

- 22** Create the *zmsimages.jar* file in the current directory:

```
jar cf ../zmsimages.jar com
```

- 23** Change to the *zms/lib* directory on the ZMS server:

```
cd /zms/lib
```

- 24** Remove these two temporary directories that are no longer necessary:

```
rm -rf temp1 temp2
```

- 25** Add new security signing information, so that the signing information is consistent for all files. When ask for password enter: **zhonezms**.

```
jarsigner -keystore myKeystore zmsclasses.jar zhone
```

- 26** Add new security signing information. When ask for password enter: **zhonezms**.

```
jarsigner -keystore myKeystore zmsimages.jar zhone
```

27 Restart the ZMS application:

```
/zms/bin/zms start
```

28 Log back in to the NetHorizhone client.

After launching NetHorizhon, the new map will be displayed as the default.

Adding a region or subregion

Before you can add devices to ZMS, you must configure a region. Up to three levels of subregions can be added to regions for more detailed device grouping.

1 Right click the region or subregion icon and select **Add**.

The **Add Region Configuration** or **Add Subregion Configuration** dialog box appears.

2 In the **Name** box, enter the name associated with the region or subregion.

3 In the **Map Name** field, choose the map location you want to use.

Use the scroll bars to display the portion of the map you want to use as the regional or subregion map.

As you move your cursor over the map, NetHorizhon displays the latitude and longitude of the cursor location.

4 Click **Edit**.

5 Holding down the Shift key, click on the map to define at least three points for the device.

6 Click **Done**.

The regional or subregional boundaries appear on the map.

7 Click **Add**.

The region or subregion now appears on the map marked by the specified boundaries.



Note: If the region or subregion configuration is set to *read*, users cannot create, modify, or delete the regions or subregions. However, actions on the entities within the region/subregion, such as devices and cards, are allowed.

Related topics:

[Navigating regions and subregions on page 54](#)

[Modifying a region or subregion on page 54](#)

[Deleting a region or subregion on page 55](#)

Navigating regions and subregions

To increase magnification of your map, click **Zoom In**.

To decrease magnification of your map, click **Zoom Out**.

To set your map to a specific area, click **Zoom to Designated Area**. Using the cursor, point and drag diagonally to draw a selection border around the area. NetHorizon magnifies your map to the specified area.

To specify boundaries, click **Edit**.

To modify existing boundaries, click a polygon point and drag and drop it to the map location you want.

To clear existing boundaries, click **Clear**.

To specify new boundaries, shift-click on the map to specify polygon points (minimum 3, maximum 10 points).

As you specify points, NetHorizon draws a polygon that represents the region or subregion boundaries.

When you have finished specifying boundaries, click **Done**.

To reposition the region, click on the region or subregion and drag and drop it to the map location you want.

To save your changes, click **Add** or **Modify**.

Modifying a region or subregion

- 1 Right click the region or subregion icon and select **Modify**.

The **Modify Region Configuration** or **Modify Subregion Configuration** dialog box appears.

- 2 Make modifications to the region name in the **Name** box.
- 3 To make modifications to the region or subregion area, click **Edit** in the **Map** field.
- 4 Reposition region area in the in the **Map** field.
- 5 Click **Done**.
- 6 Click **Close** when you are finished modifying the region or subregion.



Note: If the region or subregion configuration is set to *read*, users cannot create, modify, or delete regions. However, actions on the entities within the region or subregion, such as devices and cards, are allowed.

Related topics:

[Adding a region or subregion on page 53](#)

[Navigating regions and subregions on page 54](#)

[Deleting a region or subregion on page 55](#)

Deleting a region or subregion

To delete a region or subregion, you should first delete all the devices in this region or subregion.

- 1 Expand the desired region or subregion.
- 2 Right-click a device and select **Delete**, or select **Edit > Delete**.
NetHorizon deletes the device.
- 3 Make sure all the devices in this region or subregion are deleted.
- 4 Right click the region or subregion icon and select **Delete**.

A prompt appears: “Deleting this object also deletes any objects configured on it. Do you want to continue?”

- 5 Click **OK**.

The selected region or subregion is removed from the navigation display.

Related topics:

[Adding a region or subregion on page 53](#)

[Navigating regions and subregions on page 54](#)

[Modifying a region or subregion on page 54](#)

[Deleting a device on page 57](#)

Adding a device

You must add a device to NetHorizon before you can manage it. Devices to be added must be reachable over an IP network and you must know the SNMP read-write community name (the default is ZhonePrivate).

Managing a device across an interface with a source based route active on it may interfere with the device source based routing.

For the IPDSLAM devices (2600, 4200, 8620, 8820, 4000, and 12000), use the Web Interface to ensure SNMP is enabled on the device before adding the device to ZMS. Some uplink types and cards may not be supported in ZMS. See the Release Notes for a complete list of the supported uplinks and cards.

To add a device:

- 1 Right-click a device icon or region icon, and select **Add**.

The **Add Device Configuration** dialog box appears.

- 2 Enter the following information:

- **IP Address**

Enter the device IP address.

- **SNMP Version**

SNMP V1/V2: Default value. When the users selected SNMP V1/V2, **Community Name** is mandatory.

SNMP V3: When the users selected SNMP V3, **Community Name** is not displayed, and all the SNMP V3 related parameters (i.e. Username, Authentication Protocol, Authentication Password, Privacy Protocol, and Privacy Password) are internally setup.

- **Community Name**
- **ZMS IP Address**

Click **Add**.

At the confirmation message, click **OK**.

NetHorizon connects to the device and starts the config sync process. For the IPDSLAM devices, the config sync process is not performed.

Keep in mind that synchronizing may take several minutes, depending on the configuration. You cannot perform tasks on objects that appear dimmed. You can perform tasks on other devices.

When the device synchronization completes, the dialog box displays the status **Complete**.

- 3 After config sync is done, to view any errors encountered, click **Show Errors** (**Show Errors** appears dimmed if there are no errors).

Click **Show Summary** to view a summary of the config sync process.

- 4 Click **Done**.

The device icon with its name, IP address, and model appears in the tree view. From here, you can manage it.

For the IPDSLAM devices (2600, 4200, 8620, 8820, 4000, and 12000), double-clicking the device in the ZMS tree launches the Web Interface tool for that device. To receive traps in ZMS, add the ZMS server IP address as one of the trap destinations.

Related topics:

[Adding a single card on page 131](#)

[Adding multiple cards on page 132](#)

[Adding redundant MALC, MXK and Raptor cards on page 133](#)

[Modifying a card's ATM bandwidth settings on page 144](#)

[Autodiscovering devices on page 56](#)

Autodiscovering devices

NetHorizon supports the use of autodiscovery to add devices for management. Devices to be added must be reachable over an IP network and you must know the SNMP read-write community name (the default is ZhonePrivate).

The autodiscovery features can be run on-demand or scheduled. The autodiscovery process searches a specified range of IP addresses and optionally filters the devices by selected type(s).

When devices are found, NetHorizon automatically adds them to the Default Region as they are discovered. The results of the autodiscovery process are stored in Discovery Log file, available from Tools > Task Log Files.

To run the autodiscovery process:

- 1** From the Tools menu, click **Autodiscovery**.

The **Autodiscovery** dialog box appears.

- 2** Enter the following information:

Start IP Address

End IP Address

Community Name

SNMP Timeout (msecs)

Ensure that the timeout value accounts for network delay, while not over extending the time required to complete the discovery process. An increased SNMP timeout period allows for more delay in the device response times, while also increasing the discovery period.

Device Type: Click the Browse button to display a list of devices types. Hold Ctrl to select multiple device types. Non-SLMS devices are grouped under the Fault Management Device type.

Immediate/Schedule: Click the desired option. For scheduled discovery, also enter the time to initiate the discovery process.

- 3** Click **Apply** to configure the specified autodiscovery settings.

SNMP pings are initiated to located the devices with the specified parameters. Responses must be received within the SNMP timeout period.

Discovered devices are added to the Default Region in the NetHorizon Tree. The results of the autodiscovery process are stored in Discovery Log file, available from Tools > Task Log Files.

- 4** Click **Close** to exit the dialog.

Related topics:

[Adding a single card on page 131](#)

[Adding multiple cards on page 132](#)

[Adding redundant MALC, MXK and Raptor cards on page 133](#)

[Modifying a card's ATM bandwidth settings on page 144](#)

Deleting a device

To delete a device, right-click the device and select **Delete**, or select **Edit > Delete**.

NetHorizon deletes the device.

Related topics:

[Adding a device on page 55](#)

[Managing a device on page 58](#)

Managing a device

After a device has been added to NetHorizon, right-click the device and select **Modify**, or select **Edit > Modify** to provision the device.

Related topics:

[Adding a device on page 55](#)

[Deleting a device on page 57](#)

[Finding an object on page 59](#)

Finding a device

There are two ways to find a device:



Note: The wildcard “*” can be used to find a device while entering either device name or device IP. For example: MXK*, 10.51.1.*.

- 1 1st method: After a device has been added to NetHorizon, right-click a region or subregion and select **Locate Device by Name or IP**. Enter the desired device name or IP address and click **Find**. The list of device found by Device Name or Device IP will be displayed in the Locate Device By Name or IP window. To highlight the device in the tree, just select this device in the list, and click **Navigate To Tree**.
- 2 2nd method: After a device has been added to NetHorizon, select **Tools > Locate > Locate Device by Name or IP**. Enter the desired device name or IP address and click **Find**. The list of device found by Device Name or Device IP will be displayed in the Locate Device By Name or IP window. To highlight the device in the tree, just select this device in the list, and click **Navigate To Tree**.

Related topics:

[Adding a device on page 55](#)

[Managing a device on page 58](#)

[Deleting a device on page 57](#)

[Finding an object on page 59](#)

Moving a device to a different region or subregion

You can move devices from one region or subregion to another. To move a device:

- 1 Right-click a device and select **Change Regions** or **Change Subregions**.

The **Move Device to a Different Region** or **Move Device to a Different Subregion** dialog box appears.

- 2 Click the Browse button to choose a new region or subregion for the device.
After the device has been moved, NetHorizon will automatically refresh the display.

Finding an object

- 1 After an object has been added to NetHorizon, select **Tools > Find Objects**. The Find Objects dialog appears.

- 2 Enter the desired object information in the **Find Objects** dialog.

- Select Parent: This value specifies the scope of the find operation. Only objects that are under the specified node in the navigation tree will be returned. Click the browse button to select a node. (mandatory)

- Name: This field is used to filter objects by their name. If a value is entered in this field, only objects that have names that match the specified pattern will be included in the response.

This field accepts the * wildcard value if wildcard search is enabled in the *NetHorizon.properties* file. For example, if enter **1-1*** in the Name field, only objects that have a name starting with 1-1 will be included in the response. It could be 1-1-x-x and 1-1x-x-x.

Note that the name is case-sensitive. For example, if enter ***gpon*** in the Name field, the card with name GPON will not be displayed in the response.

- VLAN ID: This field is used to filter objects by VLAN. A value should only be entered in this field when searching for bridges or IP interfaces. Because these are the only objects that have a VLAN. If a value is entered in this field, only objects on the specified VLAN will be included in the response.
- Ending VLAN ID: This field is used with the VLAN ID field to filter objects by VLAN ID range. Leaving this field empty will search for the VLAN ID given in the VLAN ID field.
- Port Description: This field is used to filter objects by the description. This field appears only after selecting All Types, Ports, Bond Groups, or ONT/ONUs in the Type field.

If a value is entered in this field, only ports or bond groups that have descriptions that match the specified pattern will be included in the response.

By default, this field does not accept wildcard searches. This field accept the * wildcard value if wildcard search is enabled in the *NetHorizon.properties* file. For example, if enter **pots*** in the Description field, only ports, bond groups, ONT/ONUs that have a description string starting with pots will be included in the response. It could be Pots 1 and pots1. It is not case-sensitive.

- **ONT Serial No Vendor Id:** This field is used to filter ONT/ONU objects by the ONT serial number vendor ID, such as: ZNTS. It only appears after selecting ONT/ONUs in the Type field.

This field accept the * wildcard value if wildcard search is enabled in the *NetHorizon.properties* file. Note that the vendor ID is case-sensitive.

- **ONT Serial No Vendor Specific:** This field is used to filter ONT/ONU objects by the ONT serial number vendor specific, such as: 266999. It only appears after selecting ONT/ONUs in the Type fields.

This field accept the * wildcard value if wildcard search is enabled in the *NetHorizon.properties* file.

- **Type:** This field is used to specify the object type to search for. Only objects that match the specified type will be returned. It could be All Types, Cards, Bond Groups, Ports, Bridges, IPs, ONT/ONUs.

- 3 Click **Find** to locate the object(s). The list of matched objects will be displayed.

This example specifies the following values in each field:

Select Parent= Regions, Name= 1-1*, VLAN ID=200, Type= Bridges.

The response will contain bridge records on the all regions, have a name that starts with 1-1, and are on VLAN 200.

- 4 Right-click a displayed object and select the desired menu item to access more configuration dialogs.
 - Select the **Modify** and **View** menu item to access the modify and view screens for the selected object.
 - Select **Manage Bridging**, **Manage IP**, or **Manage Ports** menu item to display just the bridge, IP objects, or ports under the selected object.
 - Select the **View alarms** menu item to display just the alarm under the selected object.
 - Select the **Navigate to the Tree** menu item to move the active cursor to the selected object in the ZMS navigation tree.

Related topics:

[Adding a device on page 55](#)

[Managing a device on page 58](#)

[Deleting a device on page 57](#)

Finding a port by its serial number

ZMS can locate a port with its serial number (vendor specific) in the navigation tree if this port has been assigned serial numbers.

- 1 After an ONT has been assigned a serial number, select **Tools > Locate > Locate Port by Serial Number** menu item from the menu bar.

The **Locate Port by Serial Number** dialog box appears.

- 2 Enter the serial number in the **Serial Number Vendor Specific** field, and then click **Locate**.

The matched port will be highlighted in the navigation tree.

Locating a device in the network using its MAC address

If the MAC address exists, MXK can always locate the MXK ONU (GPON) or Active Ethernet (AE) interface through ZMS. However, locating the CPE LAN interface is a best effort. It can only do that if the CPE is configured with USP and RG mode is rg-bridged.

Depending on the network topology, it is possible the same MAC address is learned at multiple interfaces if the bridges are of TLS. In that case, Find MAC will display the first interface the MAC address is located.

- 1 Select **Tools > Locate > Locate Port by MAC Address** menu item from the menu bar.

The **Locate Port by MAC Address** dialog box appears.

- 2 Enter the hexadecimal MAC address of the port, and then click **Locate**. ZMS searches all reachable devices in the network, and display the matched port information in the **Locate MAC Address Results** window.
- 3 To navigate to the ONU where the MAC address resides in the navigation tree, click the **Navigate to Physical** button.

This feature requires MX/MXK/MXK-F running software versions supporting this feature.

Please refer to MXK/MX/MXK-F release notes for feature support versions.

Adding topology links to ZMS maps

You can add and manage topology links which can be used to interconnect MXKs, MALCs, and XPs devices on the ZMS geographical map view.

ZMS also allows defining a label when a topology link is created. This label can be used to store link or circuit information which might be required by the Network Operation Center (NOC).

For RPR rings and topologies where devices are physically linked together, ZMS automatically adds the topology links for these physical links.

To add or manage topology links:

- 1 For RPR rings and other topologies where devices are physically connected, the topology links automatically appear in the ZMS maps.
- 2 To display alarms for the physical links, right-click the link and select the alarms option.

Topology links can also be used with subregions.

- 3 For devices that are not physically linked, in the ZMS map right-click a device and select **Add Link To**. The **Add Link** dialog box appears.
- 4 Select the nodes to be joined by the logical link in the ZMS map, enter a map name and a link description (up to 128 characters), and then click **Add**. The logical link appears in the ZMS map.

ZMS currently allows customers to create a topology link which can be used to interconnect MXKs, MALCs, and XPs on the ZMS geographical map view. With this new enhancement, ZMS allows defining a label when a topology link is created. This label can be used to store link or circuit information which might be required by the NOC.

To modify the link description, right-click on the link in the ZMS map and select **Modify Description**. The **Modify Link Description** dialog box appears.

Change the description and click **Modify**.

Using the message console window

The console windows allows you to view system messages (such as errors that may occur as you configure a device) generated by NetHorizon.

To view system messages, select **View > Console** from the menu bar.

NetHorizon displays the Console dialog box, listing messages generated during your current NetHorizon session.

To clear the Console dialog box and start displaying new messages, select **File > Edit > Clear** (or click the Clear icon).

To close the Console dialog box, click **File > Close** from the Console dialog box.

Selecting templates

Select a template to use to configure the object. Templates can either be user-defined or system default templates.

See also:

[Data templates on page 361](#)

[Physical port templates on page 148](#)

[Voice configuration templates on page 306](#)

[External DHCP subnet template on page 437](#)

[Packet rule member template on page 438](#)

[Packet rule group template on page 438](#)

[CPE Management Templates on page 299](#)

ZMS Web Client Launch

Chassis procedures

This section lists the procedures related to the chassis and card usage.

[Adding a single card on page 131](#)

[Adding multiple cards on page 132](#)

[Adding redundant MALC, MXK and Raptor cards on page 133](#)

[Enabling a card on page 133](#)

[Deleting a card on page 138](#)

[Modifying a card's ATM bandwidth settings on page 144](#)

[Viewing card state on page 136](#)

[Rebooting a single card on page 136](#)

Templates

Configuration templates are available to standardize common configurations.

[Voice configuration templates on page 306](#)

[Physical port templates on page 148](#)

[Creating ATM traffic descriptor configuration templates on page 361](#)

[Creating AAL2 to GR-303 voice configuration templates on page 308](#)

[Creating POTs to AAL2 configuration templates on page 314](#)

[Creating AAL2 to V5.2 \(PSTN\) voice configuration templates on page 306](#)

Device

[Performing immediate configuration backup on a single device on page 75](#)

[Configuring a clock source on page 139](#)

[Rebooting a device on page 80](#)

[Performing immediate synchronization with a single device on page 81](#)

[Viewing clock source status on page 140](#)

[Shelf monitoring on page 140](#)

Management

[Adding an SNMP access list on page 66](#)

[Adding an SNMP community name on page 64](#)

[Configuring a trap forwarding address on page 66](#)

[Deleting a trap forwarding address on page 68](#)

[Editing a configuration on page 79](#)

[Restoring a configuration on page 80](#)

[Viewing a trap forwarding addresses on page 67](#)

Services

[Adding ATM cross connect on MALC, and Raptor using the wizard on page 364](#)

[Adding an ATM cross connect \(VP switched connection\) on page 369](#)

[Adding voice gateway AAL2 subscribers on page 347](#)

[Adding POTS to AAL2 voice connections using the wizard \(MALC\) on page 318](#)

[Changing VCL rates on page 141](#)

Software images

[Deleting a software image on page 138](#)

[Downloading a software image to a single or multiple devices on page 71](#)

[Setting the card default image on page 137](#)

SNMP configuration

Topics:

[Adding an SNMP community name](#)

[Configuring a trap forwarding address](#)

[Adding an SNMP access list](#)

[Viewing a trap forwarding addresses](#)

[Deleting a trap forwarding address](#)

Adding an SNMP community name

SNMP community name acts as passwords. SNMP managers require the community name to access the system.



Note: Configuring a community name disables the ZhonePrivate default community name. If you configure a community name, you must change community name ZMS uses to manage the device.

To add an SNMP community name:

- 1 From the **Modify Device** dialog box, click **Community Names** in the tree view.

The **Community Names** window appears.

- 2 Click **Add**.
- 3 The **Add Community Name** dialog box appears.
- 4 Specify a **Name**.
- 5 Define an access level.
- 6 (Optional). Click the browse button to select an access list to associate with this community name.
- 7 (Optional). If you want this community name to be used by ZMS to manage the device, select **Set as preferred community name**.
- 8 Click **Add**, then **Close** to save the information.

When you return to the **Community Names** dialog box, the name you created is listed.

Related topics:

[Adding an SNMP access list on page 66](#)

[Configuring a trap forwarding address on page 66](#)

[Deleting an SNMP community name on page 65](#)

Deleting an SNMP community name

SNMP community name acts as passwords. SNMP managers require the community name to access the system.

To delete an SNMP community name:

- 1 From the **Modify Device** dialog box, click **Community Names** in the tree view.

The **Community Names** window appears.

- 2 Highlight a community name to delete.
- 3 Click **Delete**, then **Close**.

When you return to the **Community Names** dialog box, the name you deleted is no longer listed.

Related topics:

[Adding an SNMP access list on page 66](#)

[Configuring a trap forwarding address on page 66](#)

Adding an SNMP access list

Access lists are used to limit which IP addresses can use individual community names to access a particular device. If no community name exists on a device, ZMS uses the default community name **ZhonePrivate**, which allows read and write access to all parameters on the device (Administrator access).

To add an access list:

- 1 Right-click a device and select **Modify**.

The **Modify Device** dialog box appears.

- 2 From the **Modify Device** dialog box, click **Access List** in the tree view.

The **Access List** window appears. If there are any access lists configured, they are displayed.

- 3 Click **Add**.

The **Add Access List** dialog box appears.

- 4 (Optional). Specify a **Name**.

- 5 Click **Access List Entries** in the tree view.

- 6 Click **Add**.

The **Add Access Lists** dialog box appears.

- 7 Enter an **IP Address** for the SNMP manager that is allowed access to this device.

- 8 Click **Add** after entering an IP address.

- 9 After you have added all the IP addresses to the list, click **Close**.

When you return to the **Access List** dialog box, the access list you entered is listed.

Related topics:

[Adding an SNMP community name on page 64](#)

[Viewing a trap forwarding addresses on page 67](#)

Configuring a trap forwarding address

Trap destinations use the SNMP community name **ZmsTrapPrivate**. To add a trap destination:

- 1 Right-click a device and select **Modify**.

- 2 From the **Modify Device** dialog box, click **Trap Configuration** in the tree view.

The **Trap Configuration** window appears.

- 3 Click **Add**.

The **Add Trap Configuration** dialog box appears.

- 4 (Optional). Specify a **Name**.
- 5 Click **Trap Configuration** in the tree view.
- 6 In the **Destination** field, enter the IP address to which you want traps forwarded.
- 7 Select a severity level. This defines the level of traps that are sent to the destination.
- 8 Set **Admin Status** to **Enabled**.
- 9 Click **Add** to save the information, then **Close**.

When you return to the **Trap Forwarding** dialog box, the forwarding IP address you entered is listed.

Related topics:

[Adding an SNMP community name on page 64](#)

[Adding an SNMP access list on page 66](#)

[Deleting a trap forwarding address on page 68](#)

[Viewing a trap forwarding addresses on page 67](#)

Adding a trap forwarding address

Trap destinations use the SNMP community name **ZmsTrapPrivate**. To add a trap destination:

- 1 Highlight a device and select **View > Faults > Manage Traps**.
The **Add Trap Configuration** dialog box appears.
- 2 Click **Add**.
The **Enter IP Address** dialog box appears.
- 3 In the **IP Address** field, enter the IP address to which you want traps forwarded.
- 4 Enter a community name.
- 5 Click **OK** to save the information, then **Close**.

When you return to the **Trap Forwarding** dialog box, the forwarding IP address you entered is listed.

Related topics:

[Adding an SNMP community name on page 64](#)

[Adding an SNMP access list on page 66](#)

[Deleting a trap forwarding address on page 68](#)

[Viewing a trap forwarding addresses on page 67](#)

Viewing a trap forwarding addresses

- 1 Right-click a device and select **Modify**.

- 2 From the **Modify Device** dialog box, click **Trap Configuration** in the tree view.

The **Trap Configuration** window appears.

- 3 Highlight a trap destination, then click **View**.

Related topics:

[Configuring a trap forwarding address on page 66](#)

[Deleting a trap forwarding address on page 68](#)

Deleting a trap forwarding address

To delete a trap forwarding address:

- 1 Right-click a device and select **Modify**.
- 2 From the **Modify Device** dialog box, click **Trap Configuration** in the tree view.

The **Trap Configuration** window appears.

- 3 Highlight a trap destination, then click **Delete**.
- 4 At the confirmation prompt, click **OK**.

Related topics:

[Configuring a trap forwarding address on page 66](#)

[Viewing a trap forwarding addresses on page 67](#)

Device configuration

Topics:

[Downloading files to a single or multiple devices](#)

[Downloading a software image to a single or multiple devices](#)

[Backing up configurations](#)

[Performing hitless software upgrades](#)

[Performing immediate configuration backup on a single device](#)

[Deleting a software image](#)

[Flashing the software image](#)

[Editing a configuration](#)

[Rebooting a device](#)

[Restoring a configuration](#)

[Performing immediate synchronization with a single device](#)

[Performing scheduled synchronization with a single device or multiple devices](#)

- Upgrading a device using ZMS
- Configuring device identity
- Configuring device administration settings
- Configuring MXK user privilege management
- Configuring MXK users in bulk
- Configuring shelf inventory manager
- Enabling or disabling secure mode on device
- Configuring device alarm level settings (alarm suppression)
- Configuring ZMS connectivity settings
- Configuring device community names
- Configuring device access lists
- Configuring device trap configuration settings
- RADIUS Configuration
 - Configuring user authentication method
 - Configuring RADIUS client profiles
 - Configuring RADIUS index
- Configuring device location settings
- Configuring voice DSP settings
- Configuring DSCP to COS (802.1p)
- Configuring device video source settings
- Configuring device system clock settings
- Configuring device NTP configuration settings
- Configuring device bulk statistics configuration settings
- Configuring device global STP parameters
- Configuring port access security
- Configuring GigaMux 1600/3200 device settings
- Configuring CPE device settings
- Configuring EZ Touch Provisioning™ CPEs
- Configuring Malc XP device settings
- Configuring Raptor XP device settings
- Configuring MXK device settings
- Configuring 1U MX-150 device settings
- Configuring 1U MX-160, MX-161, MX-162 device settings
- Configuring 1U MX-180, MX-280 device settings

[Configuring 1U MX-260, MX-261, MX-262 device settings](#)

[Configuring 1U MXP-150 device settings](#)

[Configuring 1U MXP-160, MXP-260 device settings](#)

[Configuring 1U MXP-180, MXP-280 device settings](#)

[Configuring 1U MXK-194, MXK-198 device settings](#)

[Secure Shell \(SSH\)](#)

[Configurable Temperature Alarm Severity and Ranges](#)

[Create vdsl-vect-config](#)

.

.

Downloading files to a single or multiple devices

Use this procedure to download the files (i.e. HTTP tar file and CPE/ONT image file), except the software image load, to the device. The files are downloaded from the directory */tftpboot/filedownload* in the ZMS server to the directory */card1* in the device.

1 To download files to a single device:

a right-click the device and select **Download File**.

NetHorizon displays the **Download File** dialog box for the selected device.

b Select one or multiple files to download in the **Download File** dialog box and click **Download**.

2 To download files to a single or Multiple (bulk) devices:

a Select **Tools > Download File**.

NetHorizon displays multiple devices and files in the **Bulk File Download** dialog box.

b Complete the parameters in the **Bulk File Download** dialog box:

Select the type of device— Select the type of device to receive the download. A list of available devices appears.

Select Specific Devices for downloading image— Select a single or multiple devices to which the file will be downloaded. Use shift key or Ctrl key to select multiple devices.

Select File to Download— Select a single or multiple files to be downloaded. Use shift key or Ctrl key to select multiple files.

Once or Immediate—Specify whether to download the files at the scheduled date and time or immediately.

Time— If selected **Once**, you can specify the scheduled date and time to download the files in the displayed format. By default, the current date is displayed.

- c** Click **Apply**.
- d** To check the status of the file downloads or to manage scheduled file downloads, click **Manage**.

The **Manage File Downloads** dialog box appears.

- To delete a scheduled file download, select the desired download and click the **Delete Load** button.
- To delete a device from a scheduled file download, select the desired device and click the **Delete Device** button.
- To modify a scheduled file download, select the desired download, specify the desired file to download and click the **Apply** button.
- When finished managing software downloads, click the **Close** button.

Related topics:

[Performing immediate upgrade on a single ONT/ONU on page 237](#)

[Performing immediate/scheduled upgrade on multiple ONT/ONUs on page 239](#)

[Performing auto upgrade on an ONT/ONU on page 241](#)

[Downloading a software image to a single or multiple devices on page 71](#)

Downloading a software image to a single or multiple devices

Use this procedure to download the software image to a MALC/MXK/XP or Raptor Uplink card.

To perform a hitless upgrade, follow the procedure in [Performing hitless software upgrades on page 74](#).

- 1** To download a software image to:
 - Single device, right-click the device and select **Download Software Image**.
NetHorizon displays the **Download Software Image** dialog box for the selected device. Complete the parameters in the **Download Software Image** dialog box and click **Download**.
 - Single or Multiple (bulk) devices, select **Tools > Download Software Image**.
NetHorizon displays multiple devices in the **Download Software Image** dialog box.

2 Complete the parameters in the **Download Software Image** dialog box:

Select the type of device— Select the type of device to receive the download. A list of available devices appears.

Select Specific Devices for downloading image— Select a single or multiple devices to which the software image will be downloaded.

Primary Load Server—Enter the IP address of the primary software load server. If no primary load server is available, set this value to 0.0.0.0. If the system is unable to load the software file from the primary load server, the system attempts to load the software from the secondary load server.

Secondary Load Server—Enter the IP address of the secondary or back-up software load server.

TFTP Sub-Directory (optional)—Enter the desired files to be downloaded if the files are in a sub-directory under the TFTP directory. The default TFTP directory on the ZMS server is /tftpboot. If this field is left blank, ZMS assumes that the files to be downloaded are located in /tftpboot.

Select TFTP Server File Name—Enter the desired filename or click the browse button and select single or multiple filenames to be downloaded from the File Selection dialog. The list of files is not verified with the installed files. Ensure the selected file is actually available on the /tftpboot server.

Device Sub-Directory (optional)—Enter the desired files to be downloaded into a device sub-directory. If a value exists in this field, all downloaded files will be put in this sub-directory. Ensure the selected directory is actually existed on the device.

Save On Device As— Displays the selected filename for verification. This filename may be changed if the downloaded image file will have a different filename than the default image name.

String to append to all filenames (i.e. “.old”)— Specify a value to be appended to all downloaded filenames. If the field is left blank the files will be downloaded with the same name as they have on the TFTP server.

Auto Flash—If this value is checked, then ZMS will issue the flash image command after all files have downloaded. The flash image command is only issued if the correct raw file is one of the files being downloaded.

Auto Upgrade—This option is available if the **Auto Flash** is checked. There are three values in this field:

- No Upgrade: No commands are sent to the device.
- Reboot Upgrade: The reboot command will be issued after a successful image flash response is received.

- **Hitless Upgrade:** If uplinks are redundant, the command to perform a hitless upgrade will be issued after a successful image flash response is received. If uplinks are not redundant, the reboot command will be issued after a successful image flash response is received.

Immediate/Schedule—Specify whether to download the files immediately or at the scheduled date and time.

Time—Specify the scheduled date and time to download the files in the displayed format. By default, the current date and time are displayed.

3 Click **Download**.

For immediate downloads, NetHorizon downloads the software image. Keep in mind that it can take some time for the download process to complete.

For scheduled downloads, NetHorizon schedules the downloads of the selected software images.

For example:

If the TFTP directory looks like:

```
/tftpboot
    1.13.2.1
        malcrprgige.bin
        malcrprgigeraw.bin
    1.14.1.1
        malcrprgige.bin
        malcrprgigeraw.bin
```

To download all 1.13.2.1 files to an "old" sub-directory on the Malc, use:

```
TFTP Sub-Directory = 1.13.2.1
Device Sub-Directory attribute = old
TFTP Server filename =
malcrprgige.bin,malcrprgigeraw.bin
String to append to all filenames =
```

To download all 1.13.2.1 files to the top level directory on the MALC, but name the files malcrprgige.bin.old and malcrprgigeraw.bin.old:

```
TFTP Sub-Directory = 1.13.2.1
Device Sub-Directory attribute =
TFTP Server filename =
malcrprgige.bin,malcrprgigeraw.bin
String to append to all filenames = .old
```

4 To check the status of the download or to manage scheduled downloads, click **Manage**.

The **Manage Software Download** dialog box appears.

- To delete a scheduled image download, select the desired download and click the **Delete Load** button.
- To delete a device from a scheduled image download, select the desired device and click the **Delete Device** button.
- To modify a scheduled image download, select the desired download, specify the desired download changes and click the **Apply** button.
- When finished managing software downloads, click the **Close** button.

5 To view the status of images downloads, select **Tools> Download Image Log Viewer**. The Download Image Log Viewer dialog appears.

Related topics:

[Deleting a card on page 138](#)

[Enabling a card on page 133](#)

[Flashing the software image on page 77](#)

[Rebooting a single card on page 136](#)

[Setting the card default image on page 137](#)

[Upgrading a device using ZMS on page 78](#)

[Viewing card state on page 136](#)

[Downloading files to a single or multiple devices on page 70](#)

Performing hitless software upgrades

NetHorizon enables you to perform hitless software upgrades. You can perform the hitless software upgrades in the **Tools > Download Software Image** dialog box or **Edit > Equipment Provisioning > Device Configuration > Upgrade Software Image** dialog box.

Hitless upgrades allow for context switching between an active and passive uplink cards so that firmware upgrades can occur on a non-active card:

1. It is mandatory to have two uplink cards to be able to perform hitless upgrade.
2. ZMS client users will need to download the raw files in addition to the regular binary files.
3. Active uplink card will then put the new image on standby card and reboot the standby card.
4. Once the standby card comes up and start running with the new code, active uplink card will update itself with the new image and reboot itself.
5. In that process, original standby card will be come active and active will become standby.
6. Line cards will be updated with new image and rebooted.

This procedure is only valid when upgrading from 1.12.2.108 or later to a newer release.

To perform a hitless software upgrade:

- 1 In the ZMS tree, select the desired device to upgrade.
- 2 Select **Edit > Equipment Provisioning > Device Configuration > Upgrade Software Image** from the menu bar or right-click and select **Upgrade Software Image**.

The **Upgrade Software Image** dialog box appears with the upgrade option.

- 3 To start the upgrade process, click the **Start** button. This initiates the upgrade process. The **Start** button changes to the **Stop** button to enable termination of the upgrade process.

The following status messages appear at the different stages of the upgrade process

- Upgrade Not Started
- Standby Upgrade In Progress...
- Standby Upgrade Completed
- Standby Upgrade Aborted
- Swact In Progress...
- Swact Completed
- Swact Aborted

Other ZMS operations can be performed while the upgrade process is running.

- 4 To exit the dialog, click the **Close** button.
- 5 For help, click the **Help** button.

Backing up configurations

Configuration back ups can be done immediately before upgrading or after major configuration changes, or scheduled for daily or weekly intervals. ZMS enables configuration backups for single devices or multiple devices. After backing up the configuration, the configuration can be restored on the device at any time.

By default, all 2.3.1.100 and greater MXKs are using the binary format file (infobl.v8) to backup. You have the choice to backup to a text format file while performing immediate configuration backup on a single device, but not when you are performing bulk and scheduled backups.

Performing immediate configuration backup on a single device

To perform an immediate configuration backup on single device:

- 1 Right-click a device and select **Backup Device Configuration**.

The **Backup Device Configuration** dialog box appears for the selected device.

2 Enter the filename and click **Start Backup**.

If you want to backup to a text format file instead of a binary format file, click the **Backup in text format** checkbox.

A dialog box appears showing the backup progress. For GigaMux devices, the filename cannot contain forward or backward slashes.

3 When the backup is complete, click **Close**.

NetHorizon downloads a given device's configuration file and saves it on the ZMS server with the following filename:

*SpecifiedName_date and time of
backup_IPAddress_DeviceType_Device.<txt, bin, or zms>*

Backups of ZMS database files are stored with a .zms filename extension.

The file is stored in a directory named *dumprestore* under the TFTP root directory (*/tftpboot* by default). The TFTP root directory's value is automatically set in the ZMS properties file (*DumpRestore.properties*) when ZMS is installed.

For GigaMux devices, ZMS uses FTP for backup and restore of configurations. The file is stored in the home directory of ZMS FTP user (*/opt/zmsftp* by default). The FTP root directory's value is automatically set in the ZMS properties file (*CSS.properties*) when ZMS is installed.

For IPDSLAMs, the backup and restore feature is supported on the 2600/4200 devices.

Setting backup device configurations

Backup device configurations enable immediate and scheduled configuration backups on single and multiple devices. To perform backup device configurations:

1 From the main menu, select **Tools > Backup Device Configuration**.

The **Backup Device Configuration** dialog box appears for all available devices.

2 Select the desired type of device.

3 Select a single device, or use shift/Ctrl key to select multiple devices in the list of available devices.

4 Click the radio button for the desired backup configuration option:

- Disable

Disables the configuration backup for the selected devices.

- Immediate

Starts the immediate configuration backup for the selected devices.

- Daily

Specifies the desired time to schedule the configuration backup for the selected devices.

- Weekly

Specifies the desired time to schedule the configuration backup for the selected devices.

- 5 Click **Apply** to perform immediate configuration backups or configure scheduled backups.

A dialog box appears showing the backup progress.

When a backup is performed from the **Backup Device Configuration** window, NetHorizon downloads device configuration files and saves them on the ZMS server with the following filename:

AUTO-CURRENT_IPAddress_DeviceType.<txt, bin, or zms>

Backups of ZMS database files are stored with a .zms filename extension.

Backup files are stored in a directory named *dumprestore* under the TFTP root directory (*/tftpboot* by default). The TFTP root directory's value is automatically set in the ZMS properties file (*DumpRestore.properties*) when ZMS is installed.

For GigaMux devices, ZMS uses FTP for backup and restore of configurations. The file is stored in the home directory of ZMS FTP user (*/opt/zmsftp* by default). The FTP root directory's value is automatically set in the ZMS properties file (*CSS.properties*) when ZMS is installed.

- 6 When the backup is complete, click **Close**.

When the next configuration backup is performed on a device, the original configuration backup file is saved with the filename:

AUTO-BACKUP_IPAddress_DeviceType.<bin or zms>

Only one auto-backup file is saved per device. Additional archives of configuration backups must be performed by the user.

Related topics:

[Editing a configuration on page 79](#)

[Restoring a configuration on page 80](#)

[Upgrading a device using ZMS on page 78](#)

Flashing the software image

Flashing a card updates the boot partition on the PC card or flash memory. This is only supported on MALC Uplink cards and Raptor Uplink cards.

You must flash the card before loading the software images.

To flash the card:

- 1 Right-click an uplink card and select **Flash Software Image**.

The **Flash Software Image** dialog box appears.

- 2 Specify the name of the software image for the card.

The following table lists the cards' boot file names.

Card	Name of software image
Uplink-2-GE	<i>malcrprgige.bin</i> <i>malcrprgigeraw.bin</i> (Boot partition image file)
Uplink-DS3/E3-ATM/IP	<i>malcds3f.bin</i> <i>malcds3fraw.bin</i> (Boot partition image file)
Uplink-OC3/STM1-ATM/IP	<i>malcoc3f.bin</i> <i>malcoc3fraw.bin</i> (Boot partition image file)
Uplink-T1/E1-ATM/IP-8	<i>malct1imaf.bin</i> <i>malct1imafraw.bin</i> (Boot partition image file)
Uplink-T1/E1-ATM/TDM/IP-16	<i>malct1e1tdmf.bin</i> <i>malct1e1tdmfraw.bin</i> (Boot partition image file)
UP-O12/S4/GE/TDM-ATM/IP	<i>malcoc12.bin</i> <i>malcoc12raw.bin</i> (Boot partition image file)
UP-O12-S4/HP-GE-LX/T-E1	<i>malcgige.bin</i>
UP-O12-S4/HP-GE-SX/T-E1	<i>malcgigeraw.bin</i> (Boot partition image file)

- 3 Click **Flash**.
- 4 Monitor the progress of the flash process in the Status field. Click **Refresh** to update the status of the operation.

If the card is part of a redundant group, both card's boot partitions will be updated.

Upgrading a device using ZMS

Before upgrading a device using ZMS, make sure you have met the following prerequisites:

- A TFTP server is active on the network and reachable from ZMS
- The software images are loaded on the TFTP server
- The current configuration of the device has been backed up using the **Backup Device** command. See [Backing up configurations on page 75](#).

To upgrade the device software:

- 1 Download the software images to the device. See [Downloading a software image to a single or multiple devices on page 71](#).
- 2 Flash the boot partition of the Infoservices or Uplink card. See [Flashing the software image on page 77](#).

- 3 Restore the device configuration. See [Restoring a configuration on page 80](#).
- 4 Synchronize the device with ZMS. See [Performing immediate synchronization with a single device on page 81](#)

Related topics:

[Downloading a software image to a single or multiple devices on page 71](#)

[Flashing the software image on page 77](#)

[Rebooting a single card on page 136](#)

[Setting the card default image on page 137](#)

[Viewing card state on page 136](#)

Editing a configuration

By editing a configuration, you can use an existing configuration as the basis for another device.



Note: The device that is being provisioned with the edited configuration must have the same hardware set up as the original device.

- 1 Right-click on the device that contains a configuration you want to reuse and select **Edit Device Configuration**.

The **Restore Device Configuration** dialog box appears showing all the backup configuration files for that device.

The configuration files are displayed in the following syntax:

filename_date and time of backup_IP address of device_type of file_device

- 2 Select a file.

The **Details of Configuration** area fills in the information from the configuration file and allowing you to edit the information. At a minimum you must change the IP address of the device.

- 3 After making the necessary changes, enter a new file name for the modified configuration file in the **Save As** field.

- 4 Click **OK**.

ZMS saves the configuration file.

- 5 To apply this configuration to a device, right-click the device and select **Restore Device Configuration**.

Related topics:

[Performing immediate configuration backup on a single device on page 75](#)

[Restoring a configuration on page 80](#)

Rebooting a device

To reboot a device:

- 1 Right-click a device and select **Reboot Device**.
- 2 At the confirmation prompt, click **Yes**.

NetHorizon reboots all the cards on the device.

Keep in mind that it can take some time for the reboot process to complete.

Related topics:

[Rebooting a single card on page 136](#)

Restoring a configuration

To restore a device configuration:

- 1 Right-click a device and select **Restore Device Configuration**.

The **Restore Device Configuration** dialog box appears showing all the backed-up configuration files for that device.

The backup configuration files use the following syntax:

SpecifiedName_date and time of backup_IPAddress_DeviceType_Device

- 2 Select a file from the **Restore Device Configuration** dialog box.
- 3 On MALC, and Raptor systems, select the **Reboot device after restoring configuration** option. (On Z-Edge 64 and Sechtor 100A systems, the device will automatically reboot after restoring the configuration.)

On MXK, restore a binary file will automatically check the **Reboot device after restoring configuration** checkbox.

- 4 By default, a restore means restore device and ZMS database. You can select Restore Device Only or Restore ZMS only too.
- 5 Click **Restore**.

The **Confirm Restore** dialog box appears.

- 6 Click **Yes**.

The **Restore Device Configuration** dialog box appears showing the restore progress.



Note: You can also delete backed-up files from the **Restore Device Configuration** dialog box. Select the file to be deleted, click **Delete**, and then click **Yes** in the **Delete Confirm** dialog box.

Related topics:

[Performing immediate configuration backup on a single device on page 75](#)

[Editing a configuration on page 79](#)

Performing immediate synchronization with a single device

When you adding a device, the ZMS configuration synchronization service automatically synchronizes elements in the system. The function of the configuration synchronization service is to ensure that the configuration information on a network device and in the ZMS database are synchronized.

However, in the following situations, you may need to manually perform a full synchronization:

- When you configure and add a device, if the device, the ZMS database, and NetHorizon appear to be out of synchronization.
- When you add a card, if the card indefinitely shows the status **Reserved** in the tree display.
- When ZMS components and device software are upgraded.



Note: Keep in mind that performing a full synchronization can seriously affect ZMS performance. To avoid affecting ZMS services, perform a full synchronization during low-usage periods only.

- 1 Right-click the device and click **Synchronize with Device**.

- 2 At the confirmation prompt, click **OK**.

NetHorizon displays the **Device Synchronization Progress** dialog box.

- 3 To view any errors encountered, click **Show Errors** (**Show Errors** appears dimmed if there are no errors).

Keep in mind that synchronizing may take several minutes. During the process, the device you selected and all its children appear dimmed in the tree display. The device has the status **Synchronizing**. You cannot perform tasks on objects that appear dimmed. You can perform tasks on other objects.

When the device synchronization completes, the dialog box displays the status **Complete**.

- 4 To view any errors encountered, click **Show Errors** (**Show Errors** appears dimmed if there are no errors).

To view a summary of the config sync process, click **Show Summary**.

- 5 Click **Done**.

When the synchronizing is complete, the device and its children are no longer dimmed in the tree display.

Related topics:

[Performing scheduled synchronization with a single device or multiple devices on page 82](#)

Performing scheduled synchronization with a single device or multiple devices

You can perform immediate or scheduled configuration synchronization tasks on a single device or multiple devices in the **Scheduled Device Synchronization** dialog.

- 1 Select **Tools > Scheduled Synchronization with Device** from the menu bar.

The **Scheduled Device Synchronization** dialog appears.

- 2 Click the Browse button to display a list of devices types.

Hold down the CONTROL or SHIFT keys to select multiple devices.

Click **OK**.

- 3 Click **Add to Table** to display all the selected devices and their IP addresses, device types in the table.

- 4 Click the desired config sync option.

Immediate— To perform config sync on the selected device(s) immediately.

Scheduled— For scheduled config sync, also select the time to initiate the sync process.

Disable— To cancel the scheduled config sync tasks.

- 5 Click **Apply** to perform the specified config sync settings.

For scheduled config sync, the time setting will be displayed in the Scheduled Time column. The results of the scheduled config sync process are available from Tools > Task Log Files.

For cancelled config sync tasks. The time setting in the Scheduled Time column will be empty.

Related topics:

[Performing immediate synchronization with a single device on page 81](#)

Configuring device identity

- 1 Right-click a device and select **Modify**. The **Modify Device Configuration** dialog box appears.
- 2 Select **Identity** from the tree menu. The **Device Identification** dialog box appears.
- 3 Specify desired settings.

For information on the settings, see the online help.

Configuring device administration settings

- 1 Right-click a device and select **Modify**. The **Modify Device Configuration** dialog box appears.

- 2 Select **Administration** from the tree menu. The **Device Administration** dialog box appears.
- 3 Specify the desired administration settings.

For information on the settings, see the online help.

Configuring MXK user privilege management

For security reason, users now can manage MXK user accounts from ZMS. Operations of MXK user accounts in ZMS include creating, modifying, listing, getting and deleting user accounts.

To manage MXK user accounts from ZMS, right-click a MXK device on the tree view, and then select **Modify**. In the **Modify Device Configuration** window, select **User Configuration**. In the **User Configuration** window, ZMS users can add , modify, view, delete MXK user accounts.

For each user account, you can set user name, user password, user prompt, user admin, and access levels. You can enable or disable the following access levels:

Admin, Voice, Data, Manf, Data Base, Systems, Tool, Debug.

Configuring MXK users in bulk

Use the “Manage MXK Users” menu item in the “Tools” pull-down menu to configure MXK bulk user.

View the MXK users of selected devices

To view the MXK users of the selected devices:

- 1 Select the “Manage MXK Users” menu item from the “Tool” pull-down menu. The MXK User Configuration window appears.
- 2 In the MXK User Configuration window, click on the Select Devices “...” button to open the Select Device window.
- 3 In the tree view of the Select Device window, you can select any combination of regions, containers, and devices with the Ctrl and Shift keys, and then click OK.
- 4 In the MXK User Configuration window, click the Retrieve Users button, all MXK users defined in the selected devices are listed.
- 5 To sort the MXK users in the list by IP Address, User Name, User Prompt, User Access Level, or User Admin, click the corresponding column header.
- 6 To view the details of each MXK user, select this user, and then click View. The View MXK Users Configuration window appears. Note that only one selected MXK user can be viewed at a time.

Add a MXK user to selected device(s)

A new MXK user can be added to all selected devices in bulk.

To add a MXK user to the selected device(s):

- 1 Make sure the devices displayed in the Select Devices field are your desired devices. If not, use the “...” button to re-select devices.

Click the Add button in the MXK User Configuration window.

This information window appears:

“You will add a common user to all selected devices shown their IP address above.”

- 2 Click OK on the information window. The Add MXK User Configuration window appears.
- 3 Enter the settings for the new MXK user, and click Add. The newly created MXK user will be added to all selected device(s), and displayed in the MXK User Configuration window.

You can click the “Retrieve Users” button to refresh the window.

Modify a MXK user of a selected device

One MXK user can be modified for one device at a time.

To modify the details of a MXK user of a device:

- 1 Select the desired MXK user in the MXK User Configuration window, click the Modify button. The Modify MXK User Configuration window appears.
- 2 Enter the changes for the MXK user, and click Modify. The updated information of this MXK user will be displayed in the MXK User Configuration window.

Change the password for the MXK users have same username on different devices

Multiple MXK users with same User Name can be selected across different devices, and change their password in bulk.

To modify the password for the MXK users in bulk:

- 1 In the MXK User Configuration window, select the MXK user with same user name across different devices with the ctrl or shift key. Click the Modify button. The Change Password window appears.
- 2 Enter the new password twice, and then click OK.

Delete the MXK users from devices

Selected MXK users can be deleted in bulk, or one device at a time. Note that the MXK users with “admin” user name cannot be deleted from a device.

To delete the MXK users from devices:

- 1 In the MXK User Configuration window, select the MXK user with the ctrl or shift key. Click the Delete button. The Delete window appears:
 “Deleting these objects also deletes any objects configured on it. Do you want to continue?”
- 2 Click OK to remove the MXK users from devices.

Configuring shelf inventory manager

Added the **Shelf Inventory Manager** window to manage and display the shelf inventory information for selected devices or regions. To access this window, select **Shelf Inventory Manager** from the **Tools** pull-down menu.

Enabling or disabling secure mode on device

- 1 Right-click a device and select **Modify**. The **Modify Device Configuration** dialog box appears.
- 2 Select **Administration** from the tree menu. The **Device Administration** dialog box appears.
- 3 Specify the desired administration settings.

Choose **Enabled** in the Secured FTP field to indicate what secure features will be used for the following applications:

- config sync -> Secure File Transfer Protocol (SFTP)
- bulk statistics -> SFTP
- dump restore -> SFTP
- software download -> SFTP
- SSH (Secure Shell) to device.
- WebUI -> HTTPS (HTTP secure).

Choose **Disabled** in the Secured FTP field to indicate:

- config sync -> FTP
- bulk statistics -> FTP
- dump restore -> TFTP
- software download -> TFTP
- Telnet to device and SSH to device
- WebUI -> HTTP.

- 4 Click **Modify**.

Configuring port access security

The NetHorizon provides the capability to provide security on the UDP/TCP ports which the device uses for management. Use the **port-access** profile to

define the UDP/TCP port and the IP address or IP address subnet that allows access to that port.

The port access security feature is a white list mechanism. If a host's IP address is not specified in a **port-access** profile, users from that host cannot access on that port.

The ports used for management are:

- telnet, port 23
- SSH, port 22
- HTTP, port 80
- HTTPS, port 443
- SNMP, port 61

If you choose to restrict access to the SNMP port then there must be a rule to allow the device its own SNMP access.

By default, **port-access** profiles do not exist and all ports are open. After a **port-access** profile is configured for a port all other IP addresses or subnets are blocked. This restriction only takes effect after the first **port-access** profile is created. Up to 100 **port-access** profiles can be created on device



Note: Port access security is not independent from setting secure mode for SFTP and SSH in the **Modify Device Configuration** dialog box. If secure is enabled which provides SSH and SFTP while limiting telnet access, but you have provided access with the port-access profile for telnet to a device (or range of devices), the device(s) will not have access.

- 1** To configure the port access control, right-click a device and select **Modify**.

The **Modify Device Configuration** dialog box appears.

- 2** Click **Access Controls** tab.
- 3** To add access control on port, click **Add**. The **Add Access Control Configuration** dialog box appears.
- 4** Specify the desired parameters.

- AccessIndex

The index of the access control profile.

- Port Number

Admin port number of application service.

23: Only the authorized IP subnet will be able to access the device using Telnet.

22: Only the authorized IP subnet will be able to access the device using SSH.

80: Only the authorized IP subnet will be able to access the device Web UI using HTTP.

443: Only the authorized IP subnet will be able to access the device Web UI using HTTPS.

161: for SNMP. Note that if you choose to restrict access to the SNMP port then there must be a rule to allow the device its own SNMP access.

- Source Address

The IP address that device will accept packets from.

- Net Mask

Pass the range that device will accept with regards to the Source Address.

For information on the settings, see the online help.

- 5 Click **Add**.

Configuring device alarm level settings (alarm suppression)

- 1 Right-click a device and select **Modify**. The **Modify Device Configuration** dialog box appears.
- 2 Select **Alarm Levels Enable** from the tree menu. The **Alarm Levels Enable** dialog box appears.
- 3 Click the radio buttons to enable/disable the desired alarm level settings.
If alarm levels are disabled using the CLI or ZMS, alarm records need to be refreshed using the **update device from database** option to synchronize the device and ZMS alarm records.

For information on the settings, see the online help.

Configuring ZMS connectivity settings

- 1 Right-click a device and select **Modify**. The **Modify Device Configuration** dialog box appears.
- 2 Select **ZMS Connectivity** from the tree menu. The **ZMS Connectivity** dialog box appears.
- 3 Specify desired ZMS connectivity settings.

For information on the settings, see the online help.

Configuring device community names

- 1 Right-click a device and select **Modify**. The **Modify Device Configuration** dialog box appears.
- 2 Select **Community Names** from the tree menu. The **Community Names** dialog box appears.

- 3 To add a community name, click the **Add** button. The **Add Community Name** dialog appears.
- 4 Enter the desired name and select the desired access options. Click **Add** to add the specified community name. Otherwise, click **Cancel**.

For information on the settings, see the online help.

Configuring device access lists

- 1 Right-click a device and select **Modify**. The **Modify Device Configuration** dialog box appears.
- 2 Select **Access List** from the tree menu. The **Access List** dialog box appears.
- 3 To add a community name, click the **Add** button. The **Add Access List** dialog appears with name setting.
- 4 Enter the desired name and select the access list entries options.
- 5 The access list entries option appears.

Enter the desired entries. Click **Add** to add the specified access list entries. Otherwise, click **Cancel**.

For information on the settings, see the online help.

Configuring device trap configuration settings

- 1 Right-click a device and select **Modify**. The **Modify Device Configuration** dialog box appears.
- 2 Select **Trap Configuration** from the tree menu. The **Trap Configuration** dialog box appears.
- 3 To add a trap destination, click the **Add** button. The **Add Trap** dialog appears with name setting.
- 4 Enter the desired name and select the trap configuration options.
- 5 The trap configuration option appears.

Enter the desired trap configuration settings. Click **Add** to add the specified trap destination. Otherwise, click **Cancel**.

For information on the settings, see the online help.

RADIUS Configuration

The MALC/MXK supports local and RADIUS (Remote Authentication Dial In User Service) access authentication. The MALC/MXK can be configured for local authentication, RADIUS authentication, RADIUS then local authentication, or RADIUS then craft authentication. RADIUS users are

configured with the Service-Type attribute as Administrative-User or NAS-Prompt-User. RADIUS is used for only login authentication, not severity levels.

When establishing a connection to the NetHorizon with RADIUS authentication, the NetHorizon passes RADIUS information securely to the RADIUS server. The RADIUS server then authenticates the user and either allows or denies access to the NetHorizon. If access is denied and the local authentication option is also configured, the NetHorizon then authenticates access based on the locally configured users and passwords. For logins and failed logins, a console message is generated with user ID and IP address of the device from which the login originated. Failed logins also are logged as alert level messages in the MALC/MXK system log file.

By default, RADIUS access uses the UDP port 1812 for authentication. This parameter can be changed in the radius-client profile.



Note: Follow the RADIUS server guidelines for RADIUS configuration instructions. For example, when using the MALC/MXK with the FreeRadius server:

- Create only one entry in the clients.conf file for each subnet or individual MALC/MXK. For individual MALC/MXKs, the IP in this file must match the IP address of the outbound interface used by the MALC/MXK to connect to the RADIUS server.
- The MALC/MXK uses the value stored in the RADIUS system.sysname file for the NAS-Identifier attribute.
- The shared-secret in the MALC/MXK radius-client profile, must exactly match the shared-secret in the RADIUS client entry.

Configuring user authentication method

The NetHorizon can be configured for local authentication, RADIUS authentication, RADIUS then local authentication, and RADIUS then craft authentication.

To configure user authentication method:

- 1** Right-click a device and select **Modify**. The **Modify Device Configuration** dialog box appears.
- 2** Click the table menu.
- 3** Click the value field of the **User Authentication Method**.
- 4** Select the user authentication method. Click **Modify** to accept the change on the user authentication. Otherwise, click **Close**.



Caution: If the *radius* authentication mode is used, local authentication is disabled so the MALC/MXK may become inaccessible if IP connectivity to the RADIUS server is lost or other changes prevent the MALC/MXK from receiving RADIUS authentication.

Configuring RADIUS client profiles

To configure RADIUS client profiles:

- 1 Right-click a device and select **Modify**. The **Modify Device Configuration** dialog box appears.
- 2 Select **Radius Clients** from the tree menu. The **Radius Clients** dialog box appears.
- 3 To add a RADIUS client profile, click the **Add** button. The **Add Radius Client** dialog appears with Group index number, Client ID number, and RADIUS settings for Server Name, UDP Port, Shared Secret, Retry Count, and Retry Interval. The Index number is used to group RADIUS client profiles so multiple profiles can be assigned to a MALC/MXK. The ID number specifies the order in which RADIUS client profiles are referenced. For example, the Index 1/ ID 1 specifies that this profile is the first profile in group 1.
 - Group Index

The Index number is used to group RADIUS client profiles so multiple profiles can be assigned to a MALC/MXK. The Group Index number is in the range of 1- 2137483647.
 - Client Id

The ID number specifies the order in which RADIUS client profiles are referenced. The Client Id number is in the range of 1- 2137483647.
 - Server Name/IP Address

The RADIUS server host name or IP address.
 - UDP Port

The destination UDP port number for RADIUS authentication packets when authenticating using this server. By default, RADIUS access uses the UDP port 1812 for authentication. UDP port number is in the range of 1-65535.
 - Shared Secret

This is the shared secret used by the RADIUS client and server for authentication and packet encryption.
 - Retry Count

The number of times to retry a failed request before to request the next configured RADIUS server. By default, the retry count value is 5. The retry counts is in the range of 1-255.

– Retry Interval

The minimum time (in seconds) the device will wait the RADIUS authentication before assuming an error occurred and the request is retired. By default, the retry interval is 1 second. The retry interval is in the range of 1-60.

- 4 Enter the desired Index number, ID number, and RADIUS settings.
- 5 Click **Add** and **Close**, the newly created RADIUS client profile appears in the **Radius Clients** dialog box.
- 6 To modify an existing RADIUS client profile, in the **Radius Clients** dialog, select the desired RADIUS client and click **Modify**. The **Modify Radius Client** dialog appears.
- 7 Enter the new RADIUS settings for the RADIUS client profile.
- 8 Click **Modify** and **Close**, the RADIUS client profile with new settings appears in the **RADIUS Clients** dialog box.
- 9 To delete a RADIUS client profile. Select the desired RADIUS client in the RADIUS Clients dialog box, click **Delete**. The **Confirmation** dialog box appears.
- 10 In the Confirmation dialog box, click **OK** to delete this RADIUS client profile, otherwise click **Cancel**.
- 11 To view the detail information of a RADIUS client profile. Select the desired RADIUS client in the **RADIUS Clients** dialog box, click **View**. The **View Radius Clients** dialog box appears.

For information on the settings, see the online help.

Configuring RADIUS index

The NetHorizon can be configured for local authentication, RADIUS authentication, RADIUS then local authentication, and RADIUS then craft authentication. Multiple radius-client profiles can be defined using the index and subindex numbers. This index scheme can be used to create index numbers for groups of RADIUS servers. When an index number is specified in the system profile, the MALC/MXK attempts authentication from each RADIUS server in that group in sequential order of the subindex numbers.

To configure RADIUS support:



Note: Before beginning this procedure, ensure that the MALC/MXK has IP connectivity to the RADIUS server.

- 1 Update the RADIUS server with settings for the Zhone prompts.

- 2 Follow the steps in the [Configuring RADIUS client profiles on page 90](#) to create a RADIUS client profile on the NetHorizon with the desired index number, Id number, and RADIUS settings for server name, shared secret, number of retries, and other parameters. The index number is used to group RADIUS client profiles so multiple profiles can be assigned to a NetHorizon. The ID number specifies the order in which RADIUS client profiles are referenced. This example specifies the RADIUS client 1/1 with server name 172.24.36.248 and a shared-secret of *secret*. The Index 1/Id 1 specifies that this profile is the first profile in group 1.
- 3 In the system profile on the NetHorizon, follow the steps in the [Configuring user authentication method on page 89](#) to set the desired user authentication method. This example sets the User Authentication Method of **Radius Then Local**.
- 4 In the system profile on the NetHorizon specify the index of the RADIUS profile to use. This example specifies the **Radius Authentication Index** of 1. This index is configured with RADIUS client profile 1/1. The MALC/MXK first attempts authentication using the server specified in RADIUS client 1/1. If this authentication fails, the MALC/MXK attempts authentication based on the local system profile.
To set the RADIUS Authentication Index, right-click a device and select **Modify**. The **Modify Device Configuration** dialog box appears.
- 5 Select **Administration** from the tree menu. The **Administration** dialog box appears.
- 6 Click the **Radius Authentication Index** Browse button. Select the value of 1. Click **OK**.
- 7 In the Administration dialog box, click the **Modify**.

Configuring device location settings

- 1 Right-click a device and select **Modify**. The **Modify Device Configuration** dialog box appears.
- 2 Select **Location** from the tree menu. The **Location** dialog box appears.
- 3 Specify the desired location settings.
For information on the settings, see the online help.
- 4 Click **Modify**.

Configuring voice DSP settings

- 1 Right-click a device and select **Modify**. The **Modify Device Configuration** dialog box appears.
- 2 Select **Voice DSP Config** from the tree menu. The **Voice DSP Config** dialog box appears.
- 3 Specify voice DSP settings.

For information on the settings, see the online help.

- 4 Click **Modify**.

Configuring DSCP to COS (802.1p)



Note: DSCP to COS (802.1p) mapping applies to all MXK cards.

Some network architectures require QoS prioritization at layer 2 and others at layer 3. In order to maintain QoS between Layer 2 Ethernet and Layer 3 IP protocols, the NetHorizon now supports mapping Differentiated Services Code Points (DSCP) to Classes of Services (CoS) as defined by IEEE 802.1p.

CoS is Layer 2 QoS marking mechanism and involves manipulating the layer 2 Ethernet 802.1p tag. CoS uses 3 bits and therefore values can be anything from 0 to 7. DSCP involves manipulating the IP header info (specifically the ToS field). DSCP uses 6 bits and value range from 0 to 63. DSCP and ToS are different use of the same bits. Therefore, the following standard mapping table can be used as a reference when provisioning DSCP to COS (802.1p).

Table 4: Default DSCP to CoS (802.1p) mapping

DSCP	0–7	8–15	16–23	24–31	32–39	40–47	48–55	56–63
CoS	0	1	2	3	4	5	6	7

Viewing or Modifying DSCP to CoS mapping

To view or modify the values in the DSCP to CoS mapping (802.1p):

- 1 Right-click an MXK and select **Modify**. The **Modify Device Configuration** dialog box appears.
- 2 Select **DscpToCos** from the tree menu. The **Dscp Index** appears in the **DscpToCos** dialog box.
- 3 Click **View** to view the default mappings.
- 4 If you want to change the settings, click **Modify**. The **Modify DscpToCos** dialog appears.
- 5 You can keep the default mappings, or change it as desired.
- 6 Click **Modify** to save the changes.

Assigning DSCP to COS mapping to MXK

To assign the DSCP to COS mapping (ingress packet rule) to MXK when creating a bridge:

- 1 Create a DSCP to COS mapping packet rule
 - a Right-click an MXK, and select **Modifying Bridge**.

The **Manage Bridge Logicals** dialog appears.

- b** In the **Manage Bridge Logicals** dialog, click **Bridge Filtering** tab.
- c** In the **Packet Rule Group** pane, click **Add**.
- d** In the **Add Packet Rule Group Configuration** window, select DscpToCos as type, use the Dscp Index browser button to select Dscp Index 1.
- e** Click **Add**.

A packet rule group with a DscpToCos packet rule member is created.

- 2** In the **Manage Bridge Logicals** dialog, click **Bridge Logical** tab.

- 3** In the **Bridge Logical** pane, click **Add**.

The **Bridge Logical on Device** window appears.

- 4** In the **Bridge Logical on Device** window:
 - a** Expand port levels and select an UNI port under an uplink card,
 - b** Select the bridge type, assign the VLAN ID, and specify other necessary fields for creating a bridge.
 - c** To assign the DSCP to COS mapping packet rule, select the **Use Existing Packet Rules** field, and then click the browser button of the **Ingress Packet Rule Group Index**. In the **Packet Rule Group browser** window select the packet rule group that contains the DscpToCos packet rule member, then click **OK**.
- 5** Click **Add**.

A bridge with the DSCP to COS packet mapping is added in MXK.

Assigning DSCP to COS mapping to an Unified Service Provisioning CPE

You can assign DSCP to CoS mapping to Unified Service Provisioning CPE when creating MXK bridge and CPE connections.

A **DSCP 2 Cos Index** field is added into the **CPE Connection On Device** dialog box for this feature.

- 1** Right-click an MXK, and select **Manage USP Service**.
- 2** In the **Manage CPE Services** window, click **CPE Connection** tab.
- 3** Click **Add**.
- 4** In the **CPE Connection On Device** window:
 - a** Expand the tree and then select an ONU port in the **Select Port** pane,
 - b** Specify a GEM port ID, a GTP index, a bridge template, a VLAN ID, and specify the other necessary fields for creating an MXK bridge and its CPE connection.

- c To assign the DSCP to COS mapping, click the browser button of the **DSCP 2 Cos Index**. In the **DSCP To Cos Index browser** window select a set of DSCP to CoS mapping, then click **OK**.
- 5 Click **Add**.
The DSCP to COS mapping is assigned to the CPE.

Configuring device video source settings

- 1 Right-click a device and select **Modify**. The **Modify Device Configuration** dialog box appears.
- 2 Select **Video Source Config** from the tree menu. The **Video Source Config** dialog box appears.
- 3 To add a video source, click the **Add** button. The Add ATM VLC to Multicast Map dialog appears.
- 4 Enter or select the desired IP interface. Multiple IP interfaces may be selected per device.
For information on the settings, see the online help.
- 5 Click **Modify**.

Configuring device system clock settings

- 1 Right-click a device and select **Modify**. The **Modify Device Configuration** dialog box appears.
- 2 Select **System Clock Source** from the tree menu. The **System Clock Source** dialog box appears.
- 3 Specify the desired system clock settings.
For information on the settings, see the online help.
- 4 Click **Modify**.

Configuring device NTP configuration settings

- 1 Right-click a device and select **Modify**. The **Modify Device Configuration** dialog box appears.
- 2 Select **NTP Config** from the tree menu. The **NTP Config** dialog box appears.
- 3 Specify the desired NTP settings.
For information on the settings, see the online help.
- 4 Click **Modify**.

Configuring device bulk statistics configuration settings

- 1 Right-click a device and select **Modify**. The **Modify Device Configuration** dialog box appears.

- 2 Select **Bulk Stats Config** from the tree menu. The **Bulk Stats Config** dialog box appears.
- 3 Specify the desired bulk statistic settings.
For information on the settings, see the online help.
- 4 Click **Modify**.

Configuring device global STP parameters

To view or modify the global STP parameters, perform the following task:

- 1 To view the global STP parameters, right-click a device and select **View**.
The **View Device Configuration** dialog box appears.
- 2 Click **STP Params Configuration** tab to view the STP parameters.
- 3 To modify the global STP parameters, right-click a device and select **Modify**.
The **Modify Device Configuration** dialog box appears.
- 4 Select **STP Params Configuration** from the tree menu. The **STP Params Configuration** dialog box appears.
- 5 Specify the desired global STP parameters.
 - Name
Set this field if STP or RSTP is running. Use the name of the bridge as a key.
 - Revision
Set this field if STP or RSTP is running. By default is 0.
 - Bridge Priority
The priority ID that is to be advertised for this bridge. By default this value is 36000. The value is in the range of 0 to 65535.
 - Force Version
This parameter indicates the protocol to initiate with.
2 is RSTP, 0 is STP. By default is 2.
 - Forward Delay
The delay used by STP bridges to transition root and designated ports to Forwarding state (a normal operational state), in the unit of seconds. By default this value is 15. The value is in the range of 4 to 30.
 - Hello Time
The interval between periodic transmissions of configuration messages by designated ports, in the unit of seconds. By default this value is 2. The value is in the range of 1 to 2.
 - Migrate Time

The initial value of the mdelayWhile and edgeDelayWhile timers, in the unit of seconds. By default, this value is 3.

The mdelayWhile (migration delay timer) is used by the port protocol migration state machine to allow time for another RSTP Bridge on the same LAN to synchronize its migration state with this Port before the receipt of a BPDU can cause this Port to change the BPDU types it transmits.

The edgeDelayWhile (edge delay timer) is remaining in the absence of a received BPDU, before this port is identified as an operational Edge Port.

- Hold Count

The transmit hold count that is used by the port transmit state machine to limit transmission rate. By default, this value is 3. The value is in the range of 1 to 10.

- Max Age

The maximum age of the information transmitted by the bridge when it is the root bridge, in the unit of seconds. By default, this value is 20. The value is in the range of 6 to 40.

For information on the settings, see the online help.

6 Click **Modify**.

Configuring GigaMux 1600/3200 device settings

1 Right-click a GigaMux 1600/3200 series device and select **Modify**. The **Modify Device Configuration** dialog box appears.

2 Select **System Info** from the tree menu. The **Modify Device Configuration** dialog box appears with system information.

3 Specify the desired system info settings.

For information on the settings, see the online help.

4 Click **System Configuration** from the tree menu. The **System Configuration** settings appears.

5 Specify the desired system configuration settings.

For information on the settings, see the online help.

6 Click **Ethernet** from the tree menu. The **Ethernet** setting appears.

7 Specify the desired Ethernet settings.

For information on the settings, see the online help.

8 Click **Telnet** from the tree menu. The **Telnet** setting appears.

9 Specify the desired Telnet settings.

For information on the settings, see the online help.

10 Click **SNMP** from the tree menu. The **SNMP** setting appears.

- 11 Specify the desired SNMP settings.

For information on the settings, see the online help.

- 12 Click **IMN Routing Parameters** from the tree menu. The **IMN Routing Parameters** setting appears.

- 13 Specify the desired IMN Routing Parameter settings.

For information on the settings, see the online help.

- 14 Click **IMN Static Routing Table** from the tree menu. The **IMN Static Routing Table** setting appears.

- 15 Specify the desired IMN Static Routing Table settings.

Click Add to add a static IP address to the routing table. The Add INM Static Route dialog appears. ‘

For information on the settings, see the online help.

- 16 Click **External Alarm Input Table** from the tree menu. The **External Alarm Input Table** setting appears.

- 17 Specify the desired External Alarm Input Table settings.

For information on the settings, see the online help.

Configuring CPE device settings

Topics:

[Adding CPE](#)

[Initializing a CPE](#)

[Downloading file to a CPE](#)

[Downloading software to a CPE](#)

[Activating software on a CPE](#)

[Upgrading software on a CPE](#)

[Executing configure script on a CPE](#)

[Backing up database on a CPE](#)

[Restoring database on a CPE](#)

[Synchronizing alarms on a CPE](#)

[Telnetting a CPE](#)

[Launching CPE WebUI on a CPE](#)

[Launching secured CPE WebUI on a CPE](#)

[CPE Manager Enhancements - Bulk Operations](#)

[Automatic Web Cut-through to ZMS](#)

Adding CPE

CPE Manager

The SLMS CPE Manager provides a means for managing customer premises equipment (CPE) devices without requiring provisioning of routable IP addresses to reach these CPE end-points. While the CPE Manager is specifically designed for Zhone's EtherXtend family of CPE products, CPE Manager can be used with any CPE device which supports IP addresses on a VLAN.

In many service provider networks, the increasing usage of IP-aware CPE devices creates an operational challenge for service providers because the number of devices which require IP addresses cause IP address space depletion, making it hard to assign routable addresses for these devices.

A solution to this problem is the SLMS CPE Manager. CPE Manager adds proxy capability to SLMS, allowing one IP interface on the Zhone central office device to provide IP access to all the subtended CPE devices connected to it. This one IP interface is created on an upstream port which is routable on the service providers management network, and it provides IP address and protocol port translation when forwarding packets to and from managed CPE devices. In this way, IP can be used for CPE management without having to consume IP address space or having to add network routes for reachability of line side CPE devices.



Note: Whenever a CPE is added into ZMS, it automatically adds ZMS as the trap destination.

CPE Manager support for Active Ethernet/ GPON CPEs

The MxK supports CPE manager on the ONT types:

- zNID GE 22xx/42xx/9xxx. (i.e. Active Ethernet ONTs)
- zNID GPON 22xx/42xx/9xxx (i.e. GPON ONTs)

These ONTs can be connected to the MxK Active Ethernet line card's ethernet port or GPON OLT line card's GPON OLT port.

These CPEs are added the same way as the Ethx-30xx CPEs. Note, that for these CPEs the **Execute Config Script** option is not available.

There are two fields only for GPON CPE manager:

- Gpon (GEM) portID: The ID of the GEM port to use for the CPE manager connection. The zNID GPON 22xx/42xx/9xxx devices only support GEM 5xx, so this field is read-only.
- GPON Traffic Profile index: The GPON traffic profile to use for the GPON for the CPE manager connection.

Adding CPE by CPE manager

To add a CPE by CPE manager, perform some steps with CLI first, and then configure the **Add CPE Device** dialog box:

- 1 Add a public address for the CPE manager with CLI.

Note that adding the public address for the MALC/MXK requires the MALC/MXK has already been given an IP address.

For example:

```
cpe-mgr add public 192.168.254.1
```

- 2 Configure the local network with CLI. The local network IP address must be a class A address. For example:

```
cpe-mgr add local network 12.0.0.1
```

- 3 Synchronize the MALC/MXK with ZMS by right-clicking the MALC/MXK device in the tree view and selecting **Synchronize with Device**.
- 4 By adding the public address, the NAT status is enabled in the MALC/MXK.
- 5 From the tree view, expand the G.SHDSL, T1E1, ActiveE, or GPON card, and then expand the Bond Groups, Ethernet (GigE) port or ONU.
- 6 Right-click a bond group, Ethernet port or ONU, and select **CPE Management> Configure CPE**.

The **Add CPE device** dialog box appears.

- In the **Add CPE Device** dialog box:
 - Check the **Use CPE Manager to communicate with CPE** box.
 - Configure the community string for the CPE device.
 - Click **Add**.
- 7 After adding a CPE device by CPE manager, the public IP address and the port mapped to the CPE appear in the tree view.
 - 8 And it creates the Port Address Translation (PAT) bindings for this CPE device automatically.

To verify or troubleshoot CPE manager in the PAT binding profiles, right-click a MALC/MXK and select **Modify**, and from the **Modify Device** dialog box click **PAT Bindings**. The **PAT Bindings** dialog box appears

Adding CPE with a static IP address

- 1 From the tree view, expand the G.SHDSL, T1E1, ActiveE, or GPON card, and then expand the Bond Groups, Ethernet (GigE) port or ONU.
- 2 Right-click a bond group, Ethernet (GigE) port or ONU, and select **CPE Management> Add CPE**.

The **Add CPE device** dialog box appears.

- In the **Add CPE Device** dialog box:
- Uncheck the **Use CPE Manager to communicate with CPE** box.
- Configure the IP address for the CPE device.
- Configure the community string for the CPE device.
- Click **Add**.

3 The CPE IP address appears next to the physical's name in the tree view.

Initializing a CPE

Initializing a CPE

Initialize the CPE when ZMS was not able to communicate with the CPE when the CPE was added.

- 1** From the tree view, expand the G.SHDSL or T1E1 card, and then expand the Bond Groups.
- 2** Right-click a bond group and select **CPE Management> Initialize CPE**.
- 3** Once the CPE is initialized, the **Initialize CPE** option will be removed from the menu.

Downloading file to a CPE

The Download file to CPE feature is used to download all files to a CPE, except for software loads.

The Download file to CPE feature is supported on EtherXtend 30xx/31xx and SkyZhone that added with/ without CPE manager, and EtherXtend 33xx/34xx that added with a static IP address.

The Download file to CPE from MALC feature is supported on EtherXtend 33xx/34xx that added with CPE manager.



Note: The Download File to CPE feature is not supported on the Verso 8000.

Downloading file to EtherXtend 30xx/31xx and SkyZhone

To allow ZMS send an SNMP command to the EtherXtend that instructs it to download a file, perform the following tasks:

- 1** Right-click a bond group and select **CPE Management> Download File to CPE**.
- 2** The **Download File To CPE** dialog box appears.

The **Download File To CPE** dialog will work if the CPE has an IP address or if it is being managed by CPE manager.

- Configure the **Download File To CPE** dialog box.

- Configure the IP address and Path of the File Server where the source file located.
- Configure the CPE File Path where the file should be download to.
- Configure the FTP User Name and FTP Password. EtherXtend 30xx/31xx and SkyZhone use FTP to download files.
- Click **Download**.

Downloading file to EtherXtend 33xx/34xx that with an IP address

- 1 Right-click a bond group and select **CPE Management> Download File to CPE**.
- 2 The **Download File To CPE** dialog box appears.
- 3 To download file to EtherXtend 33xx/34xx that with an IP address, configure the **Download File To CPE** dialog box.
 - These CPEs devices use TFTP to download files, so no FTP username and password are required. And since TFTP does not work with the CPE manager (NAT/PAT), the **Download File To CPE** dialog box only work with CPE with an IP address.
 - Configure the IP address and Path of the File Server where the source file located.
 - Configure the CPE File Path where the file should be download to.
 - Click **Download**.

Downloading file to EtherXtend 33xx/34xx that are managed by CPE manager

To download file to EtherXtend 33xx/34xx that are managed by CPE manager, you should download file to MALC first, and then download the file from MALC to CPE.

- 1 To download the file to the MALC, right-click the MALC and select **Download Software Image**.

The **Download Software Image** dialog box appears.
- 2 In the **Download Software Image** dialog box,
 - Specify the IP address of the Primary Load Server.
 - Select or type the filename ethX3300.bin as the TFTP server file name.
 - Specify directory “pub” in the Device Sub-Directory. The file must be downloaded into the “pub” directory on the MALC.
 - And then specify the other desired settings,
 - Click **Download**.

After the file is downloaded to the MALC, the **Download File from Malc** option will be available in the **CPE Management** menu.

- 3 To download the file from MALC to CPE, right-click a bond group and select **CPE Management> Download File From Malc**.
- 4 In the **Download File From Malc** dialog box,
 - Configure the MALC File Path where the source file located.
 - Configure the CPE File Path where the file should be download to.
 - Click **Download**.

Downloading software to a CPE

The Download software to CPE feature is used to download a software load to a CPE.

Downloading software to EtherXtend 30xx/31xx and SkyZhone

To allow ZMS send an SNMP command to the EtherXtend that instructs it to download a software load, perform the following tasks:

- 1 Right-click a bond group and select **CPE Management> Download Software to CPE**.

- 2 The **Download Software To CPE** dialog box appears.

The **Download Software To CPE** dialog will work if the CPE has an IP address or if it is being managed by CPE manager.

- Configure the **Download Software To CPE** dialog box.
- Configure the IP address and Path of the File Server where the source software load located.
- Configure the CPE File Path where the software load should be download to.
- Configure the FTP User Name and FTP Password. EtherXtend 30xx/31xx and SkyZhone use FTP to download software load.
- Click **Download**.

Downloading software to EtherXtend 33xx/34xx that with an IP address

- 1 Right-click a bond group and select **CPE Management> Download Software to CPE**.
- 2 The **Download Software To CPE** dialog box appears.
- 3 To download file to EtherXtend 33xx/34xx that with an IP address, configure the **Download Software To CPE** dialog box.

- These CPEs devices use TFTP to download files, so no FTP username and password are required. And since TFTP does not work with the CPE manager (NAT/PAT), the **Download Software To CPE** dialog box only work with CPE with an IP address.
- Configure the IP address and Path of the File Server where the source software load located.
- Configure the CPE File Path where the software load should be download to.
- Click **Download**.

Downloading software to EtherXtend 33xx/34xx that are managed by CPE manager

To download software load to EtherXtend 33xx/34xx that are managed by CPE manager, you should download software to MALC first, and then download the software from MALC to CPE.

- 1** To download the software to the MALC, right-click the MALC and select **Download Software Image**.

The **Download Software Image** dialog box appears.

- 2** In the **Download Software Image** dialog box,
 - Specify the IP address of the Primary Load Server.
 - Select or type the filename ethX3300.bin as the TFTP server file name.
 - Specify directory “pub” in the Device Sub-Directory. The file must be downloaded into the “pub” directory on the MALC.
 - And then specify the other desired settings,
 - Click **Download**.

After the file is downloaded to the MALC, the **Download File from Malc** option will be available in the **CPE Management** menu.

- 3** To download the file from MALC to CPE, right-click a bond group and select **CPE Management> Download Software From Malc**.
- 4** In the **Download Software From Malc** dialog box,
 - Configure the MALC File Path where the source software load located.
 - Configure the CPE File Path where the software load should be download to.
 - Click **Download**.

Activating software on a CPE

The Activate Software feature is used to activate a new software load on a CPE.

Activating software on a CPE

To start running a software load on a CPE after downloading the file to this CPE, perform the following tasks:



Note: The Active Software feature is not supported on the Verso 8000.

- 1 Right-click on the bond group, select **CPE Management**, and then select **Activate Software**.
- 2 The confirm window appears.
- 3 Click **Yes**.

Upgrading software on a CPE

The Upgrade software feature is used to download and activate a software on a CPE.

The Upgrade software feature is supported on EtherXtend 30xx/31xx and SkyZhone that added with/ without CPE manager, and EtherXtend 33xx/34xx that added with a static IP address.

Upgrading software on a CPE

To upgrade software on a CPE, perform the following tasks:

- 1 Right-click on the bond group, select **CPE Management**, and then select **Upgrade Software**.
- 2 The **Download and Activate Software** dialog box appears.
- 3 In the **Download and Activate Software** dialog box,
 - Configure the File Server IP where the source software load located.
 - Configure the File Server Path where the software load should be download to.
 - Configure the FTP User Name and FTP Password if the CPE is EtherXtend 30xx/31xx and SkyZhone.
 - Click **Download**.
- 4 Click **Upgrade**.

Executing configure script on a CPE

The Execute config script feature is used to execute a set of commands located in a configuration script. The configuration script has be exist on the

CPE. If necessary, use **Download File to CPE** to download the script to the CPE prior to executing script.

The Execute config script feature is supported on EtherXtend 30xx/31xx and SkyZhong that added with/ without CPE manager.

Executing configure script on a CPE

To execute config script on a CPE, perform the following tasks:

- 1 Right-click on the bond group, select **CPE Management**, and then select **Execute Config Script**.
- 2 The **Execute Config Script** window appears.
- 3 Enter the file path of the CPE Management script, and click **Execute**.

Backing up database on a CPE

The Backup database feature creates a backup of the CPE's configuration and stores it at the indicated location. The config sync FTP username and password are used to download the file. The file is stored in the same directory as config sync files are stored.

Backing up database on a CPE

To backup database on a CPE, perform the following tasks:

- 1 Right-click on the bond group, select **CPE Management**, and then select **Database Backup**.

The **Backup CPEs Database** window appears.

Specify a file name for the backup file. This is the default file names:

EtherXtend30xx/31xx filename=
modelType_SerialNumber_date_time.tar.gz

EtherXtend33xx/34xx filename= modelType_IPAddress_data_time.bkp

- 2 Click **Backup**.

Restoring database on a CPE

The Restore database feature restores CPE's configuration from a database backup file that saved on the ZMS server.

Restoring database on a CPE

To restore database on a CPE, perform the following tasks:

- 1 Right-click on the bond group, select **CPE Management**, and then select **Database Restore**.
- 2 The **Restore CPEs Database** window appears. It shows the backup files from the CPE backup directory on the ZMS server.

- 3 Select a backup file, and click **Restore**.

Synchronizing alarms on a CPE

The Synchronizing CPE alarms feature is used to synchronize alarms between CPE device and ZMS server.

The Synchronizing CPE alarms feature is supported on EtherXtend 33xx/34xx that added with/ without CPE manager.

To synchronize alarms on a CPE, right-click on the bond group, select **CPE Management**> **Synchronize CPE alarms**.

Telnetting a CPE

To telnet to the remote EtherXtend, right-click a bond group and select **CPE Management**> **Telnet to CPE**.

Launching CPE WebUI on a CPE

The Launching CPE WebUI feature is supported on EtherXtend 30xx/31xx that added with/ without CPE manager and SkyZhone.

To launch the Web User Interface of the remote EtherXtend, right-click a bond group and select **CPE Management**> **Launch CPE Web UI**.

Launching secured CPE WebUI on a CPE

The Launching secured CPE WebUI feature is same as the Launching CPE WebUI feature except that it uses https.

The Launching secured CPE WebUI feature is supported on EtherXtend 30xx/31xx that added with/ without CPE manager and SkyZhone.

To launch the secured WUI of the remote EtherXtend, right-click a bond group and select **CPE Management**> **Launch Secured CPE Web UI**.

CPE Manager Enhancements - Bulk Operations

Bulk operations for CPE management are supported on device and card levels. The device node must have a card that supports bond groups. Same as the card node, it must support bond group. The bulk CPE management works the same as the CPE management for a single CPE. It calls the appropriate actions for all CPEs under the selected card or device.

The following sections describe the supported bulk CPE management features:

- [Downloading file to CPEs](#)
- [Downloading software to CPEs](#)
- [Activating software on CPEs](#)

- [Upgrading software on CPEs](#)
- [Executing script on CPEs](#)
- [Backing up CPE databases on CPEs](#)

Downloading file to CPEs

The Download file to CPEs feature is used to download all files except for software loads to all CPEs under the same card or device.

- 1 Right-click on a device that contains a card which supports a bond group or on a card which supports a bond group, and select **CPE Management> Download File to CPEs**.
- 2 The **Download File To All CPEs** dialog box appears.
 - Configure the **Download File To All CPEs** dialog box.
 - Configure the IP address and Path of the File Server where the source file located.
 - Configure the CPE File Path where the file should be download to.
 - Configure the FTP User Name and FTP Password for EtherXtend 30xx/31xx and SkyZhone.
 - Click **Download**.

Downloading software to CPEs

- 1 Right-click on a device that contains a card which supports a bond group or on a card which supports a bond group, and select **CPE Management> Download Software to CPEs**.
- 2 The **Download Software To All CPEs** dialog box appears.

The **Download Software To All CPEs** dialog will work if the CPE has an IP address or if it is being managed by CPE manager.

 - Configure the **Download Software To All CPEs** dialog box.
 - Configure the IP address and Path of the File Server where the source software load located.
 - Configure the CPE File Path where the software load should be download to.
 - Configure the FTP User Name and FTP Password for EtherXtend 30xx/31xx and SkyZhone.
 - Click **Download**.

Activating software on CPEs

The Activate Software on CPEs feature is used to activate a new software load on all CPEs under the same card or device.

- 1 Right-click on a device that contains a card which supports a bond group or on a card which supports a bond group, and select **CPE Management > Activate Software on CPEs**.
- 2 The **Activate Software On All CPEs** window appears.
- 3 Click **Activate**.

Upgrading software on CPEs

The Upgrade software on CPEs feature is used to download and activate software on all CPEs under the same card or device.

The Upgrade software feature is supported on EtherXtend 30xx/31xx and SkyZhone that added with/ without CPE manager, and EtherXtend 33xx/34xx added with a static IP address.

- 1 Right-click on a device that contains a card which supports a bond group or on a card which supports a bond group, and select **CPE Management > Upgrade Software on CPEs**.
- 2 The **Upgrade All CPEs** dialog box appears.
- 3 In the **Upgrade All CPEs** dialog box,
 - Configure the File Server IP where the source software load located.
 - Configure the File Server Path where the software load should be download to.
 - Configure the FTP User Name and FTP Password for EtherXtend 30xx/31xx and SkyZhone.
 - Click **Download**.
- 4 Click **Upgrade**.

Executing script on CPEs

The Execute config script on CPEs feature is used to execute a set of commands located in a configuration script. The configuration script has to be exist on the CPE. If necessary, use **Download File to CPE** to download the script to the CPE prior to executing script.

The Execute config script feature is supported on EtherXtend 30xx/31xx and SkyZhone added with/ without CPE manager.

- 1 Right-click on a device that contains a card which supports a bond group or on a card which supports a bond group, and select **CPE Management > Execute Script on CPEs**.
- 2 The **Execute Configuration Script On All CPEs** window appears.
- 3 Enter the file path of the CPE Management script, and click **Execute**.

Backing up CPE databases on CPEs

The Backup CPE Databases feature creates a backup of the CPE's configuration and stores it at the indicated location. The config sync FTP username and password are used to download the file. The file is stored in the same directory as config sync files are stored.

- 1 Right-click on a device that contains a card which supports a bond group or on a card which supports a bond group, and select **CPE Management > Backup CPE Databases**.
- 2 The **Backup Databases of All CPEs** window appears.
- 3 Click **Backup**.

Automatic Web Cut-through to ZMS

"Automatic Web Cut-through to CPE" feature was added to ZMS NH Client. When "Launch CPE Web UI" is selected by NH Client user, ZMS will auto-configure the MXK-side CPE-MGR Public and CPE-MGR Local interfaces, along with the CPE-MGR NAT interfaces. ZMS will then launch a web page with the URL of the selected CPE, allowing the NH Client user to log into the CPE's Web Interface. Unless the user had previously added the CPE via the "Add CPE Device" screen, "Launch CPE Web UI" will result in the session to be active for 24 hours, at which time the CPE-MGR NAT interface will be deleted. User will then have to select "Launch CPE Web UI" again to initiate a new CPE Web session. If the user had previously added the CPE via "Add CPE Device" screen, the CPE-MGR NAT interface will be active until user specifically deletes it.

Configuring EZ Touch Provisioning™ CPEs

Topics:

[EZ Touch Provisioning™ Overview](#)

[Adding EZ Touch CPE by CPE Manager](#)

[Adding download servers for CPE Configuration Manager](#)

[Creating CPE Configuration Manager](#)

[Adding CPE Configuration Manager Member to CPE Configuration Manager Group](#)

Viewing CPE Configuration Manager Member runtime details

EZ Touch Provisioning™ Overview

The EZ Touch Provisioning™ feature provides the ability to automatically discover GPON ONTs (zNIDs) or ActiveEthernet zNIDs by MXK, then download the customer-specified software version and configuration file to the zNIDs. This feature can be used to automatically upgrade newly installed zNIDs with the required software and a default configuration file. It can also be used to automatically configure a replacement zNID with the software and specific configuration file of the original zNID. The specific configuration file would include the subscriber service settings.

Note that the following sections use the term of CPE to cover the both zNID and ONT concepts.

CPE Manager, Compression Mode, Security Mode

CPE Manager is used to access the CPEs with EZ Touch Provisioning capability by MXK, all the provisioning functions are maintained in the CPE Configuration Manager.



Note: Some CPE Manager actions should not be performed on the CPE Configuration Manager provisioned CPEs, such as Upgrade Software, Download File to CPE, Download Software to CPE, Activate Software, Database Backup, Database Restore.

ZMS pick the CPE's base public port automatically to access a CPE that are added by CPE manager. The following CPE got the base port 51921.

When you adding a CPE, you have the options to select the number of ports used for protocol desired.

To select the ports to make available, the **Add CPE device** dialog box has several options depending on the selection of the **Port Mapping Compression Mode** and **Communications Type**:

- **full compression, partial compression, or no compression**

Selection of the **Port Mapping Compression Mode** mode defines how many ports may be accessed using the NAT-PAT binding, the more ports are accessed per device, the fewer devices that will be able to be accessed. The defaults for compact mode is full mode (the three port mapping). With the full mode, the MXK can translate 3 ports per CPE device. Each MXK can support up to 1400 CPE devices.

With partial mode, the MXK can translate 4 ports per CPE device. Each MXK can support up to 1000 CPE devices.

With none compression mode, the MXK can translate 9 ports per CPE device. Each MXK can support up to 480 CPE devices. Security mode is not applicable in this case.

- **normal or secure**

Selection of the **Communications Type** defines whether those ports will use security mode, for example HTTP or HTTPS, telnet or SSH. For security mode, the default is normal, which means the security mode is disabled.

For the detail information about the CPE manager, refer to the *MXK Configuration Guide*.

CPE Configuration Manager, CPE Configuration Manager Group, CPE Configuration Manager Member

CPE Configuration Manager is configured on the CO device side. Its the place for customer to define the required software image version and file name, configuration file name, download server IP address, etc., for a specific CPE type.

EZ Touch Provisioning has a mechanism for automatically maintaining multiple CPE types by grouping CPE Configuration Managers. Multiple CPE Configuration Managers may in the same group, but only one CPE Configuration Manager can exist for each unique CPE type. This association allows the defining of multiple CPE type configurations for a given interface.

Each interface will be assigned to a CPE Configuration Manager Group. This interface is considered as a CPE Configuration Manager Member. The interface here could be GEM port (e.g. 1-4-1-502/gponport) for GPON ONT or Ethernet port (e.g. 1-6-1-0/eth) for ActiveE zNID. The CPEs attached to the interface must be one of the types supported by this group. Multiple interfaces may use the same CPE Configuration Manager Group.

After adding CPE Configuration Manager Member to the CPE Configuration Manager Group:

- The CPE Configuration Manager with the same CPE type as the attached CPE will check the pre-defined configuration file or software version. If mismatched, CPE Configuration Manager will download the files from the download server to the CPE.
- If later on, this CPE is replaced with a different type at that interface, another CPE Configuration Manager in the group will take over, and check the requirements. If mismatched, CPE Configuration Manager will upgrade the replacement CPE as well.



Note: If the customer wants the replacement CPE device to automatically receive the software load and configuration of the previous CPE, it must be of the same type as the original.

How to group CPE Configuration Managers can be varied by user's requirements. Below are two example use cases:

- Use Case No.1:

- Group No.1 contains CPE Configuration Managers for zNID-GE-4220, zNID-GPON-4220, zNID-GE-4224 CPE types, and is assigned to residential users.
- Group No.2 contains CPE Configuration Managers for zNID-GE-4220, zNID-GPON-4222, zNID-GE-4224 CPE types, and is assigned to business users.
- Use Case No.2:
 - Group No.1 contains CPE Configuration Managers for zNID-GE-4220, zNID-GE-4222, zNID-GE-4224 CPE types, and is assigned to all the interfaces under an ActiveE card.
 - Group No.2 contains CPE Configuration Managers for zNID-GPON-4220, zNID-GPON-4222, zNID-GPON-4224 CPE types, and is assigned to all the ONT interfaces under a GPON card.

Adding EZ Touch CPE by CPE Manager

To add a CPE by CPE manager, perform some steps with CLI first, and then configure the **Add CPE Device** dialog box:

- 1 Add a public address for the CPE manager with CLI.

Note that adding the public address for the MXK requires the MXK has already been given an IP address. This IP address needs to match the IP address on the uplink interface you plan to use for CPE manager.

For example:

```
cpe-mgr add public 192.168.254.1
```

- 2 Synchronize the MXK with ZMS by right-clicking the MXK device in the tree view and selecting **Synchronize with Device**.
- 3 By adding the public address, the NAT status is enabled in the MXK.
- 4 From the tree view, expand the ActiveE or GPON card, and then expand the Ethernet (GigE) port or ONU.
- 5 Right-click an Ethernet port or ONU, and select **CPE Management>Add CPE**.

Note that at this step, the CPE device is not physically attached to the port yet.

The **Add CPE device** dialog box appears.

- In the **Add CPE Device** dialog box:
 - Check the **Use CPE Manager to communicate with CPE** box.
 - Configure the **Community String** for the CPE device.

- For the GPON ONT, a **GPON Traffic Profile Index** must be selected for the GEM port.
- Select the **Port Mapping Compression Mode** to define how many ports maybe accessed using the NAT-PAT binding, the more ports are accessed per device, the fewer devices that will be able to be accessed. This field is mainly for GPON ONTs.

Full Compression: It is the default value. With full compression mode, the MXK can translate 3 ports per CPE device. Each MXK can support up to 1400 CPE devices.

Some Compression: Partial compression. With this mode, the MXK can translate 4 ports per CPE device. Each MXK can support up to 1000 CPE devices.

No Compression: With this mode, the MXK can translate 9 ports per CPE device. Each MXK can support up to 480 CPE devices. Security mode is not applicable in this case.

- Select the **Communication Type** to define whether those ports will use security protocol or not.

Normal: Security mode is disabled, Telnet and HTTP will be used.

Secure: Security mode is enabled, SSH and HTTPS will be used.

- Click **Add**.

6 After adding a CPE device by CPE manager, the public IP address and the base public port mapped to the CPE appear in the tree view.

7 And it creates the Port Address Translation (PAT) bindings for this CPE device automatically.

To verify or troubleshoot CPE managers in the PAT binding profiles at the MXK level, right-click an MXK and select **Modify**, and from the **Modify Device** dialog box click **PAT Bindings**. The **PAT Bindings** dialog box appears

To verify or troubleshoot CPE managers at the CPE level, right-click a CPE and select **CPE Management> CPE Manager**, and from the **Modify CPE Information** dialog box click **CPE Communication**. The **CPE Communication** dialog box appears

8 Ordinarily the default global CPE manager settings are acceptable. However if you need to change the default settings, such as Local VLAN ID, Local SLAN ID, or Concurrent Update Limit, you could use the **CPE Manager Global** window.

- In the **Modify Device** dialog box click **CPE Manager Global**, the **CPE Manager Global** window appears.

- **Local VLAN ID:** This is the VLAN ID used for the CPE manager as the management VLAN between a CO device and locally managed CPEs. VLAN 7 is the default management VLAN settings of Zhone zNIDs and EtherXtend devices. All CPEs must have a DHCP client on this same VLAN.



Note: The local VLAN ID value can NOT be changed if any CPEs are currently configured for even basic CPE manager use.

- **Local SLAN ID:** This is the SLAN ID used for the CPE manager as the management SLAN between a CO device and locally managed CPEs. It will be supported in the future.
- **Concurrent Update Limit:** It is the number of CPEs that can be updating at a time. Those updates must be automatically started by the MXK. By default, the concurrent update limit is 5.
- Click **Modify**.



Note: If ZMS was not able to communicate with the CPE when the CPE was added, initialize the CPE will be necessary. To initialize the CPE, right-click the CPE, and then select **CPE Management> Initialize CPE**.

Adding download servers for CPE Configuration Manager

Add one or multiple download servers' destination IP addresses and login credentials. Make sure the download server is reachable by the MXK. And this server stores the desired CPE software image file and the generic or specific configuration file that could be downloaded to the CPE Configuration Manager provisioned CPEs. This server must support the file transfer methods required by the CPEs (ftp or sftp) for both upload and download.

To add a download server by CPE Configuration Manager:

- 1 Right-click an MXK and select **Modify**, and from the **Modify Device** dialog box click **CPE Manager Download Servers**. The **CPE Manager Download Servers** window appears.
- 2 Click **Add**.
The **Add CPE Manager** dialog box appears.
- 3 In the dialog box:
 - Enter the **Server IP address** of the download server.
 - Enter the **User Name** and **Password** of the download server. CPE needs them when accessing files on the download server. The username and password are currently character limited to 16 characters.

- Select this download server is default server or not. If set to True, when a new CPE configuration manager is created that does not select a Download Server, then the index of this default server will be used. This is only used during config time, not runtime.
 - Click **Add**.
- 4 The newly created download server appears in the **CPE Manager Download Servers** window.
 - 5 To modify the information for a download server, select it in the **CPE Manager Download Server** window, then click **Modify**.
Make the changes in the dialog box, then click **Modify** to save them.

Creating CPE Configuration Manager

To create a CPE Configuration Manager:

- 1 Right-click an MXK and select **Modify**, and from the **Modify Device** dialog box click **CPE Manager Configuration Managers**. The **CPE Manager Configuration Managers** window appears.
- 2 Click **Add**.
The **Add CPE Manager** dialog box appears.
- 3 In the dialog box:
 - Enter the **Name** of the CPE Configuration Manager. A CPE Configuration Manager must have a name. The maximum length of the name is 32 characters.
 - Assign a CPE Configuration Manager Group index to the CPE Configuration Manager in the **CPE Manager Group** field.
 - Specify the **CPE Type**. The CPE type is case-sensitive and must match what shown in the CPE WEBUI status window, e.g. ZNID-GE-4220, ZNID-GPON-4224.
 - Specify the **Required CPE SW Version** field. If the software version reported by the connected CPE doesn't match the required CPE SW version that defined in the MXK CPE Configuration Manager, then a software update will be initiated for the CPE. The software version number must start with the uppercase S for SIP zNID software file, or start with the uppercase M for an MGCP zNID software file. For examples: S2.2.030, M2.2.020.
 - Specify the **Required CPE SW File** field. The software file name is case-sensitive, it must match the one stored in the download server. The maximum length of the software file name is 32 characters. This file must be available in the base path location on the download server.

- Specify the **Required CPE Web UI Version** field. This field only applies to certain CPE types, such as EthX3444 and EthX3484. If the WEBUI version reported by the connected CPE does not match the required CPE WebUI version that defined in the MXK CPE Configuration Manager, then an upgrade of the WEBUI file will be initiated.



Caution: If set the **Required CPE Web UI Version** field to the CPEs that do not support it, will cause problems.



Note: It is recommended to leave the **Required CPE Web UI Version** field blank, but set the **Required CPE Web UI File** field. In that case the CPE will be told to download a new WEB UI file whenever it is also told to download a new software image file. This allows the WEB UI file to be tied directly to the software image version.

- Specify the **Required CPE Web UI File** field. The CPE WEB UI file must be available in the base path location on the download server. The maximum length of the WEB UI filename is 32 characters.
- Specify the **Required CPE Generic Config File** field. Generic configuration files are CPE type specific. A unique generic configuration file must be created for every CPE type that is deployed in the network. The generic configuration filename should include the four digit CPE model number for ease of identification. For example, generic4220.conf. The generic configuration filename is case-sensitive, it must match the one stored in the download server. The maximum length of the configuration file name is 32 characters.



Note: Note that if the Required CPE Generic Configuration File is specified in the CPE Configuration Manager, the CPE has to specify the Specific Configuration Filename for the configuration backup purpose.

CPE will look for the specific configuration file first, if cannot find the file in the download server, then look for the generic configuration file. If the names of the generic configuration file do not match, the CO device will inform the CPE to download the generic configuration file from the download server at the base path location.

- Specify the **CPE Lease Time update** field. This field indicates the short lease time (in seconds) granted to a CPE during download of files. This field is also used for throttling a download storms. The default value is 300 seconds. This value should be long enough to accommodate the maximum time to download all files a CPE may need.

- Specify the **CPE Lease Time Oper** field. This field indicates the long lease time (in seconds) granted to a CPE if there is no upgrade required. The default value is 86400 seconds (1 day). This value should be short enough to accommodate frequent checks for configuration changes, but not too frequent to burden the CO device.
- Select a download server index in the **CPE Manager Download Server** field.
- Specify the base path on the download server in the **CPE Manager Download Path** field. This path location will contain the software image, WEBUI file, generic configuration file, and sub-paths to CPE specific configuration files. The maximum length of the base pathname is 32 characters.
- Select the download secure mode in the **CPE Manager Secure Downloads** field.
 Disable means do not use secure download methods (use ftp or tftp).
 Enable means use secure download methods (sftp).
 No preference is the default value.
- Disable or Enable whether traps are sent from the CO device for events relating to this CPE Configuration Manager in the **CPE Manager Traps** field. Default value is Enabled.
- Click **Add**.

4 The newly created CPE Configuration Managers appear in the **CPE Manager Configuration Managers** window.

5 To modify the information for a CPE Configuration Manager, select it in the window, then click **Modify**.

Make the changes in the dialog box, then click **Modify** to save them.

Adding CPE Configuration Manager Member to CPE Configuration Manager Group

After completed global settings of the CPE Configuration Manager. You can add CPE Configuration Manager members to the CPE Configuration Manager group now. By adding an interface to a CPE Configuration Manager group, the attached CPE can be provisioned by the matching CPE Configuration Manager in the group.

To add an interface to the CPE Configuration Manager group:

- 1** From the tree view, expand the ActiveE or GPON card, and then expand the Ethernet (GigE) port or ONU, Right-click the interface and select **CPE Management>CPE Manager**, and from the **Modify CPE Information** dialog box click **CPE Manager Config**. The **CPE Manager Config** dialog box appears.
- 2** In the **CPE Manager Config** dialog box:

- Specify a CPE Configuration Manager group ID to this interface in the **CPE Manager Group** field to indicate which group the attached CPE is a member. This field is required and must point to a valid Group index.
- Enable or disable whether traps are sent from the CO device for events relating to the CPE Configuration Manager Member in the **CPE Manager Trap Enable** field.
- Specify the specific configuration filename for this CPE in the **Specific Configuration File**. CPE will look for the specific configuration file with this filename in the specific download path of the download server, if found it, then download it. The maximum length of the specific configuration filename is 32 characters.



Note: The Specific Configuration Filename has to be specified in order to do the EZ touch backup on the CPE device.

- Specify the **Specific Download Path** field. This is the path to the CPE specific configuration files. This path is a sub-path to the base path of the download server. The default value of this field is <CO Public IP address>/<slot>/<port>/<subport>/<interface type>. User can define their own values, however, this path must exist for files to be downloaded. The maximum length of the specific download pathname is 40 characters. If the CPE is required to upload to this path, it may create this path before doing the upload. The total path the CPE will use to access specific configuration files is a concatenation of these two path fields:

<CPE Configuration Manager Download Base Path>/ <CPE Configuration Manager Specific Download Path>
- Click **Modify**.

Viewing CPE Configuration Manager Member runtime details

After activating the attached CPE device, you will be able to view the runtime details of CPE Configuration Manager Members, use the **CPE Manager Status** window and the **CPE Information** window.

- 1 From the tree view, expand the ActiveE or GPON card, and then expand the Ethernet (GigE) port or ONU, Right-click the interface and select **CPE Management > CPE Manager**, and from the **Modify CPE Information** dialog box click **CPE Manager Status**. The **CPE Manager Status** dialog box appears.
- 2 Click **CPE Information**. The **CPE Information** dialog box appears.

Configuring Malc XP device settings

- 1 Right-click a Malc XP device and select **Modify**. The **Modify Device Configuration** dialog box appears.

- 2 Select the desired settings.

For information on the settings, see the online help.

Configuring Raptor XP device settings

- 1 Right-click a Raptor XP device and select **Modify**. The **Modify Device Configuration** dialog box appears.
- 2 Select the desired settings.

For information on the settings, see the online help.

Configuring MXK device settings

- 1 Right-click an MXK device and select **Modify**. The **Modify Device Configuration** dialog box appears.
- 2 Select the desired settings.

For information on the settings, see the online help.

Configuring 1U MX-150 device settings

The MX-150 platform provides low-cost, high-density subscriber access concentration in the Zhone Single Line Multi-Service (SLMS) architecture.

The MX-150 is a next generation design that carries data and video services over DSL lines and Gigabit Ethernet/Fast Ethernet uplinks. The NetHorizon aggregates local loop traffic from a variety of media and sends it to an upstream Fast Ethernet/Gigabit Ethernet device.

The MX-150 can be deployed in Central Office environments, outdoor cabinets, or controlled environmental vaults for remote terminal applications. The MX-150 is intended for restricted access locations only.

The MX-150 includes the following model

- MX-150A
48-port ADSL2+, no splitters, 2 FE/GE uplink ports.
 - MX-151A
48-port ADSL2+, 600 Ohm splitters, 2 FE/GE uplink ports.
 - MX-152A
48-port ADSL2+, 900 Ohm splitters, 2 FE/GE uplink ports.
- 1 Right-click an MX-150 device (the MX-150 includes the models: MX-150A, MX-151A, MX-152A) and select **Modify**. The **Modify Device Configuration** dialog box appears.

- 2 Select the desired settings.

For information on the settings, see the online help.

Configuring 1U MX-160, MX-161, MX-162 device settings

- 1 Right-click an MX-160 device (the MX-160 includes the models: MX-160, MX-161, MX-162, MX-160-16P) and select **Modify**. The **Modify Device Configuration** dialog box appears.
- 2 Select the desired settings.

For information on the settings, see the online help.

Configuring 1U MX-180, MX-280 device settings

- 1 Right-click an MX-180 device (the MX-180 includes the models: MX-180, MX-280, MX-180-LT-TP-RJ45) and select **Modify**. The **Modify Device Configuration** dialog box appears.
- 2 Select the desired settings.

For information on the settings, see the online help.

Configuring 1U MX-260, MX-261, MX-262 device settings

The MX-260 platform provides low-cost, high-density subscriber access concentration in the Zhone Single Line Multi-Service (SLMS) architecture.

The MX-260 is a next generation design that carries data and video services over VDSL2 lines and Gigabit Ethernet/Fast Ethernet uplinks. The MX-260 aggregates local loop traffic from a variety of media and sends it to an upstream Fast Ethernet/Gigabit Ethernet device.

The MX-260 can be deployed in Central Office environments, outdoor cabinets, or controlled environmental vaults for remote terminal applications. The MX-260 is intended for restricted access locations only.

The MX-260 platform includes the following models:

- MX-260
MX-260 24 ports VDSL2+ with three FE/GE uplinks and one GPON uplink.
 - MX-261
MX-261 24 ports VDSL2+ with 600 ohm POTS splitters, three FE/GE uplinks, and one GPON uplink.
 - MX-262
MX-262 24 ports VDSL2+ with 900 ohm POTS splitters, three FE/GE uplinks, and one GPON uplink.
- 1 Right-click an MX-260, MX-261, or MX-262 device and select **Modify**. The **Modify Device Configuration** dialog box appears.

2 Select the desired settings.

For information on the settings, see the online help.

Configuring 1U MXP-150 device settings

The MXP-150 platform provides low-cost, high-density subscriber access concentration in the Zhone Single Line Multi-Service (SLMS) architecture.

The MXP-150 is a next generation design that carries voice, data, and video services over DSL lines and Gigabit Ethernet/Fast Ethernet uplinks. The NetHorizon aggregates local loop traffic from a variety of media and sends it to an upstream Fast Ethernet/Gigabit Ethernet device.

The MXP-150 can be deployed in Central Office environments, outdoor cabinets, or controlled environmental vaults for remote terminal applications. The NetHorizon is intended for restricted access locations only.

The MXP-150 model is MXP-150A, 48-port ADSL2+, Annex A, VOIP/POTS, 2 FE/GE uplink ports.

1 Right-click an MXP-150 device and select **Modify**. The **Modify Device Configuration** dialog box appears.

2 Select the desired settings.

For information on the settings, see the online help.

Configuring 1U MXP-160, MXP-260 device settings

The MXP-160/260 platform provides low-cost, high-density subscriber access concentration in the Zhone Single Line Multi-Service (SLMS) architecture.

The MXP-160/260 is a next generation design that carries data, voice, and video services over VDSL2 lines and Gigabit Ethernet/Fast Ethernet uplink interfaces for GPON interface. The MXP-160/260 aggregates local loop traffic from a variety of media and sends it to an upstream Fast Ethernet/Gigabit Ethernet device. The MXP-160/260 supports 24 ports of VDSL2 traffic and life-line POTS to deliver high-definition, multiple standard definition video streams, high speed data, and packet voice services to each subscriber.

The MXP-160/260 can be deployed in Central Office environments, outdoor cabinets, or controlled environmental vaults for remote terminal applications. The NetHorizon is intended for restricted access locations only.

The MXP-160/260 includes the following models:

- MXP-160

MXP-160 provides 24 ports of VDSL2+ and four 100/1000 Mbps Ethernet slots (copper or fiber) with VoIP POTS.

- MXP-260

MXP-260 provides 24 ports of VDSL2+ with three 100/1000 Mbps Ethernet slots (copper or fiber) and one GPON uplink with VoIP POTS.

- 1 Right-click an MXP-160 or MXP-260 device and select **Modify**. The **Modify Device Configuration** dialog box appears.
- 2 Select the desired settings.

For information on the settings, see the online help.

Configuring 1U MXP-180, MXP-280 device settings

The MXP-180/280 platform provides low-cost, high-density subscriber access concentration in the Zhong Single Line Multi-Service (SLMS) architecture.

The MXP-180/280 is a next generation design that carries data, voice, and video services over Fast Ethernet line interfaces and Gigabit Ethernet/Fast Ethernet uplink interfaces or GPON interface. The MXP-180/280 aggregates local loop traffic from a variety of media and sends it to an upstream Fast Ethernet/Gigabit Ethernet device. The MXP-180/280 supports 24 ports of Fast Ethernet traffic and life-line POTS to deliver high-definition, multiple standard definition video streams, high speed data, and packet voice services to each subscriber.

The MXP-180/280 can be deployed in Central Office environments, outdoor cabinets, or controlled environmental vaults for remote terminal applications. The NetHorizon is intended for restricted access locations only.

The MXP-180 provides four 100/1000 Mbps Ethernet SFP slots (copper or fiber) and 24 ports of Fast Ethernet SFP slots (copper or fiber) with VoIP POTS or, with the TP-RJ45 models, fixed RJ45 interfaces with VoIP POTS.

The MXP-280 provides three 100/1000 Mbps Ethernet SFP slots (copper or fiber) and one GPON uplink and 24 ports of Fast Ethernet SFP slots (copper or fiber) with VoIP POTS or, with the TP-RJ45 models, fixed RJ45 interfaces with VoIP POTS.

- 1 Right-click an MXP-180 or MXP-280 device and select **Modify**. The **Modify Device Configuration** dialog box appears.
- 2 Select the desired settings.

For information on the settings, see the online help.

Configuring 1U MXK-194, MXK-198 device settings

The MXK-194/198 platform provides low-cost, high-density subscriber access concentration in the Zhong Single Line Multi-Service (SLMS) architecture.

The MXK-194/198 is a next generation design that carries data and video services over GPON downlinks and Gigabit Ethernet/Fast Ethernet or,

depending on the model, 10 Gigabit Ethernet uplinks. The MXK-194/198 aggregates local loop traffic from a variety of media and sends it to an upstream Fast Ethernet/Gigabit Ethernet device.

The MXK-194/198 can be deployed in Central Office environments, outdoor cabinets, or controlled environmental vaults for remote terminal applications. The MXK-194/198 is intended for restricted access locations only.

The MXK-194/198 includes the following models:

- MXK-194
Four subscriber facing GPON ports, eight FE/GE uplinks.
 - MXK-198
Eight subscriber facing GPON ports, eight FE/GE uplinks.
- 1 Right-click an MX-194 or MX-198 device and select **Modify**. The **Modify Device Configuration** dialog box appears.
 - 2 Select the desired settings.

For information on the settings, see the online help.

Secure Shell (SSH)

Secure Shell (SSH) is a command interface and protocol for securely getting access to a remote computer. SSH commands are encrypted and secure in two ways. Both ends of the client/server connection are authenticated using a digital certificate, and passwords are protected by being encrypted. The user can run either SSH or Telnet command depending on the device security configuration.

The user can connect to a MALC or MXK using the SSH client of your choice to encrypt the session.

The user need to make sure the PC that installed ZMS client has the putty.exe installed in the *C:/Program Files/putty/* directory.

To open the SSH client, right-click a MALC or MXK device and select **SSH To Device**.

Configurable Temperature Alarm Severity and Ranges

The **Outlet Temperature High Threshold** and **Outlet Temperature Low Threshold** fields are added to the **Modify Device Configuration** and the **View Device Configuration** windows:

By default, **Outlet Temperature High Threshold** is set to 65, **Outlet Temperature Low Threshold** is set to -12.

A minor alarm is raised when the outlet temperature is at the **Outlet Temperature High Threshold**. Major alarm is raised when the outlet temperature is **Outlet Temperature High Threshold**+5. Critical alarm is raised when the outlet temperature is **Outlet Temperature High**

Threshold + 10. For example, if the **Outlet Temperature High Threshold** is configured as 35, alarms will be in the order of 35, 40, 45 for Minor, Major, and Critical. If the **Outlet Temperature High Threshold** is configured as 65, alarms will be in the order of 65, 70, 75 for Minor, Major, and Critical.

When the **Outlet Temperature Low Threshold** is set and the outlet sensor reaches the configured temperature, a Minor alarm is raised.

Create vdsl-vect-config

The VDSL vectoring profile supports configuration of VDSL vectoring Power Spectral Density (PSD) shapes and four upstream and four downstream disable bands for a VDSL vectoring group. Vectoring groups are supported on a Board Level Vectoring (BLV) basis.

The PSD shape is set on a slot or system basis. A system configuration is applied to all slots which do not have a slot-based configuration. The system configuration is created when the **Slot Number** parameter in the **Add VDSL Vectoring Profile** dialog box is set to 0. The slot configuration is created when the **Slot Number** parameter in the **Add VDSL Vectoring Profile** dialog box is set to the slot number.

The slot configuration overrides any system level configuration for a specific slot. Otherwise, adding and assigning new VDSL vectoring profiles or updating existing VDSL vectoring profiles are rejected if a slot is already assigned.

View vdsl-vect-config attributes

Viewing the vdsl-vect-config attributes

Access to the **Add/View/Modify VDSL Vectoring Profile** to view profile attributes and their allowed values.

- 1 Right-click a MXK device, and then select **Modify**.
- 2 In the **Modify Device Configuration** dialog box, select **VDSL Vectoring Profile** from the tree view.
- 3 Click **Add** in the **VDSL Vectoring Profiles** pane, the **Add VDSL Vectoring Profile** dialog box appears.

Same set of attributes and allowed values will be appeared in the **Modify VDSL Vectoring Profile** dialog box and the **View VDSL Vectoring Profile** dialog box as well.

[Table 5](#) defines the **vdsl-vect-config** profile attributes.

Table 5: vdsl-vect-config parameter definitions

Attributes	Definitions
Slot Number	This field is used to configure which slot will use the VDSL2 PSD Shape configured in the PSD Shape field for the given index.
PSD Shape	REGION-A-NUS0 REGION-A-EU-32 REGION-A-EU-36 REGION-A-EU-40 REGION-A-EU-44 REGION-A-EU-48 REGION-A-EU-52 REGION-A-EU-56 REGION-A-EU-60 REGION-A-EU-64 REGION-A-EU-128 REGION-A-ADLU-32 REGION-A-ADLU-36 REGION-A-ADLU-40 REGION-A-ADLU-44 REGION-A-ADLU-48 REGION-A-ADLU-52 REGION-A-ADLU-56 REGION-A-ADLU-60 REGION-A-ADLU-64 REGION-A-ADLU-128 REGION-B-998-M1X-A REGION-B-998-M1X-B REGION-B-998-M1X-NUS0 REGION-B-998-M2X-A REGION-B-998-M2X-M REGION-B-998-M2X-B REGION-B-998-M2X-NUS0 REGION-B-998-E17-M2X-NUS0 REGION-B-998-E17-M2X-NUS0-M REGION-B-998-ADE17-M2X-NUS0-M REGION-B-998-ADE17-M2X-A REGION-B-998-ADE17-M2X-B REGION-B-998-E30-M2X-NUS0 REGION-B-998-E30-M2X-NUS0-M REGION-B-998-ADE30-M2X-NUS0-M REGION-B-998-ADE30-M2X-NUS0-A REGION-B-997-M1C-A-7 REGION-B-997-M1X-M-8 REGION-B-997-M1X-M REGION-B-997-M2X-M-8 REGION-B-997-M2X-A REGION-B-997-M2X-M REGION-B-997-HPE17-M1-NUS0 REGION-B-997-HPE30-M1-NUS0 REGION-B-997-E17-M2X-A REGION-B-997-E30-M2X-NUS0 REGION-B-997-BT-ANFP REGION-C-138-B REGION-C-276-B REGION-C-138-CO REGION-C-276-CO REGION-C-TCMISDN REGION-C-1104-CO-17A REGION-C-1104-CO-30A DISABLED This field is used to configure the VDSL2 PSD Shape on Vectoring enabled blades. Vectoring expects all ports to have the same or compatible PSD shapes. When set to a PSD shape this field updates the PSD shape for all ports on the blade and sets the vectoring application PSD shape.
Downstream Disable Start Tone1	Configuration of the start tone index for the first downstream tone band used for VDSL vectoring disabling. The range for each field is 0-4096. Default: 0
Downstream Disable End Tone1	This value must be greater than Downstream Disable Start Tone1. If a band fails validation it is not configured, validation stops, and subsequent bands are ignored. Any previous band which passed validation is still accepted and configured. The range for each field is 0-4096. Default: 0

Table 5: vdsl-vect-config parameter definitions (Continued)

Attributes	Definitions
Upstream Disable Start Tone1	Configuration of the start tone index for the first upstream tone band used for VDSL vectoring disabling. The range for each field is 0-4096. Default: 0
Upstream Disable End Tone1	Configuration of the end tone index for the first upstream tone band used for VDSL vectoring disabling. This value must be greater than Upstream Disable Start Tone1. If a band fails validation, it is not configured, validation stops, and subsequent bands are ignored. Any previous band which passed validation is still accepted and configured. The range for each field is 0-4096. Default: 0
Downstream Disable Start Tone2	Configuration of the start tone index for the second down stream tone band used for VDSL vectoring disabling. This value must be greater than Downstream Disable End Tone1. If a band fails validation, it is not configured, validation stops, and subsequent bands are ignored. Any previous band which passed validation is still accepted and configured. The range for each field is 0-4096. Default: 0
Downstream Disable End Tone 2	Configuration of the end tone index for the second downstream tone band used for VDSL vectoring disabling. This value must be greater than Downstream Disable Start Tone2. If a band fails validation, it is not configured, validation stops, and subsequent bands are ignored. Any previous band which passed validation is still accepted and configured. The range for each field is 0-4096. Default: 0
Upstream Disable Start Tone 2	Configuration of the start tone index for the second upstream tone band used for VDSL vectoring disabling. This value must be greater than Upstream Disable End Tone1. If a band fails validation, it is not configured, validation stops, and subsequent bands are ignored. Any previous band which passed validation is still accepted and configured. The range for each field is 0-4096. Default: 0
Upstream Disable End Tone 2	Configuration of the end tone index for the second upstream tone band used for VDSL vectoring disabling. This value must be greater than Upstream Disable Start Tone 2. If a band fails validation, it is not configured, validation stops, and subsequent bands are ignored. Any previous band which passed validation is still accepted and configured. The range for each field is 0-4096. Default: 0

Table 5: vdsl-vect-config parameter definitions (Continued)

Attributes	Definitions
Downstream Disable Start Tone 3	Configuration of the start tone index for the third down stream tone band used for VDSL vectoring disabling. This value must be greater than Downstream Disable End Tone2. If a band fails validation, it is not configured, validation stops, and subsequent bands are ignored. Any previous band which passed validation is still accepted and configured. The range for each field is 0-4096. Default: 0
Downstream Disable End Tone3	Configuration of the end tone index for the third downstream tone band used for VDSL vectoring disabling. This value must be greater than Downstream Disable Start Tone3. If a band fails validation, it is not configured, validation stops, and subsequent bands are ignored. Any previous band which passed validation is still accepted and configured. The range for each field is 0-4096. Default: 0
Upstream Disable Start Tone3	Configuration of the start tone index for the third upstream tone band used for VDSL vectoring disabling. This value must be greater than Upstream Disable End Tone2. If a band fails validation, it is not configured, validation stops, and subsequent bands are ignored. Any previous band which passed validation is still accepted and configured. The range for each field is 0-4096. Default: 0
Upstream Disable End Tone3	Configuration of the end tone index for the third upstream tone band used for VDSL vectoring disabling. This value must be greater than Upstream Disable Start Tone3. If a band fails validation, it is not configured, validation stops, and subsequent bands are ignored. Any previous band which passed validation is still accepted and configured. The range for each field is 0-4096. Default: 0
Downstream Disable Start Tone4	Configuration of the start tone index for the fourth down stream tone band used for VDSL vectoring disabling. This value must be greater than Downstream Disable End Tone3. If a band fails validation, it is not configured, validation stops, and subsequent bands are ignored. Any previous band which passed validation is still accepted and configured. The range for each field is 0-4096. Default: 0

Table 5: vdsl-vect-config parameter definitions (Continued)

Attributes	Definitions
Downstream Disable End Tone4	Configuration of the end tone index for the fourth downstream tone band used for VDSL vectoring disabling. This value must be greater than Downstream Disable Start Tone4. If a band fails validation, it is not configured, validation stops, and subsequent bands are ignored. Any previous band which passed validation is still accepted and configured. The range for each field is 0-4096. Default: 0
Upstream Disable Start Tone4	Configuration of the start tone index for the fourth upstream tone band used for VDSL vectoring disabling. This value must be greater than Upstream Disable End Tone 3. If a band fails validation, it is not configured, validation stops, and subsequent bands are ignored. Any previous band which passed validation is still accepted and configured. The range for each field is 0-4096. Default: 0
Upstream Disable End Tone4	Configuration of the end tone index for the fourth upstream tone band used for VDSL vectoring disabling. This value must be greater than Upstream Disable Start Tone 4. If a band fails validation, it is not configured, validation stops, and subsequent bands are ignored. Any previous band which passed validation is still accepted and configured. The range for each field is 0-4096. Default: 0

vdsl-vect-config profile configuration

Rules for creating vectoring groups:

- Each VDSL vectoring profile represents one vectoring group. Vectoring groups are supported on a board level vectoring basis (BLV).
- Cards are assigned to a VDSL vectoring profile by the value in the **Slot Number** field.
- Each VDSL vectoring profile can have only one slot value in the **Slot Number** field.
- Each vectoring group can have only one board profile assigned to it.
- There can be only one system profile per MXK chassis.
- Each slot can have the system profile assigned to it.

Rules for vectoring configuration usage:

- Adding or updating the system VDSL vectoring profile PSD shape will cause a reset on every line for every vectoring card assigned to that profile.

- Adding or updating the VDSL vectoring profile for a specific slot will cause a reset on all the lines for that card.
- Setting the **PSD Shape** in the VDSL vectoring profile to any PSD shape other than *DISABLED* will reset and enable VDSL vectoring by assigning that PSD shape to the VDSL vectoring group and all the ports associated with that VDSL vectoring profile.

When configuring the VDSL vectoring profile:

- The disable band end tone index must be greater than the corresponding disable band start tone index. For example starting with:
Downstream Disable End Tone1 > Downstream Disable Start Tone1
Upstream Disable End Tone1 > Upstream Disable Start Tone1
- The disable band start tone index for a subsequent band must be greater than the preceding disable band's disable band end tone index. For example:
Downstream Disable Start Tone2 > Downstream Disable End Tone1
Upstream Disable Start Tone2 > Upstream Disable End Tone1
- Only tone bands which follow the first two rules will be applied. If any tone band is zero, or is not starting at a higher index, it and all subsequent tone bands are ignored.
- Keeping the default of 0 allows all tones.

Card configuration

Topics:

[Adding a single card](#)

[Adding multiple cards](#)

[Enabling a card](#)

[Adding redundant MALC, MXK and Raptor cards](#)

[Modifying redundant MALC, MXK, or Raptor cards](#)

[Modifying card configurations](#)

[Rebooting a single card](#)

[Viewing card state](#)

[Setting the card default image](#)

[Deleting a card](#)

[Deleting a software image](#)

[Configuring a clock source](#)

[Viewing clock source status](#)

[Changing VCL rates](#)

[Creating an ATM VPI profile](#)

[Modifying a card's ATM bandwidth settings](#)

[Modifying GigaMux 1600/3200 card configurations](#)

[Modifying EFM SHDSL card configurations](#)

Adding a single card

If you are adding a redundant card, see [Adding redundant MALC, MXK and Raptor cards on page 133](#).

To add a card:

- 1 Right-click an empty slot and select **Add**.

The Add Card wizard appears.

- 2 Select the type of card you want to add and click the next button.

The **Configuration** dialog box appears. The example below shows an ADSL card.

- 3 (Optional) Change the name of the software image used by the card.

To change the name of the software image, click the **Change** button and enter the filename. Then click **OK**.



Note: The software image must be on the device. See [Downloading a software image to a single or multiple devices on page 71](#).

- 4 For ATM-capable cards, specify the **ATM Configuration**.

This setting determines what portion of the bandwidth is devoted to various ATM service categories.

For information on the settings, see the online help.

- 5 Click **Add**.

For existing cards, ZMS makes the changes on the device.

For each new card, ZMS creates a card profile on the device.

In the device chassis dialog box, NetHorizon changes each new card state from **Not Configured** to **Reserved**.

Once a new card is inserted in the slot and the card becomes active, ZMS obtains the card's configuration information from the device (this process may take some time). Once the information is received, NetHorizon removes the status **Reserved** from the card. The card is now active.

Related topics:

[Adding redundant MALC, MXK and Raptor cards on page 133](#)

[Modifying a card's ATM bandwidth settings on page 144](#)

[Modifying redundant MALC, MXK, or Raptor cards on page 134](#)

[Redundancy overview on page 457](#)

[Viewing card state on page 136](#)

Adding multiple cards

NetHorizon provides a shortcut that you can use to add many cards to a device from a single screen.

To add multiple cards to a device:

- 1 Right-click the **Cards** icon for the device and select **Configure Cards**.

The device chassis dialog box appears. This dialog box displays all the configured cards in the chassis. Empty slots contain a drop down list box listing the cards that can be installed in that slot.

- 2 To add a card, select the card from the **Type** field, select the card installed in that slot.

While you configure new cards, they are listed with the card state **Not Configured**.

When you select a card type, NetHorizon automatically fills in the basic settings for the card in the remaining fields in the dialog box. In most cases, the defaults should be accepted.

If you need to modify the ATM configuration for ATM-capable cards, see the online help for a description of the ATM parameters.

- 3 If you want to reset the card settings for the card you are configuring, click **Reset**.

NetHorizon resets the parameters to the values that were last saved (only for the selected card).

- 4 Continue adding cards to the system. When finished, click **Apply**.

After clicking **Apply**, the following occurs:

- For existing cards, ZMS makes the changes on the device.
- For each new card, ZMS creates a card profile on the device.
- In the device chassis dialog box, NetHorizon changes each new card state from **Not Configured** to **Reserved**. In the tree display, each new card has the status **Reserved**.
- Once a new card is inserted in the slot and the card becomes active, ZMS obtains the card's configuration information from the device (this process may take some time). Once the information is received, NetHorizon removes the status **Reserved** from the card in the tree display. The card is now active.

Related topics:

[Adding a single card on page 131](#)

[Modifying a card's ATM bandwidth settings on page 144](#)

[Viewing card state on page 136](#)

Enabling a card

When a card's **Admin Status** parameter is set to **Disabled**, the card is disabled from accepting requests from other elements and is not completely manageable by ZMS.

NetHorizon displays the card in the tree display with the status **Disabled**. To recover ZMS manageability for the card, re-enable the card.

- 1 Right-click a card and select **Enable Card**.
- 2 At the confirmation prompt, click **Yes**.

NetHorizon re-enables the card.

Keep in mind that enabling may take several minutes. During the process, the card has the status **Enabling**. The card and all its children appear dimmed in the tree display. You cannot perform tasks on objects that appear dimmed.

When the card is fully enabled, the card and its children are no longer dimmed in the tree display.

Related topics:

[Deleting a card on page 138](#)

[Deleting a software image on page 138](#)

[Downloading a software image to a single or multiple devices on page 71](#)

[Rebooting a single card on page 136](#)

[Setting the card default image on page 137](#)

[Viewing card state on page 136](#)

Adding redundant MALC, MXK and Raptor cards

MALC, MXK and Raptor devices support the following redundant card types:

- mtac/tac (metallic) cards
- Uplink cards

When you add a second MTAC card of the same type to a device, ZMS automatically groups the cards into a redundancy group and assigns a group number. Each card represents a card redundancy entry in the group.



Note: ZMS assigns the redundancy group number to associate the cards in the group. This group number may differ from the **card-group-id** set by the CLI.

To add a redundant card:

- 1 The Add Card wizard appears.
- 2 Right-click an empty slot next to an active card that supports redundancy and click **Add**.
- 3 Select the type of card you want to add and click the next button.
The **Configuration** dialog box appears.
- 4 Specify the card this card is to be made redundant with.
The card must be of the same type.
- 5 Accept the rest of the defaults unless you want to change the name of the software image used by the card.



Note: Both redundant cards must use the same software image.

To change the name of the software image, click the **Change** button and enter the filename. Then click **OK**.

- 6 Click **Add**.
NetHorizon adds the card to the device. Since this is a redundant card, perform all configuration, with the exception of the physical interface configuration, on the active card. As changes are made to the active card configuration, they are copied over to the standby card.

Related topics:

[Redundancy overview on page 457](#)

Modifying redundant MALC, MXK, or Raptor cards

By default, MALC, MXK, and Raptor redundant cards have the same redundancy weight. This means that all cards have an equal chance to become active. If you want to make a particular card the preferred active card, assign a preference to it.

To modify card redundancy settings:

- 1 right-click a card redundancy group and select **Modify**.
The **Modify Card** dialog box appears.
- 2 In the tree view, select **Redundant Cards**.
The **Redundant Cards** screen appears. This screen displays the current redundancy options for the cards.
- 3 Highlight the card you want to change and select **Modify**.
The **Modify Card Redundancy State Configuration** dialog box appears.
- 4 Change the weight, as necessary.
- 5 Click **Modify** then **Close**.

Related topics:

[Redundancy overview on page 457](#)

[Adding redundant MALC, MXK and Raptor cards on page 133](#)

Modifying card configurations

Card configurations, for example ReachDSL, can be modified from ZMS.

To modify a card configurations

- 1 Select the desired card in the ZMS tree.
- 2 From the right-click menu, select **Modify**.

The **Modify [card] Configuration** dialog appears with quick options for hardware, configuration, status, runtime, and software.

Hardware options are view-only and cannot be modified. Click **Close** to exit the dialog box.

- 3 For configuration options, click Configuration. The configuration options appear.

The following options appear:

- Name
- Slot ID
- Current Ver FileName
- Software Load (Enable/Disable)
- Line Voltage

After completing the software changes, click **Modify** to apply the changes. Click **Reset** to return to the default settings. Click **Refresh** to update the displayed settings. Click **Close** to exit the dialog box.

- 4 For status options, click Status. The status options appear.

The Status options are view-only and cannot be modified. Click **Close** to exit the dialog box.

- 5 For runtime options, click Runtime. The Runtime options appear.

The Runtime options are view-only and cannot be modified. Click **Close** to exit the dialog box.

- 6 For software options, click Software. The software options appear.

The following options appear:

- Current S/W Version
- Upgrade Ver Filename
- Software Upgrade (Enable)
- Software Upgrade Status

After completing the software changes, click **Modify** to apply the changes. Click **Reset** to return to the default settings. Click **Refresh** to update the displayed settings. Click **Close** to exit the dialog box.

Related topics:

[Applying physical port templates to a port on page 160](#)

[Creating ADSL Alarm templates on page 152](#)

Rebooting a single card

For some cards, such as non-redundant MALC or Raptor Uplink cards, rebooting a card reboots the entire device.

To reboot a card:

- 1 Right-click a card and select **Reboot**.
- 2 At the confirmation prompt, click **Yes**.

NetHorizon reboots the card.

Keep in mind that it can take some time for the reboot process to complete. During the process, the card has the status **Rebooting**. The card and all its children appear dimmed in the tree display. You cannot perform tasks on objects that appear dimmed.

When the reboot process is complete, the card and its children are no longer dimmed in the tree display.

Related topics:

[Deleting a card on page 138](#)

[Downloading a software image to a single or multiple devices on page 71](#)

[Enabling a card on page 133](#)

[Downloading a software image to a single or multiple devices on page 71](#)

[Setting the card default image on page 137](#)

[Viewing card state on page 136](#)

Viewing card state

To view the status of the cards in a device:

- 1 Right-click the card icon for a device and select **View Card States**.
The **Card States** dialog box appears.

Possible state are:

Blocked From Booting: Card is blocked from booting.

Booting: Card is booting from EEPROM.

Configuring: card is downloading its software image.

Dumping: Card is dumping fatal data

Empty: Slot is empty.

Hardware Not Present: The slot may have been configured, but the card has been physically removed from the chassis.

In Fault: Card is in a fault state.

Inserted: The card has been physically installed in the chassis, but it has not been configured.

Loading: Card is loading code from code loader

Performing Post Tests: Card is performing POST tests.

Reserved: Card has been configured from NetHorizon but not physically installed.

Rebooting: Card is resetting.

Running: card is physically installed and operational.

- 2 To refresh the display click **Refresh**.

Related topics:

[Adding a single card on page 131](#)

[Shelf monitoring on page 140](#)

Setting the card default image

Once you have downloaded a software image, you can specify which cards, by default, use the software image.

- 1 Right-click the device and click **Set Card Default Image**.

NetHorizon displays the **Card Default Image** dialog box for the device.

- 2 Complete the parameters in the **Card Default Image** dialog box:

Card Type—Choose the card type.

Default Image File Name—Enter the file name for the code image to be used by cards of that type.

- 3 Click **Modify**.

NetHorizon sets the default software image. Note that this image name can be overridden by the setting in the **Card Configuration** dialog box (accessed by right clicking the Card icon and selecting **Configure Cards**).

Related topics:

[Deleting a card on page 138](#)

[Downloading a software image to a single or multiple devices on page 71](#)

[Enabling a card on page 133](#)

[Downloading a software image to a single or multiple devices on page 71](#)

[Rebooting a single card on page 136](#)

[Setting the card default image on page 137](#)

[Viewing card state on page 136](#)

Deleting a card

Deleting a card removes it from NetHorizon. After a card has been deleted it can no longer be managed. Deleting a line card also deletes associated items with that card, such as subscribers and VCLs.



Note: Voice subscribers must be deleted from voice cards before the card can be deleted.

To delete a card:

- 1 First, disable the card. Right-click a card and select **Disable Card**.
NetHorizon disables the card.
- 2 Right-click the disabled card and select **Delete**.
- 3 In the confirmation dialog box, click **OK**.

Related topics:

[Deleting a software image on page 138](#)

[Enabling a card on page 133](#)

[Downloading a software image to a single or multiple devices on page 71](#)

[Rebooting a single card on page 136](#)

[Setting the card default image on page 137](#)

[Viewing card state on page 136](#)

Deleting a software image

You can delete a software image that is no longer used by cards on a device (not supported on the Sector 100A or Z-Edge).

- 1 Right-click a device and select **Delete Software Image**.
NetHorizon displays the **Delete Software Image** dialog box for the device.
- 2 Enter the pathname for the software image to be deleted.
- 3 Click **Delete**.
NetHorizon deletes the software image.

Keep in mind that it can take some time for the delete process to complete.

- 4 To check the status of the deletion, click **Refresh**. NetHorizon updates the **Delete Status** parameter with the current status from the device.

The **Delete Status** parameter indicates when the deletion is successful.

Related topics:

[Deleting a card on page 138](#)

[Enabling a card on page 133](#)

[Downloading a software image to a single or multiple devices on page 71](#)

[Rebooting a single card on page 136](#)

[Setting the card default image on page 137](#)

[Viewing card state on page 136](#)

Configuring a clock source

Note the following information about redundant clock sources:

- Only interfaces that are active are eligible to provide the system clock.
- By default, interfaces are not eligible to provide clock.
- The clock source with the highest weight becomes the active clock source. Weights are from 1 (lowest priority) to 10 (highest priority).
- If there are multiple active interfaces configured as eligible clock sources, the system selects a clock source based on the weight configured in the **System Clock Source** dialog box.
- If multiple eligible clock sources are configured with the same weight, the first active source becomes the clock source.
- By default, clock sources are revertive. If a standby clock source becomes active after the failure of a primary clock source, the system will revert to the primary clock source after that clock source becomes active again. Note that the clock source must be active for 30 seconds before the system will revert back to the primary clock source.

To configure a clock source:

- 1 Right-click a device and select **Modify**.
The **Modify Device Configuration** dialog box appears.
- 2 In the tree view, click **System Clock Source**.
The **System Clock Source** dialog box appears.
- 3 (Optional). Change the clock source to non-revertive, or accept the default (revertive)
- 4 Click **Configure**.
The **Configure System Clock Source** dialog box appears.

- 5 Select the **Eligibility** checkbox next to a clock source to mark it as eligible.
- 6 (Optional). Set a weight for the clock source.
- 7 Click **Modify**.
- 8 Click **Close**.

Related topics:

[Viewing clock source status on page 140](#)

Viewing clock source status

To view clock source status:

- 1 Right-click a device and select **Modify**.
The **Modify Device Configuration** dialog box appears.
- 2 In the tree view, click **System Clock Source**.
The **System Clock Source** screen appears.
- 3 Click **Status**.
The **System Clock Source Status** dialog box appears.
- 4 To refresh the display, click **Refresh**.
- 5 When finished, click **Close**.

Related topics:

[Configuring a clock source on page 139](#)

Shelf monitoring

To view specific shelf assets and functional status, right-click on the device which you want to monitor and then select **View Shelf Status**.

The **View Shelf Monitoring** dialog box appears.

This screen displays the following information:

- **Identification of Shelf Assets**—Displays identifying information about the shelf
- **Shelf status**—Displays the status of the shelf's power, temperature, fan tray, and contact alarms, as well as the number of shelf resets.
- **Fans on Shelf**—Displays the speed of the fans in the shelf as well as the threshold speeds which will trigger user alerts if any fan is measured to be operating at less than the threshold.
- **Temperature Sensors on Shelf**—Displays the readings from temperature sensors on the shelf as well as high and low threshold temperatures which will trigger user alerts.

Related topics:

[Viewing card state on page 136](#)

Network Time Protocol

NetHorizon supports the Simple Network Time Protocol (NTP), described in RFC 2030. SNTP synchronizes devices on the network with a timing source. When NTP is enabled, setting the system time with the CLI **setdatetime** command is not allowed.

The device will get the time from the NTP server every hour. If the system clock has drifted more than 9 seconds from the source clock, the system time will be reset.

To enable NTP:

- 1 Right click a device and select **Modify**.
The **Modify Device Configuration** dialog box appears.
- 2 Click **NTP Config**.
The **NTP Config** dialog box appears.
- 3 Enter the following information:
 - **Primary Server IP Address:** The IP address of the primary NTP server.
 - **Secondary Server IP Address:** The IP address of the secondary NTP server. If the primary NTP server is not available, the NetHorizon will use the secondary server.
 - **Local Time Zone:** the time zone the device is operating in.
 - **Daylight Savings Time in Effect:** whether daylight savings time is in effect.
- 4 Click **Modify**, then **Close**.

See also:

[Configuring a clock source on page 139](#)

[Viewing clock source status on page 140](#)

Changing VCL rates

The **Modify VCL Rates** dialog box defines the allowable values for the PCR and SCR for certain traffic types. The values in this profile are used as follows:

- The SCR for rt-VBR traffic descriptors must use one of the first 16 rates.
- The PCR for CBR traffic descriptors can use any of the 32 rates.

- For a UBR traffic descriptor, if the **Usage Parameter Control** setting in an ATM traffic descriptor is not enabled, or if PCR is greater than modem trained rate, then the UBR traffic is shaped to one of the 32 rates. The shaper will pick a rate that is equal to or less than the modem trained rate. If there are multiple rates less than the modem trained rate, the one closest to the trained rate will be selected.



Note: The number of rates supported differ depending on the device.



Caution: Changing the VCL Rate values requires a system reboot.

Note the following about the values in this profile:

- Rates are in cells per second (CPS)
- Duplicate rates are not permitted
- Rates must be in ascending order within the first 16 rates and also within the second 16 rates.

To change VCL rates:

- 1 Right-click a device and select **Modify VCL Rates**.
The **Modify VCL Rates** dialog box appears.
- 2 Modify the rates as desired.
- 3 When finished, click **Modify**.
NetHorizon will reboot the device to change the rates.
- 4 Click **Close**.

Related topics:

[Adding ATM cross connect on MALC, and Raptor using the wizard on page 364](#)

[Adding ATM cross connect on MALC, and Raptor \(advanced mode\) on page 366](#)

[Adding an ATM cross connect \(VP switched connection\) on page 369](#)

[Creating ATM cross connect configuration templates on page 362](#)

[Creating ATM traffic descriptor configuration templates on page 361](#)

[Creating an ATM VCL for data on page 372](#)

[Creating an ATM VPL on page 373](#)

[Creating an ATM VPI profile on page 143](#)

[Finding ATM VCLs and cross connects on page 461](#)

[Pinging ATM VCL endpoints on page 462](#)

Creating an ATM VPI profile

ATM VPI profiles define VPI/VCI ranges for ATM-capable cards as well as whether the VPI is used for VP- or VC-switched connections. Adding an ATM VPI profile requires a system reboot.

To create an ATM VPI:



Note: It is recommended that all VPI provisioning be completed immediately after adding the card to reduce the number of system reboots.

- 1 Navigate to the port you want to create an VPI profile on.
For DS3 fanouts, create an VPI on the uplink port and the desired DS3 port. To create the DS3 fanout cross connects, see [Adding ATM cross connect on MALC, and Raptor \(advanced mode\) on page 366](#).
- 2 Expand the tree view to display the **ATM Logical** label.
- 3 Right-click the **ATM VPI Profile** label and select **Add**.
- 4 The **Add ATM VPI Profile Configuration** dialog box appears.
- 5 Specify the following:
(Optional). Specify a name.
Specify whether this VPI is going to be used for VC-, VP-switched, or voice gateway connections. For DS3 fanout VPIs, use the Switch Type VC-VP Terminated.
Specify the VPI for the VPL.
Maximum VC: Specify the maximum VPI to use for this port. For a switched VP, this value must be 0. For a switched VC, this value must be a power of 2 greater than or equal to 64.
- 6 Click **Add**.
Adding a VPI profile requires the card to be rebooted before any further ATM provisioning will be allowed on that card. Note that if you are adding a VPI profile to a MALC or Raptor Uplink card, the entire system will be rebooted.
- 7 At the reboot confirmation dialog box, click **Yes**.
NetHorizon creates the VPI and reboots the card.
- 8 Click **Close**.

Related topics:

[Adding ATM cross connect on MALC, and Raptor using the wizard on page 364](#)

[Adding an ATM cross connect \(VP switched connection\) on page 369](#)

[Adding an ATM cross connect \(VC switched connection\) on page 369](#)

[Changing VCL rates on page 141](#)

[Creating ATM cross connect configuration templates on page 362](#)
[Creating ATM traffic descriptor configuration templates on page 361](#)
[Creating an ATM VCL for data on page 372](#)
[Creating an ATM VPL on page 373](#)
[Finding ATM VCLs and cross connects on page 461](#)
[Pinging ATM VCL endpoints on page 462](#)

Modifying a card's ATM bandwidth settings

For some ATM cards, such as the MALC or Raptor Uplink cards, you must specify the amount of bandwidth devoted to each ATM service category. (This does not apply to DSL cards.)

Note that changing the bandwidth allocation reboots the card and in the case of non-redundant Uplink cards, the entire device.

To change the ATM bandwidth allocation:

- 1 From the tree view, right-click an ATM card such as a MALC Uplink card and select **Modify**.

The **Card Configuration** dialog box appears.

- 2 In the **ATM Configuration** list box, select the ATM configuration.

For details on the settings, see the online help.

- 3 Click **Modify**, then **Close**.

- 4 Reboot the card by selecting **Card > Reboot Card**.

Reboot the card by right-clicking the card and selecting **Reboot Card**.

Related topics:

[Adding a single card on page 131](#)
[Adding multiple cards on page 132](#)
[Adding ATM cross connect on MALC, and Raptor using the wizard on page 364](#)
[Adding an ATM cross connect \(VP switched connection\) on page 369](#)
[Adding an ATM cross connect \(VP switched connection\) on page 369](#)
[Changing VCL rates on page 141](#)
[Creating ATM cross connect configuration templates on page 362](#)
[Creating ATM traffic descriptor configuration templates on page 361](#)
[Creating an ATM VCL for data on page 372](#)
[Creating an ATM VPL on page 373](#)
[Pinging ATM VCL endpoints on page 462](#)

Modifying GigaMux 1600/3200 card configurations

Card configurations for GigaMux 1600/3200 modules can be modified from ZMS.

To modify a card configurations

- 1 Select the desired GigaMux card in the ZMS tree.
- 2 From the right-click menu, select **Modify**.

The **Modify [card] Configuration** dialog appears with quick options for hardware, configuration, status, runtime, and software. This example shows the dialog for the OCM module.

When viewing cards, options are view-only and cannot be modified. Click **Close** to exit the dialog box.

- 3 For configuration options, click **Configuration**. The configuration options appear. For module parameter options, click **Card Parameters**. The module parameter options appear. For connection parameter options, click **Connection Parameters**. The connection parameter options appear.

After completing the software changes, click **Modify** to apply the changes. Click **Reset** to return to the default settings. Click **Refresh** to update the displayed settings. Click **Close** to exit the dialog box.

Redundant card configuration settings

To configure card redundancy, click the **Redundant Cards** category in the configuration dialog box in the tree view. From here, you can configure the card redundancy.



Note: The actual parameters you can configure for card redundancy depend on the type and the release version of the device on which the card resides.

See also:

For details on the settings, see the online help.

Modifying EFM SHDSL card configurations

Card configurations for the MALC-EFM-SHDSL-24, MALC-EFM-SHDSL-24 NTWC and the MALC-EFM-SHDSL-24-NTP cards can be modified from ZMS.

To modify a G.SHDSL-24 card configurations

- 1 Select the G.SHDSL-24 card in the ZMS tree.
- 2 From the right-click menu, select **Modify**.

The **Modify G.SHDSL Card Configuration** dialog appears with quick options for hardware, configuration, status, runtime, and software.

When viewing Hardware Information, Status, and Runtime, options are view-only and cannot be modified. Click **Close** to exit the dialog box.

- 3 For configuration options, click **Configuration**. The configuration options appear. For software options, click **Software**. The software parameter options appear.

After completing the software changes, click **Modify** to apply the changes. Click **Reset** to return to the default settings. Click **Refresh** to update the displayed settings. Click **Close** to exit the dialog box.

Wetting current settings

Wetting current feature is only apply to MALC-EFM-SHDSL-24-NTWC card. By default, the wetting current parameter is disabled. Wetting current provides 10-15mA per G.SHDSL line. To enable wetting current, select the **Standard** option.



Note: Enabling wetting current from ZMS causes the card to reboot.

See also:

For details on the settings, see the online help.

Port status

Topics:

[Configuring port status](#)

Configuring port status

NetHorizon supports port status and configuration for all ports on a card through the Port Status dialog.

- 1 Right-click the desired card and select, **Configure Port Status**.

The **Port Status** dialog box appears with a list of all the ports on the card along with port type, name, administrative status, operation status, UpTrainRate, DownTrainRate, UpAttainTrainRate, and DownAttainTrainRate.

Click **Close** to exit the dialog.

- 2 To modify or view a port, select the desired port and click **Modify/View**. The Modify/View Physical Ports dialog appears.
- 3 Specify the desired changes.
- 4 After finishing the configuration or status, click **Close**. The Port Status dialog appears. Click **Close** to exit the dialog.

See also:

[Applying physical port templates to a port on page 160](#)

[Creating ADSL Alarm templates on page 152](#)

[Creating ADSL Configuration templates on page 152](#)

- 5 To change the administration status, in the **Port Status** dialog box, select the desired port and click **Admin Up** or click **Admin Down**.
- 6 After finishing the configuration, click **Close** to exit the Port Status dialog.

Port configuration

Topics:

[Physical port templates](#)

[Changing administration status of ports](#)

[Subscriber ID/ Port description](#)

[Configuring ULC card physical ports](#)

[Configuring Uplink-OC3C/STM1-ATM/IP card physical ports](#)

[Configuring OC12 Uplink card physical ports](#)

[Configuring BPON OLT card physical ports](#)

[Configuring BPON ONT/ONU](#)

[Configuring 4-wire SHDSL card physical ports](#)

[Configuring ADSL card physical port](#)

[Configuring VDSL physical ports](#)

[Configuring T1/E1 physical ports](#)

[Configuring G.SHDSL physical ports](#)

[Viewing EtherXtender Performance Statistics](#)

[Configuring Malc XP/ Raptor XP physical ports](#)

[Configuring Link aggregation and LACP](#)

[Ethernet redundancy](#)

[Concurrent uplinks on the MXK 2.2.x](#)

[Settable alarm severity for Ethernet ports](#)

[Bond groups](#)

[Configuring RPR ports](#)

[Configuring GigaMux ports](#)

[Configuring Talk Battery Disconnect on the POTS port](#)

- Configure GPON OLT ports
- Configure GPON ONU/ONT
- Activate ONT/ONUs by assigning serial number
- GPON OMCI configuration
- Configure GPON ONT/ONU GEM Ports
- Enable ONT/ONU web interface
- View SFP presence

Physical port templates

Topics:

- Creating DSL port templates
- Creating DSL alarm profile templates
- Creating HDSL2 config profile templates
- Creating SDSL port templates
- Creating SHDSL port templates
- Creating ADSL port templates
- Creating ADSL Alarm templates
- Creating ADSL Configuration templates
- Creating POTS physical templates
- Creating POTS FXS config templates
- Creating EBS physical templates
- Creating ISDN Bri physical port templates
- Creating ISDN Bri alarm profile templates
- Creating ISDN Bri Ulc configuration templates
- Creating T1 physical templates
- Creating E1 physical port templates
- Creating T1 ATM physical port templates
- Creating E1 ATM physical port templates
- Creating E1 ATM physical port templates
- Creating VDSL physical port templates
- Creating VDSL alarm profile templates
- Creating VDSL configuration profile templates
- Applying physical port templates to a port

Creating DSL port templates

- 1** Select **Tools > Configure Templates**.
The **Template Configuration** dialog box appears.
- 2** Expand **Physical Port Templates (For Modify)**.
- 3** Expand **DSL Templates**.
- 4** Right click **Port Templates** and select **Add**.
The **Add DSL Port Configuration** dialog box appears.
- 5** Enter a name and a description for this template.
The name appears in the selection dialog boxes.
- 6** Configure the settings for the port.
For details on the settings, see the online help.
- 7** After finishing the configuration, click **Add**, then **Close**.
After adding the template, it will appear in the **Template Configuration** dialog box.

See also:

[Applying physical port templates to a port on page 160](#)

[Creating DSL alarm profile templates on page 149](#)

Creating DSL alarm profile templates

- 1** Select **Tools > Configure Templates**.
The **Template Configuration** dialog box appears.
- 2** Expand **Physical Port Templates (For Modify)**.
- 3** Expand **DSL Templates**.
- 4** Right click **Alarm Profile Templates** and select **Add**.
The **Add Alarm Profile Configuration** dialog box appears.
- 5** Enter a name and a description for this template.
The name appears in the selection dialog boxes.
- 6** Configure the settings for the port.
For details on the settings, see the online help.
- 7** After finishing the configuration, click **Add**, then **Close**.
After adding the template, it will appear in the **Template Configuration** dialog box.

See also:

[Applying physical port templates to a port on page 160](#)

[Creating DSL port templates on page 149](#)

Creating HDSL2 config profile templates

- 1 Select **Tools > Configure Templates**.

The **Template Configuration** dialog box appears.

- 2 Expand **Physical Port Templates (For Modify)**.

- 3 Expand **DSL Templates**.

- 4 Right click **Hdsl2 Config Profile Templates** and select **Add**.

The **Add Hdsl2 Config Profile Configuration** dialog box appears.

- 5 Enter a name and a description for this template.

The name appears in the selection dialog boxes.

- 6 Configure the settings for the port.

For details on the settings, see the online help.

- 7 After finishing the configuration, click **Add**, then **Close**.

After adding the template, it will appear in the **Template Configuration** dialog box.

See also:

[Applying physical port templates to a port on page 160](#)

[Creating ADSL Alarm templates on page 152](#)

[Creating ADSL Configuration templates on page 152](#)

Creating SDSL port templates

- 1 Select **Tools > Configure Templates**.

The **Template Configuration** dialog box appears.

- 2 Expand **Physical Port Templates (For Modify)**.

- 3 Expand **DSL Templates**.

- 4 Right click **SDSL Config Profile Templates** and select **Add**.

The **Add SDSL Config Profile Configuration** dialog box appears.

- 5 Enter a name and a description for this template.

The name appears in the selection dialog boxes.

- 6 Configure the settings for the port.

For details on the settings, see the online help.

- 7 After finishing the configuration, click **Add**, then **Close**.

After adding the template, it will appear in the **Template Configuration** dialog box.

See also:

[Applying physical port templates to a port on page 160](#)

[Creating ADSL Alarm templates on page 152](#)

[Creating ADSL Configuration templates on page 152](#)

Creating SHDSL port templates

- 1 Select **Tools > Configure Templates**.
The **Template Configuration** dialog box appears.
- 2 Expand **Physical Port Templates (For Modify)**.
- 3 Expand **DSL Templates**.
- 4 Right click **SHDSL Config Profile Templates** and select **Add**.
The **SHDSL Config Profile** dialog box appears.
- 5 Enter a name and a description for this template.
The name appears in the selection dialog boxes.
- 6 Configure the settings for the port.
For details on the settings, see the online help.
- 7 After finishing the configuration, click **Add**, then **Close**.
After adding the template, it will appear in the **Template Configuration** dialog box.

See also:

[Applying physical port templates to a port on page 160](#)

[Creating ADSL Alarm templates on page 152](#)

[Creating ADSL Configuration templates on page 152](#)

[Creating SDSL port templates on page 150](#)

Creating ADSL port templates

- 1 Select **Tools > Configure Templates**.
The **Template Configuration** dialog box appears.
- 2 Expand **Physical Port Templates (For Modify)**.
- 3 Expand **ADSL Templates**.
- 4 Right click **ADSL Port Configuration** and select **Add**.
The **Add ADSL Port Configuration** dialog box appears.
- 5 Enter a name and a description for this template.
The name appears in the selection dialog boxes.
- 6 Configure the settings for the port.
For details on the settings, see the online help.
- 7 After finishing the configuration, click **Add**, then **Close**.

After adding the template, it will appear in the **Template Configuration** dialog box.

See also:

[Applying physical port templates to a port on page 160](#)

[Creating ADSL Alarm templates on page 152](#)

[Creating ADSL Configuration templates on page 152](#)

Creating ADSL Alarm templates

Alarm profiles enable you to set the thresholds which cause the device to send traps when they are exceeded.

- 1 Select **Tools > Configure Templates**.

The **Template Configuration** dialog box appears.

- 2 Expand **Physical Port Templates (For Modify)**.

- 3 Expand **ADSL Templates**.

- 4 Right click **Alarm Profile Templates** and select **Add**.

The **Add ADSL Alarm Profile** dialog box appears.

- 5 Enter a name and a description for this template.

The name appears in the selection dialog boxes.

- 6 You can configure the alarm thresholds for both the CO and CPE devices.

For details on the settings, see the online help.

- 7 After finishing the configuration, click **Add**, then **Close**.

After adding the template, it will appear in the **Template Configuration** dialog box.

See also:

[Applying physical port templates to a port on page 160](#)

[Creating ADSL Configuration templates on page 152](#)

[Creating SHDSL port templates on page 151](#)

Creating ADSL Configuration templates

ADSL configuration templates set defaults for upstream and downstream ADSL templates.

- 1 Select **Tools > Configure Templates**.

The **Template Configuration** dialog box appears.

- 2 Expand **Physical Port Templates (For Modify)**.

- 3 Expand **ADSL Templates**.

- 4 Right click **Config Profile Templates** and select **Add**.

The **Add ADSL Port Configuration** dialog box appears.

- 5 Enter a name and a description for this template.

The name appears in the selection dialog boxes.

- 6 To configure the upstream interface, click the **Central Office Unit** tab.

To configure the downstream interface, click the **Customer Premise Unit** tab.

For details on the settings, see the online help.

[Single-End Loop Test \(SELT\) on page 472](#)

[Dual-End Loop Test \(DELT\) on page 473](#)

- 7 After finishing the configuration, click **Add**, then **Close**.

After adding the template, it will appear in the **Template Configuration** dialog box.

See also:

[Applying physical port templates to a port on page 160](#)

[Creating ADSL Alarm templates on page 152](#)

[Creating SHDSL port templates on page 151](#)

[Configuring ADSL card physical port on page 163](#)

Creating POTS physical templates

- 1 Select **Tools > Configure Templates**.

The **Template Configuration** dialog box appears.

- 2 Expand **Physical Port Templates (For Modify)**.

- 3 Expand **POTS Templates**.

- 4 Right click **POTS Physical Templates** and select **Add**.

The **Add Pots Physical Port Configuration** dialog box appears.

- 5 Enter a name and a description for this template.

The name appears in the selection dialog boxes.

- 6 Configure the settings for the port.

For details on the settings, see the online help.

- 7 After finishing the configuration, click **Add**, then **Close**.

After adding the template, it will appear in the **Template Configuration** dialog box.

See also:

[Applying physical port templates to a port on page 160](#)

Creating POTS FXS config templates

- 1 Select **Tools > Configure Templates**.
The **Template Configuration** dialog box appears.
- 2 Expand **Physical Port Templates (For Modify)**.
- 3 Expand **POTS Templates**.
- 4 Right click **POTS FXS Config Templates** and select **Add**.
The **Add Pots FXS Port Configuration** dialog box appears.
- 5 Enter a name and a description for this template.
The name appears in the selection dialog boxes.
- 6 Configure the settings for the port.
For details on the settings, see the online help.
- 7 After finishing the configuration, click **Add**, then **Close**.
After adding the template, it will appear in the **Template Configuration** dialog box.

See also:

[Applying physical port templates to a port on page 160](#)

Creating EBS physical templates

- 1 Select **Tools > Configure Templates**.
The **Template Configuration** dialog box appears.
- 2 Expand **Physical Port Templates (For Modify)**.
- 3 Expand **EBS Templates**.
- 4 Right click **EBS Physical Templates** and select **Add**.
The **Add Ebs Physical Port Configuration** dialog box appears.
- 5 Enter a name and a description for this template.
The name appears in the selection dialog boxes.
- 6 Configure the settings for the port.
For details on the settings, see the online help.
- 7 After finishing the configuration, click **Add**, then **Close**.
After adding the template, it will appear in the **Template Configuration** dialog box.

See also:

[Applying physical port templates to a port on page 160](#)

Creating ISDN Bri physical port templates

- 1 Select **Tools > Configure Templates**.

The **Template Configuration** dialog box appears.

- 2 Expand **Physical Port Templates (For Modify)**.

- 3 Expand **ISDN Bri Templates**.

- 4 Right click **Port Templates** and select **Add**.

The **Add ISDN BRI Physical Port Configuration** dialog box appears.

- 5 Enter a name and a description for this template.

The name appears in the selection dialog boxes.

- 6 Configure the settings for the port.

For details on the settings, see the online help.

- 7 After finishing the configuration, click **Add**, then **Close**.

After adding the template, it will appear in the **Template Configuration** dialog box.

See also:

[Applying physical port templates to a port on page 160](#)

Creating ISDN Bri alarm profile templates

- 1 Select **Tools > Configure Templates**.

The **Template Configuration** dialog box appears.

- 2 Expand **Physical Port Templates (For Modify)**.

- 3 Expand **ISDN Bri Templates**.

- 4 Right click **Alarm Profile Templates** and select **Add**.

The **Add ISDN BRI Physical Port Configuration** dialog box appears.

- 5 Enter a name and a description for this template.

The name appears in the selection dialog boxes.

- 6 Configure the settings for the port.

For details on the settings, see the online help.

- 7 After finishing the configuration, click **Add**, then **Close**.

After adding the template, it will appear in the **Template Configuration** dialog box.

See also:

[Applying physical port templates to a port on page 160](#)

Creating ISDN Bri Ulc configuration templates

- 1 Select **Tools > Configure Templates**.

The **Template Configuration** dialog box appears.

- 2 Expand **Physical Port Templates (For Modify)**.

- 3 Expand **ISDN Bri Templates**.

- 4 Right click **Ulc Configuration Templates** and select **Add**.

The **Add ISDN BRI Physical Port Configuration** dialog box appears.

- 5 Enter a name and a description for this template.

The name appears in the selection dialog boxes.

- 6 Configure the settings for the port.

For details on the settings, see the online help.

- 7 After finishing the configuration, click **Add**, then **Close**.

After adding the template, it will appear in the **Template Configuration** dialog box.

See also:

[Applying physical port templates to a port on page 160](#)

Creating T1 physical templates

- 1 Select **Tools > Configure Templates**.

The **Template Configuration** dialog box appears.

- 2 Expand **Physical Port Templates (For Modify)**.

- 3 Expand **DS1 Templates**.

- 4 Right click **T1 Physical Templates** and select **Add**.

The **Add T1 Physical Port Configuration** dialog box appears.

- 5 Enter a name and a description for this template.

The name appears in the selection dialog boxes.

- 6 Configure the settings for the port.

For details on the settings, see the online help.

- 7 After finishing the configuration, click **Add**, then **Close**.

After adding the template, it will appear in the **Template Configuration** dialog box.

See also:

[Applying physical port templates to a port on page 160](#)

Creating E1 physical port templates

- 1 Select **Tools > Configure Templates**.

The **Template Configuration** dialog box appears.

- 2 Expand **Physical Port Templates (For Modify)**.

- 3 Expand **DS1 Templates**.

- 4 Right click **E1 Physical Templates** and select **Add**.

The **Add E1 Physical Port Configuration** dialog box appears.

- 5 Enter a name and a description for this template.

The name appears in the selection dialog boxes.

- 6 Configure the settings for the port.

For details on the settings, see the online help.

- 7 After finishing the configuration, click **Add**, then **Close**.

After adding the template, it will appear in the **Template Configuration** dialog box.

See also:

[Applying physical port templates to a port on page 160](#)

Creating T1 ATM physical port templates

- 1 Select **Tools > Configure Templates**.

The **Template Configuration** dialog box appears.

- 2 Expand **Physical Port Templates (For Modify)**.

- 3 Expand **DS1 Templates**.

- 4 Right click **T1 ATM Physical Templates** and select **Add**.

The **Add ATM T1 Physical Port Configuration** dialog box appears.

- 5 Enter a name and a description for this template.

The name appears in the selection dialog boxes.

- 6 Configure the settings for the port.

For details on the settings, see the online help.

- 7 After finishing the configuration, click **Add**, then **Close**.

After adding the template, it will appear in the **Template Configuration** dialog box.

See also:

[Applying physical port templates to a port on page 160](#)

Creating E1 ATM physical port templates

- 1 Select **Tools > Configure Templates**.

The **Template Configuration** dialog box appears.

- 2 Expand **Physical Port Templates (For Modify)**.

- 3 Expand **DS1 Templates**.

- 4 Right click **E1 ATM Physical Templates** and select **Add**.

The **Add ATM E1 Physical Port Configuration** dialog box appears.

- 5 Enter a name and a description for this template.

The name appears in the selection dialog boxes.

- 6 Configure the settings for the port.

For details on the settings, see the online help.

- 7 After finishing the configuration, click **Add**, then **Close**.

After adding the template, it will appear in the **Template Configuration** dialog box.

See also:

[Applying physical port templates to a port on page 160](#)

Creating VDSL physical port templates

- 1 Select **Tools > Configure Templates**.

The **Template Configuration** dialog box appears.

- 2 Expand **Physical Port Templates (For Modify)**.

- 3 Expand **VDSL Templates**.

- 4 Right click **VDSL Port Templates** and select **Add**.

The **Add VDSL Port Configuration** dialog box appears.

- 5 Enter a name and a description for this template.

The name appears in the selection dialog boxes.

- 6 Configure the settings for the port.

For details on the settings, see the online help.

- 7 After finishing the configuration, click **Add**, then **Close**.

After adding the template, it will appear in the **Template Configuration** dialog box.

See also:

[Applying physical port templates to a port on page 160](#)

Creating VDSL alarm profile templates

- 1 Select **Tools > Configure Templates**.
The **Template Configuration** dialog box appears.
- 2 Expand **Physical Port Templates (For Modify)**.
- 3 Expand **VDSL Templates**.
- 4 Right click **VDSL Alarm Profile Templates** and select **Add**.
The **Add VDSL Port Configuration** dialog box appears.
- 5 Enter a name and a description for this template.
The name appears in the selection dialog boxes.
- 6 Configure the settings for the port.
For details on the settings, see the online help.
- 7 After finishing the configuration, click **Add**, then **Close**.
After adding the template, it will appear in the **Template Configuration** dialog box.

See also:

[Applying physical port templates to a port on page 160](#)

Creating VDSL configuration profile templates

- 1 Select **Tools > Configure Templates**.
The **Template Configuration** dialog box appears.
- 2 Expand **Physical Port Templates (For Modify)**.
- 3 Expand **VDSL Templates**.
- 4 Right click **VDSL Config Profile Templates** and select **Add**.
The **Add VDSL Port Configuration** dialog box appears.
- 5 Enter a name and a description for this template.
The name appears in the selection dialog boxes.
- 6 Configure the settings for the port.
For details on the settings, see the online help.
- 7 After finishing the configuration, click **Add**, then **Close**.
After adding the template, it will appear in the **Template Configuration** dialog box.

See also:

[Applying physical port templates to a port on page 160](#)

Applying physical port templates to a port

To apply physical port templates to a port:

- 1 Select the objects you want to modify.
Hold down the CONTROL or SHIFT keys to select multiple objects.
- 2 Right-click and select **Modify**.
In the **Template Selection** dialog box, select the template you want to apply to the selected devices.
- 3 In the configuration dialog box that appears, modify the settings as required.
- 4 Click **Modify**, then **Close**.

[Configuring ULC card physical ports on page 162](#)

[Configuring Uplink-OC3C/STM1-ATM/IP card physical ports on page 162](#)

[Configuring OC12 Uplink card physical ports on page 162](#)

[Configuring BPON OLT card physical ports on page 162](#)

[Configuring BPON ONT/ONU on page 163](#)

[Configuring 4-wire SHDSL card physical ports on page 163](#)

[Configuring VDSL physical ports on page 171](#)

[Configuring RPR ports on page 200](#)

See also:

[Creating ADSL Alarm templates on page 152](#)

[Creating ADSL Configuration templates on page 152](#)

[Creating SHDSL port templates on page 151](#)

Changing administration status of ports

ZMS users can change the admin status of ports if they have the following provisioning permissions:

- ZMS users with Port Admin Status Provisioning set to Write and Equipment Provisioning set to Read, can view the admin status of **all** ports, and change the admin status of the **line card** ports.
- If ZMS users with both Port Admin Status Provisioning and Equipment Provisioning set to Write, **or** if they with only Equipment Provisioning set to Write, they can view and change admin status of **all** ports (i.e. both uplink card ports and line card ports).

Refer to the **ZMS Administrator's Guide** for the detail permission settings.

Users can change ports admin status from the port level or slot level:

- 1 To change the admin status of the ports at port level, you can use the **Change Administration Status** dialog.
 - a In the ZMS tree view, select one port or use shift key to select multiple ports.
 - b Right-click on ports, then select **Change Admin Status**.
The **Change Administration Status** dialog appears.
 - c In the **Change Administration Status** dialog, select Up, Down, or Testing from the **Admin Status** drop-down menu.
- 2 To change the admin status of the ports from the slot level, you can use the **Configure Ports** dialog.
 - a In the ZMS tree view, right-click a slot.
 - b Select **Configure Port Status**.
The **Configure Ports** dialog appears.
 - c In the **Configure Ports** dialog, select one port or use shift key to select multiple ports.
 - d Click **Admin Up** or **Admin Down** button to change the admin status of ports.
For single port, you can also click **Modify** button in the **Configure Ports** dialog to access the **Modify Port Configuration** dialog, then change the admin status in the **Admin Status** field in the **Configuration / Status** window of this dialog.

Subscriber ID/ Port description

The ZMS has a description field for a physical. This field is in the View/Modify dialogs for all physical types.

This value is stored in ZMS, and can be config sync with the device.

Modifying description field

- 1 To modify the description field, right-click a physical and click **Modify**.
The **Modify Physical Port Configuration** window appears.
- 2 In the Identity dialog, you can modify the Description field. At last click **Modify** to confirm the change.
- 3 The description field can contain up to 64 characters. If the field is not long enough to show the full description, click “...” button to view or modify the description.
Click the “...” button. A text editor dialog for the description field pops up:
- 4 Modify the description in the text editor dialog, and click **OK**.



Note: In order to avoid the new description value to overwrite the existing value in the device by the config sync process, the user can set the useDevicePortDescription attribute to “false” in the *CSS.properties*. In that case, the new description will only be stored in ZMS, not on the device.

Configuring ULC card physical ports

- 1 From the tree view, expand the ULC card and then expand the physical interfaces.
- 2 Right-click a physical interface and select **Modify**. The **Modify ISDN BRI Physical Port Configuration** dialog box appears.
- 3 Select **ULC Configuration** from the tree display. The **ULC Configuration** dialog box appears.
- 4 Select **Enable** to enable traps. Or de-select **Enable** to disable traps.
- 5 Click **Modify** then **Close**.

Configuring Uplink-OC3C/STM1-ATM/IP card physical ports

- 1 From the tree view, expand the MALC device and expand Cards.
- 2 Right-click on a Uplink-OC3C/STM1-ATM/IP card and select **Modify**. The **Modify OC3F Uplink Card Configuration** dialog box appears.
- 3 Ensure the software load and ATM configuration settings are appropriate for your Uplink-OC3C/STM1-ATM/IP card.

For details on the settings, see the online help.

Configuring OC12 Uplink card physical ports

- 1 From the tree view, expand the MALC device and expand Cards.
- 2 Right-click on a OC12 GigE Uplink card and select **Modify**. The **Modify OC12 GIGE Uplink Card Configuration** dialog box appears.
- 3 Ensure the software load and ATM configuration settings are appropriate for your OC12 GigE Uplink card.

For details on the settings, see the online help.

Configuring BPON OLT card physical ports

- 1 From the tree view, expand the BPON OLT card and then expand the physical interfaces.
- 2 Right-click a OLT physical interface and select **Modify**. The **Modify OLT Physical Configuration** dialog box appears.
- 3 Configure the settings for the OLT physical ports.

For details on the settings, see the online help.

Configuring BPON OLT/ONU

- 1 From the tree view, expand the BPON OLT card and then expand the physical interfaces.
- 2 Right-click a OLT OLT/ONU physical interface and select **Modify**. The **Modify OltOnu Physical Configuration** dialog box appears.
- 3 Configure the settings for the OLT OLT/ONU interfaces.
For details on the settings, see the online help.

Configuring 4-wire SHDSL card physical ports

- 1 From the tree view, expand the SHDSL 4-Wire card and then expand the physical interfaces.
- 2 Right-click a SHDSL 4-Wire physical interface and select **Modify**. The **Modify G.SHDSL 4-Wire-12 Physical Configuration** dialog box appears.
- 3 Configure the settings for the 4-wire SHDSL physical ports.
For details on the settings, see the online help.

Configuring ADSL card physical port

- [Modifying ADSL Port Configuration on page 163](#)
- [Modifying ADSL2+ Phy-R™ parameters on page 167](#)
- [Modifying ADSL2+ Cabinet mode on page 169](#)

Modifying ADSL Port Configuration

ADSL port configurations can be modified from ZMS.

To modify ADSL port configurations:

- 1 Select the desired ADSL physical port in the ZMS tree.
- 2 From the right-click menu, select **Modify**.
The **Modify ADSL Port Configuration** dialog appears with quick configuration options.
- 3 Select the desired options to change.
The following options appear:
 - Admin Status
 - Name
 - Description
 - Line Status Change Traps

By default, these traps are disabled.

After completing the configuration changes, click **Modify** to apply the changes. Click **Close** to exit the dialog box.

- 4 In the Tree display, click **Status**.

The **Modify ADSL Port Configuration** dialog appears with status options.

- 5 Select the desired options to change.

The following options appear:

- Admin Status
- Oper Status
- State

After completing the configuration changes, click **Modify** to apply the changes. Click **Close** to exit the dialog box.

- 6 In the Tree display, click **Identity**.

The **Modify ADSL Port Configuration** dialog appears with ID options.

- 7 Select the desired options to change.

The following options appear:

- Name
- Description
- IfIndex
- Type

After completing the configuration changes, click **Modify** to apply the changes. Click **Close** to exit the dialog box.

- 8 In the Tree display, click **Administration**.

The **Modify ADSL Port Configuration** dialog appears with admin options.

- 9 Select the desired options to change.

The following options appear:

- NTR Mode Enabled
- Transmission Mode
- Channel Mode
- Trellis Mode
- Maximum Tx PSD on Downstream
- Annex M Mode Enabled
- Annex J Mode Enabled

This field is only displayed if the card is a 72 port ADSL card. The **Annex J Mode Enabled** field may only be set to True if the **Annex M Mode Enabled** field is False and the **Transmission Mode** field is AutoNegotiation, Adsl2, or Adsl2Plus.

- Min Downstream Tone Index (32-255)
- Max Downstream Tone Index (32-255)
- Min Upstream Tone Index (6-30)
- Max Upstream Tone Index (6-30)
- Line Status Change Traps
- Admin Up Line Alarms

After completing the configuration changes, click **Modify** to apply the changes. Click **Close** to exit the box.

10 In the Tree display, click **CO Status**.

The **Modify ADSL Port Configuration** dialog appears with CO status options.

11 Select the desired options to change.

The following options appear:

- CO Status Statistics
- ATUC Current Status Statistics

After completing the configuration changes, click **Modify** to apply the changes. Click **Close** to exit the dialog box.

12 In the Tree display, click **CPE Status**.

The **Modify ADSL Port Configuration** dialog appears with CPE status options.

13 Select the desired options to change.

The following options appear:

- CPE Status Statistics
- ATUR Current Statistics

After completing the configuration changes, click **Modify** to apply the changes. Click **Close** to exit the dialog box.

14 In the Tree display, click **Alarm Profile -Central Office Unit**.

The **Modify ADSL Port Configuration** dialog appears with alarm profile Central Office unit configuration options.

15 Select the desired options to change.

The options appear Central Office Unit statistics.

After completing the configuration changes, click **Modify** to apply the changes. Click **Close** to exit the dialog box.

- 16** In the Tree display, click **Alarm Profile - Customer Premise Unit**.

The **Modify ADSL Port Configuration** dialog appears with alarm profile Customer Premise unit configuration options.

- 17** Select the desired options to change.

The options appear for Customer Premise Unit Statistics.

After completing the configuration changes, click **Modify** to apply the changes. Click **Close** to exit the dialog box.

- 18** In the Tree display, click **Central Office Unit - Transmission Rate**.

The **Modify ADSL Port Configuration** dialog appears with Central Office transmission rate configuration options.

- 19** Select the desired options to change, different device and cards might show different options. Click **Help** to find detail description for each parameter.

After completing the configuration changes, click **Modify** to apply the changes. Click **Close** to exit the dialog box.

- 20** In the Tree display, click **Central Office - Signal Noise**.

The **Modify ADSL Port Configuration** dialog appears with Central Office signal noise configuration options.

- 21** Select the desired options to change.

The following options appear:

- Signal/ Noise Margin for Rate Upshift (0...310)
- Signal/ Noise Margin for Rate Downshift (0...310)
- Max Acceptable Signal/Noise Margin (0...310)
- Min Acceptable Signal/Noise Margin (0...310)
- Target Signal/Noise Margin (0...310)
- Min Upshift Time (0...16383)
- Max Upshift Time (0...16383)

After completing the configuration changes, click **Modify** to apply the changes. Click **Close** to exit the dialog box.

- 22** In the Tree display, click **Customer Premise - Transmission Rate**.

The **Modify ADSL Port Configuration** dialog appears with Customer Premise transmission rate configuration options.

- 23** Select the desired options to change. Different device and cards might show different options. Click **Help** to find detail description for each parameter.

After completing the configuration changes, click **Modify** to apply the changes. Click **Close** to exit the dialog box.

- 24** In the Tree display, click **Customer Premise - Signal Noise Margin**.

The **Modify ADSL Port Configuration** dialog appears with Customer Premise signal noise configuration options.

25 Select the desired options to change.

The following options appear:

- Signal/ Noise Margin for Rate Upshift (0...310)
- Signal/ Noise Margin for Rate Downshift (0...310)
- Max Acceptable Signal/Noise Margin (0...310)
- Min Acceptable Signal/Noise Margin (0...310)
- Target Signal/Noise Margin (0...310)
- Min Upshift Time (0...16383)
- Max Upshift Time (0...16383)

After completing the configuration changes, click **Modify** to apply the changes. Click **Close** to exit the dialog box.

For details on the settings, see the online help.

See also:

[Applying physical port templates to a port on page 160](#)

[Creating ADSL Alarm templates on page 152](#)

[Single-End Loop Test \(SELT\) on page 472](#)

[Dual-End Loop Test \(DELT\) on page 473](#)

Modifying ADSL2+ Phy-R™ parameters

ZMS supports Phy-R™ parameters in the ADSL2+ CO and CPE profiles.

Follow this procedure to modify Broadcom Phy-R™ parameters in the ADSL2+ CO and CPE profiles:

To modify ADSL2+ Broadcom port configuration, right-click the ADSL port in the ADSL2+ Broadcom card and select **Modify**.

The **Modify ADSL Port Configuration** dialog appears.

Click **Config Profile > Central Office Unit > Transmit Rate** to open the CO Transmit window.

In this window, shows the following Broadcom Phy-R™ parameters and relevant ADSL 2+ parameters in the ADSL 2+ CPE profile:

Max Interleave Delay — This relevant ADSL 2+ parameter (already used in the case of normal interleaving) defines the maximum allowed nominal delay. It is used by the modem to set an upper bound on the allowed receiver retransmission queue size. Since it must be at least equal to the round trip delay, retransmission cannot be activated if the Max Interleave Delay configured is lower than 4ms.

Minimum Impulse Noise Protection (0..1 | 5..160) — This relevant ADSL 2+ parameter (already used in the case of normal interleaving) defines the minimal guaranteed impulse noise protection, provided that the available data bandwidth allowed for retransmissions is not exceeded.

Downstream PHYR — Enable or disable downstream Phy-R™ parameters. By default, it is Disabled.

Maximum Impulse Noise Protection (0..1 | 5..160) — This Phy-R™ parameter defines the maximum number of consecutive retransmissions that may take place and therefore bounds the maximal jitter due to retransmissions. A default value of zero doesn't bound the number of consecutive retransmissions (that will however never exceed the Max Interleave Delay * 4 symbols).

The value range is 0 - 1 and 5 - 160:

0: Specifies no protection.

1: Specifies AUTO configuration which automatically selects the INP value based on configured line rate and configured max-delay.

5 - 160: Specifies the number of symbols in 1/10 increments.

Minimum RS overhead (0..255) — This Phy-R™ parameter allows to force a minimum amount of RS overhead. This can be used to guarantee a given amount of steady state error correction capability. A default of zero doesn't force the use of RS overhead.

The value range is 0 - 255.

Retransmission Ratio (0..255) — This Phy-R™ parameter allows to provision a minimal guaranteed retransmission bandwidth, on top of the minimum rate. In case of the repetitive impulses of known maximal length and periodicity, this parameter can be used to guarantee that the repetitive impulse noise can be corrected. A default of zero doesn't force any extra guaranteed data bandwidth for retransmissions.

The value range is 0 - 255.

Click **Config Profile > Customer Premise Unit > Transmit Rate** to open the CPE Transmit window.

In this window, shows the following Broadcom Phy-R™ parameters and relevant ADSL 2+ parameters in the ADSL 2+ CO profile:

Max Interleave Delay — This relevant ADSL 2+ parameter (already used in the case of normal interleaving) defines the maximum allowed nominal delay. It is used by the modem to set an upper bound on the allowed receiver retransmission queue size. Since it must be at least equal to the round trip delay, retransmission cannot be activated if the Max Interleave Delay configured is lower than 4ms.

Minimum Impulse Noise Protection (0..1 | 5..160) — This relevant ADSL 2+ parameter (already used in the case of normal interleaving) defines the minimal guaranteed impulse noise protection, provided that the available data bandwidth allowed for retransmissions is not exceeded.

Upstream PHYR — Enable or disable upstream Phy-R™ parameters. By default, it is Disabled.

Maximum Impulse Noise Protection (0..1 | 5..160) — This Phy-R™ parameter defines the maximum number of consecutive retransmissions that may take place and therefore bounds the maximal jitter due to retransmissions. A default value of zero doesn't bound the number of consecutive retransmissions (that will however never exceed the Max Interleave Delay * 4 symbols).

The value range is 0 - 1 and 5 - 160:

0: Specifies no protection.

1: Specifies AUTO configuration which automatically selects the INP value based on configured line rate and configured max-delay.

5 - 160: Specifies the number of symbols in 1/10 increments.

Minimum RS overhead (0..255) — This Phy-R™ parameter allows to force a minimum amount of RS overhead. This can be used to guarantee a given amount of steady state error correction capability. A default of zero doesn't force the use of RS overhead.

The value range is 0 - 255.

Retransmission Ratio (0..255) — This Phy-R™ parameter allows to provision a minimal guaranteed retransmission bandwidth, on top of the minimum rate. In case of the repetitive impulses of known maximal length and periodicity, this parameter can be used to guarantee that the repetitive impulse noise can be corrected. A default of zero doesn't force any extra guaranteed data bandwidth for retransmissions.

The value range is 0 - 255.

26 Modify the desired changes.

27 Click **Modify**.

Modifying ADSL2+ Cabinet mode

Cabinet mode is supported on the MXK, MALC, Raptor-XP-150 and MALC-XP-150A, and is normally employed on systems located in outside plant, or street cabinets which share the same binder group as ADSL services originating from the CO. When enabled, the Cabinet Mode feature disables the use of all downstream frequencies below ~1.1MHz.

While Cabinet mode is beneficial in reducing the disturbances on adjacent ADSL services from the CO, it does so by reducing the frequencies available for ADSL services from the MXK, MALC or XP. This reduction of frequencies will diminish the overall rate and reach performance of DSL services from the MXK, MALC or XP. Therefore, this feature should only be used in situations where the MXK, MALC or XP is adversely affecting the performance of ADSL services from the CO, or when mandated by the incumbent carrier in loop unbundling applications.



Note: For cabinet mode operation, the CPE device on the connection must also support the feature and be configured to respond to a shift in frequencies used during link and line training sequences. If the CPE is not able to respond to shifts in frequencies during link and line training sequences it may take a long time (if ever) to establish sync between the CPE and the DSLAM.

Cabinet mode is disabled through the **Cabinet Mode** parameter in the ADSL2+ CO profile, by setting the value to Off.

To modify ADSL2+ cabinet mode configuration, right-click the ADSL port in the device and select **Modify**.

The **Modify ADSL Port Configuration** dialog appears.

28 In the Tree display, click **Central Office Unit > Transmission Rate**.

The **Modify ADSL Port Configuration** dialog appears with the Cabinet Mode option.

29 The **Cabinet Mode** field will accept any filter number in the range from 0-15. Off means the cabinet mode is disabled.

The filter number defines the following cutoff frequency:

- 1: 603.75 khz
- 2: 646.875 khz
- 3: 690 khz
- 4: 733.125 khz
- 5: 776.25 khz
- 6: 819.375 khz
- 7: 862.5 khz
- 8: 905.625 khz
- 9: 948.75 khz
- 10: 991.875 khz
- 11: 1035 khz
- 12: 1078.125 khz
- 13: 1121.25 khz
- 14: 1164.375 khz
- 15: 1207.5 khz

30 Click **Modify**.

Configuring VDSL card physical ports

Configuring VDSL physical ports

- 1 From the tree view, expand the VDSL card and then expand the physical interfaces.
- 2 Right-click a VDSL physical interface and select **Modify**. The **Modify VDSL Physical Configuration** dialog box appears.
- 3 Configure the settings for the VDSL physical ports.
For details on the settings, see the online help.

Enabling G.INP

To enable and configure G.INP parameters in the vdsl-co-config profile and vdsl-cpe-config profile, use the following procedure:

- 1 To enable and configure the G.INP parameters in the **vdsl-co-config** profile, use the **Modify VDSL Port Configuration** window.
In the **Modify VDSL Port Configuration** window tree view, expand **Advanced** level, and then expand **CO Config Profile**, select the **Transmit Rate**.

Table 6: vdsl-co-config profile G.INP support parameter definitions

Parameter	Description
Minium INP	The minimum impulse noise protection for the downstream bearer channel expressed in symbols. One symbol equals 250 uS. No Protection, Half Symbol, Single Symbol, Two Symbols, Three Symbols, Four Symbols, Five Symbols, Six Symbols, Seven Symbols, Eight Symbols, Nine Symbols, Ten Symbols, Eleven Symbols, Twelve Symbols, Thirteen Symbols, Fourteen Symbols, Fifteen Symbols, Sixteen Symbols Default: Two Symbols
PhyR Maximum INP	PHYR maximum downstream impulse noise protection. A value of 0 specifies no protection. The values 5 through 160 specify the number of symbols in 1/10 increments. Default: 0
Downstream GINP Support	Enable or disable downstream G.INP / ITU-G.998.4. Only supported by Broadcom ports. 1 Enabled 2 Disabled

Table 6: vdsl-co-config profile G.INP support parameter definitions (Continued)

Parameter	Description
GINP Maximum Downstream Expected Throughput in Kbps	Maximum allowed value for downstream expected throughput (ETR) in kbit/s. The valid values are all multiples of 8 from 0 to the maximum of the valid values of the maximum net data rate specified in the associated Recommendation. ITU-T G.998.4 7.1.1 Control parameters and 7.1.2 Valid configurations. Default: 100000 kbps
GINP Minimum Downstream Expected Throughput in Kbps	Minimum allowed value for downstream expected throughput (ETR) in kbit/s. The valid values are all multiples of 8 from 0 to the maximum of the valid values of the minimum net data rate specified the associated Recommendation. ITU-T G.998.4 7.1.1 Control parameters and 7.1.2 Valid configurations. Default: 64
GINP Maximum Downstream Net Data Rate (NDR) in Kbps	Maximum allowed value for downstream net data rate (NDR) in kbit/s. The valid values are all multiples of 8 from 0 to the maximum of the valid values of the maximum net data rate specified in the associated Recommendation. ITU-T G.998.4 7.1.1 Control parameters and 7.1.2 Valid configurations. Default: 100000 kbps
GINP Downstream Single High Impulse Noise Event(SHINE) Ratio (0..255)	The downstream loss of rate in a 1 second interval expressed as a fraction of NDR due to a single high impulse noise event (SHINE) impulse noise environment expected by the operator to occur at a pro ginpVdslCpeEtrMin ability acceptable for the services. The valid values are all multiples of 0.001 from 0 to 0.1. This field uses 1 to equal 0.001 and 100 to equal 0.1. ITU-T G.998.4 7.1.1 Control parameters and 7.1.2 Valid configurations. Default: 10
GINP Downstream Low Error Free Rate (LEFTR) Threshold (0..99)	The downstream rate Threshold below which the Low Error Free Rate (LEFTR) defect is declared. The threshold used to declare leftr defects is expressed in fraction of the net data rate (NDR). The value 0 is a special value to indicate that the receiver shall use a special value for declaring leftr defect. The minimum valid threshold to declare leftr is ETR/2. The receiver shall ignore threshold values that are less than the minimum and shall use ETR/2 for declaring leftr defect instead. The valid values are all multiples of 0.01 from 0.01 to 0.99. This field uses 1 to equal 0.01 and 99 to equal 0.99. Default: 0

Table 6: vdsl-co-config profile G.INP support parameter definitions (Continued)

Parameter	Description
GINP Maximum Downstream delay in mSecs	The maximum downstream delay in ms. This is the upper limit for the delay that is added to the transmission delay only caused by retransmissions. Here the receiver and/or the transmitter shall identify and discard all DTUs whose payload cannot be transferred over the reference point at the receiver without violating the delay_max limit. The time stamp shall be the criterion for discarding the DTUs. The processing delay between the U-interface and the retransmission sub-layer of the receiver in the retransmission data path direction shall be excluded from consideration for delay_max in the retransmission data path direction. The valid values are all integers from 1 to 63. ITU-T G.998.4 7.1.1 Control parameters, 7.1.2 Valid configurations, and 8.1.6 Time Stamp. Default: 20 mSecs
GINP Minimum Downstream delay in mSecs	The minimum downstream delay in ms. This is the lower limit for the delay that is added to the transmission delay caused by retransmissions only. The time stamp shall be used by the outlet shaping function to determine when the payload of the DTU shall be sent to the reference point to meet the delay limits. The outlet shaping function shall minimize the additional delay that may be introduced above delay_min, and shall never exceed delay_max. The valid values are all integers from 0 to 63. ITU-T G.998.4 7.1.1 Control parameters, 7.1.2 Valid configurations, and 8.1.6 Time Stamp. Default: 0
GINP Minimum Downstream Impulsive Noise Protection (INP)	The minimum downstream impulse noise protection (INP) against single high impulse noise event (SHINE) in discrete multitone (DMT) symbols. The valid values are all integers from 0 to 63 for system with a sub-carrier spacing of 4.3125 kHz. The valid values are all integers from 0 to 127 for system with a sub-carrier spacing of 8.625 kHz. ITU-T G.998.4 7.1.1 Control parameters and 7.1.2 Valid configurations. Default: 4
GINP Minimum Downstream Bandwidth Reserved for RS (reed-solomon) (0..64)	This value specifies the downstream bandwidth reserved for RS (reed-solomon) codewords. The minimum guaranteed R/N ratio. The unit is 1/256th and the range is 0..64 (0 to 25%). Default: 0
GINP Minimum Downstream Repetitive Impulse Noise (REIN) Configuration	The minimum downstream impulse protection against electrical repetitive impulse noise (REIN) in DMT symbols. The valid values are all integers from 0 to 7 for system with a sub-carrier spacing of 4.3125 kHz. The valid values are all integers from 0 to 13 for system with a sub-carrier spacing of 8.625 kHz. ITU-T G.998.4 7.1.1 Control parameters and 7.1.2 Valid configurations. Default: 0

Table 6: vdsl-co-config profile G.INP support parameter definitions (Continued)

Parameter	Description
GINP Frequency of REIN Inter-Arrival Time in Hz	Specifies the frequency of REIN inter-arrival time. It is used in the Channel Initialization Policy and on-line reconfiguration procedures. REIN is commonly coupled from electrical power cables appliances drawing power from the AC electrical power network, having a repetition rate of twice the AC power frequency (100 or 120 Hz). The valid values are integers 100 hz or 120 hz. ITU-T G.998.4 7.1.1 Control parameters and 7.1.2 Valid configurations. 1 100 2 120 Default: 120
GINP Downstream Retransmission Mode	Downstream retransmission Mode (RTX MODE). The RTX_MODE is a configuration parameter used to control activation of retransmission during initialization. This parameter has 4 valid values: FORBIDDEN: ITU-T G.998.4 retransmission not allowed. PREFERRED: ITU-T G.998.4 retransmission is preferred by the operator. (i.e., if ITU-T G.998.4 RTX capability is supported by both XTU's, the XTU's shall select ITU-T G.998.4 operation for this direction). FORCED: Force the use of the ITU-T G.998.4 retransmission.(i.e., if ITU-T G.998.4 RTX capability in this direction is not supported by both XTU's or not selected by the XTU's, an initialization failure shall result). NOTE: Due to the optionality of ITU-T G.998.4 retransmission in upstream direction, the use of FORCED in upstream may lead to initialization failure, even if the XTU is supporting ITU-T G.998.4 (in downstream). TESTMODE: Force the use of the ITU-T G.998.4 retransmission in the test mode described in clause 10.4. (i.e., if ITU-T G.998.4 RTX capability is not supported by both XTU's or not selected by the XTU's, an initialization failure shall result).ITU-T G.998.4 11.1.13 Retransmission Mode (RTX_MODE). 1 forbidden 2 preferred(default) 3 forced 4 testmode Default: preferred

- 2 To enable and configure the G.INP parameters in the **vdsl-cpe-config** profile, use the **Modify VDSL Port Configuration** window.

In the **Modify VDSL Port Configuration** window tree view, expand **Advanced** level, and then expand **CPE Config Profile**, select the **Transmit Rate**.

Table 7: vdsl-cpe-config profile G.INP support parameter definitions

Parameter	Description
Minium INP	The minimum impulse noise protection for the upstream bearer channel expressed in symbols. One symbol equals 250 uS. No Protection, Half Symbol, Single Symbol, Two Symbols, Three Symbols, Four Symbols, Five Symbols, Six Symbols, Seven Symbols, Eight Symbols, Nine Symbols, Ten Symbols, Eleven Symbols, Twelve Symbols, Thirteen Symbols, Fourteen Symbols, Fifteen Symbols, Sixteen Symbols Default: Two Symbols
PhyR Maximum INP	PHYR maximum upstream impulse noise protection. A value of 0 specifies no protection. The values 5 through 160 specify the number of symbols in 1/10 increments. Default: 0
Upstream GINP Support	Enable or disable upstream G.INP / ITU-G.998.4. Only supported by Broadcom ports. 1 Enabled 2 Disabled (Default)
GINP Maximum Upstream Expected Throughput in Kbps	Maximum allowed value for upstream expected throughput (ETR) in kbit/s. The valid values are all multiples of 8 from 0 to the maximum of the valid values of the maximum net data rate specified in the associated Recommendation. ITU-T G.998.4 7.1.1 Control parameters and 7.1.2 Valid configurations. Default: 60000 kbps
GINP Minimum Upstream Expected Throughput in Kbps	Minimum allowed value for upstream expected throughput (ETR) in kbit/s. The valid values are all multiples of 8 from 0 to the maximum of the valid values of the minimum net data rate specified the associated Recommendation. ITU-T G.998.4 7.1.1 Control parameters and 7.1.2 Valid configurations. Default: 64
GINP Maximum Upstream Net Data Rate (NDR) in Kbps	Maximum allowed value for upstream net data rate (NDR) in kbit/s. The valid values are all multiples of 8 from 0 to the maximum of the valid values of the maximum net data rate specified in the associated Recommendation. ITU-T G.998.4 7.1.1 Control parameters and 7.1.2 Valid configurations. Default: 60000 kbps

Table 7: vdsl-cpe-config profile G.INP support parameter definitions (Continued)

Parameter	Description
GINP Upstream Single High Impulse Noise Event(SHINE) Ratio (0..255)	The upstream loss of rate in a 1 second interval expressed as a fraction of NDR due to a single high impulse noise event (SHINE) impulse noise environment expected by the operator to occur at a pro ginpVdslCpeEtrMin ability acceptable for the services. The valid values are all multiples of 0.001 from 0 to 0.1. This field uses 1 to equal 0.001 and 100 to equal 0.1. ITU-T G.998.4 7.1.1 Control parameters and 7.1.2 Valid configurations. Default: 10
GINP Upstream Low Error Free Rate (LEFTR) Threshold (0..99)	The upstream rate Threshold below which the Low Error Free Rate (LEFTR) defect is declared. The threshold used to declare leftr defects is expressed in fraction of the net data rate (NDR). The value 0 is a special value to indicate that the receiver shall use a special value for declaring leftr defect. The minimum valid threshold to declare leftr is ETR/2. The receiver shall ignore threshold values that are less than the minimum and shall use ETR/2 for declaring leftr defect instead. The valid values are all multiples of 0.01 from 0.01 to 0.99. This field uses 1 to equal 0.01 and 99 to equal 0.99. Default: 0
GINP Maximum Upstream delay in mSecs	The maximum upstream delay in ms. This is the upper limit for the delay that is added to the transmission delay only caused by retransmissions. Here the receiver and/or the transmitter shall identify and discard all DTUs whose payload cannot be transferred over the reference point at the receiver without violating the delay_max limit. The time stamp shall be the criterion for discarding the DTUs. The processing delay between the U-interface and the retransmission sub-layer of the receiver in the retransmission data path direction shall be excluded from consideration for delay_max in the retransmission data path direction. The valid values are all integers from 1 to 63. ITU-T G.998.4 7.1.1 Control parameters, 7.1.2 Valid configurations, and 8.1.6 Time Stamp. Default: 20 mSecs
GINP Minimum Upstream delay in mSecs	The minimum upstream delay in ms. This is the lower limit for the delay that is added to the transmission delay caused by retransmissions only. The time stamp shall be used by the outlet shaping function to determine when the payload of the DTU shall be sent to the reference point to meet the delay limits. The outlet shaping function shall minimize the additional delay that may be introduced above delay_min, and shall never exceed delay_max. The valid values are all integers from 0 to 63. ITU-T G.998.4 7.1.1 Control parameters, 7.1.2 Valid configurations, and 8.1.6 Time Stamp. Default: 0

Table 7: vdsl-cpe-config profile G.INP support parameter definitions (Continued)

Parameter	Description
GINP Minimum Upstream Impulsive Noise Protection (INP)	The minimum upstream impulse noise protection (INP) against single high impulse noise event (SHINE) in discrete multitone (DMT) symbols. The valid values are all integers from 0 to 63 for system with a sub-carrier spacing of 4.3125 kHz. The valid values are all integers from 0 to 127 for system with a sub-carrier spacing of 8.625 kHz. ITU-T G.998.4 7.1.1 Control parameters and 7.1.2 Valid configurations. Default: 4
GINP Minimum Upstream Bandwidth Reserved for RS (reed-solomon) (0..64)	This value specifies the upstream bandwidth reserved for RS (reed-solomon) codewords. The minimum guaranteed R/N ratio. The unit is 1/256th and the range is 0..64 (0 to 25%). Default: 0
GINP Minimum Upstream Repetitive Impulse Noise (REIN) Configuration	The minimum upstream impulse protection against electrical repetitive impulse noise (REIN) in DMT symbols. The valid values are all integers from 0 to 7 for system with a sub-carrier spacing of 4.3125 kHz. The valid values are all integers from 0 to 13 for system with a sub-carrier spacing of 8.625 kHz. ITU-T G.998.4 7.1.1 Control parameters and 7.1.2 Valid configurations. Default: 0
GINP Frequency of REIN Inter-Arrival Time in Hz	Specifies the frequency of REIN inter-arrival time. It is used in the Channel Initialization Policy and on-line reconfiguration procedures. REIN is commonly coupled from electrical power cables appliances drawing power from the AC electrical power network, having a repetition rate of twice the AC power frequency (100 or 120 Hz). The valid values are integers 100 hz or 120 hz. ITU-T G.998.4 7.1.1 Control parameters and 7.1.2 Valid configurations." 1 100 2 120 Default: 120

Table 7: vdsl-cpe-config profile G.INP support parameter definitions (Continued)

Parameter	Description
GINP Upstream Retransmission Mode	Upstream retransmission Mode (RTX MODE). The RTX_MODE is a configuration parameter used to control activation of retransmission during initialization. This parameter has 4 valid values: FORBIDDEN: ITU-T G.998.4 retransmission not allowed. PREFERRED: ITU-T G.998.4 retransmission is preferred by the operator. (i.e., if ITU-T G.998.4 RTX capability is supported by both XTU's, the XTU's shall select ITU-T G.998.4 operation for this direction). FORCED: Force the use of the ITU-T G.998.4 retransmission. (i.e., if ITU-T G.998.4 RTX capability in this direction is not supported by both XTU's or not selected by the XTU's, an initialization failure shall result). NOTE: Due to the optionality of ITU-T G.998.4 retransmission in upstream direction, the use of FORCED in upstream may lead to initialization failure, even if the XTU is supporting ITU-T G.998.4 (in downstream). TESTMODE: Force the use of the ITU-T G.998.4 retransmission in the test mode described in clause 10.4. (i.e., if ITU-T G.998.4 RTX capability is not supported by both XTU's or not selected by the XTU's, an initialization failure shall result). ITU-T G.998.4 11.1.13 Retransmission Mode (RTX_MODE). 1 forbidden 2 preferred (default) 3 forced 4 testmode Default: preferred

Configuring T1/E1 physical ports

- 1 From the tree view, expand the T1/E1 card and then expand the physical interfaces.
- 2 Right-click a T/E1 physical interface and select **Modify**. The **Modify T1/E1 Physical Port Configuration** dialog box appears.
- 3 Configure the settings for the T1/E1 physical ports.
For details on the settings, see the online help.
- 4 To configure the PWE (PseudoWire Emulation) solution for the T1/E1 physical ports of the T1/E1-PWE-24 card, you can right-click on the T1/E1 physical port, and select **Modify**. In the **Modify E1/T1 Physical Port Configuration** dialog, select PWE Bundles.
Click **Add** to open the **Add PWE Bundle Configuration** dialog.
In the dialog, click **PWE Bundle**. The **PWE Bundle** window appears.

In the dialog, click **Bundle DS0 Bits** to open the Bundle DS0 Bits window.

In the **PWE Bundle** window, click **Modify** or **View** to open the **Modify PWE Bundle Configuration** window or **View PWE Bundle Configuration** window..

For details on the settings, see the online help.

Configuring G.SHDSL physical ports

- 1 From the tree view, expand the G.SHDSL card and then expand the physical interfaces.
- 2 Right-click a G.SHDSL physical interface and select **Modify**. The **Modify DSL Physical Port Configuration** dialog box appears.

Figure 9: G.SHDSL port on MALC/ MXK/ Raptor XP

Figure 10: G.SHDSL port on EtherXtend

- 3 Configure the SNR monitoring settings for the G.SHDSL physical ports with the following parameters:
 - Target Current Condition Mode
 - Target Current Condition SNR Margin (dB)
 - Target Worse Case Mode
 - Target Worse Case SNR Margin (dB)
 - Min SNR Margin Threshold (dB)
 - SNR Margin Crossing Trap Enabled
 - Max SNR Margin Threshold Delta (dB)
 - SNR Maintenance Mode
 - Maintenance Start Time
 - Maintenance End Time
 - SNR Monitor Interval
- 4 Configure the error monitoring settings for the G.SHDSL physical ports with the following parameters:
 - Err Threshold Monitoring
 - Err Threshold Monitor Notif Trap
 - Err Threshold Monitor Interval (sec)
 - Err Threshold Monitor Clear Interval (sec)
- 5 Configure the auto discovery settings for the G.SHDSL physical ports.
- 6 Set auto-negotiate or a data rate in the **Data Rate** (Kbps) field.

Setting the parameter to 0 sets the data rate to auto-negotiate. Entering a range between 192 and 5696 defines a specific range of the data rate.

7 Select constellation setting for TCPAM in the **Constellation** field.

TCPAM configurations have a minimum and a maximum data rate depending on the constellation setting. If a data rate is set outside of the range of the constellation setting, an error message will be displayed.

Here are the additional settings for the **Constellation** parameter and rate range for the **Data Rate** (Kbps) parameter:

- Adaptive: data range in 192 - 5696
- TCPAM-004: data range in 192-2048
- TCPAM-008: data range in 192-5056
- TCPAM-016: data range in 192-7616 or an adaptive rate of 0
- TCPAM-032: data range in 768-10176 or an adaptive rate of 0
- TCPAM-064: data range in 768-12736

8 Click **Modify**, then **Close**.

1 For details on the settings, see the online help.

1 Viewing EtherXtender Performance Statistics

When the EtherXtender SHDSL line extender is used on the MALC/ MXK, the ZMS outputs SHDSL EtherXtender regenerator performance statistics as gathered by each EtherXtender on the line. The statistics are shown per line regardless of whether multiple lines are bonded.

1 To view the EtherXtend Regenerator physical line statistics for the GSHDSL port. Right-click on a GSHDSL port, then select **View EtherXtender Regenerator Statistics**.

The **View DSL Physical Performance Statistics** dialog appears.

2 If you want to refresh the data, click Refresh button in the View DSL Physical Performance Statistics dialog.

Configuring Malc XP/ Raptor XP physical ports

1 From the tree view, expand a Malc XP or a Raptor XP device and then expand the physical interfaces.

2 Right-click a Malc XP or a Raptor XP physical interface and select **Modify**. The **Modify Ethernet Physical Port Configuration** dialog box appears.

3 Configure the settings for the Malc XP/ Raptor XP physical ports.

For details on the settings, see the online help.

Configuring Link aggregation and LACP

Link aggregation provisioning is disabled in ZMS by default. To use the following instruction about how to provision Link aggregation in ZMS, you must enable linkagg in the *NetHorizhon.properties* first.



WARNING! Adding, deleting and modifying linkAgg groups is no longer allowed from ZMS since 2.4.1.28. The linkAgg provisioning must be performed from the MXK (any device's) CLI. To enable this functionality in ZMS, "allowLinkaggProvisioning" can be set to "true" in *NetHorizhon.properties*. Changing this property file requires re-signing of the jar file. Also, enabling LinkAgg may require a change to MXK as well.

Please call GSS for instructions.

Topics:

[Link Aggregation on page 181](#)

[Link Aggregation Control Protocol \(LACP\) on page 182](#)

[Prepare the uplink card for link aggregation on page 182](#)

[Creating a link aggregation group on a uplink card on page 183](#)

[Creating a link aggregation group on a Active Ethernet card on page 184](#)

[Deleting a link aggregated group on page 184](#)

[Link resiliency on page 185](#)

[Configuring interfaces for link aggregation on page 185](#)

Link Aggregation

The MALC/MXK/XP supports 802.3ad link aggregation on the uplink cards.

The MXK supports link aggregation on the Active Ethernet card.

Link aggregation allows you to aggregate two or more physical 10 Gigabit Ethernet, Gigabit Ethernet or Fast (10/100 mbps) Ethernet uplink ports into one single aggregated logical port for additional bandwidth capacity and resiliency. In general, link aggregation groups can consists of up to eight ports.

For redundant uplink cards, the link aggregated ports on each card provide redundant uplink port protection.



Note: The Ethernet switch on the remote end will need to be configured for link aggregation.

Link Aggregation Control Protocol (LACP)

The MALC/MXK/XP also support LACP, a layer 2 protocol used between network elements to exchange information regarding a link's ability to be aggregated with other similar links.

LACP control is set in the Aggregation Mode parameter in the Modify Ethernet Physical Port Configuration dialog box.

The default for the aggregation mode parameter is on.

The aggregation mode parameter field has four values defined as follows:

- **Active**
The setting for LACP use, the Ethernet link sends and receives LACP messages and link aggregates automatically when the remote system responds with the appropriate LACP messages.
- **On**
This Ethernet link can be aggregated manually using the **Modify Link Aggregation** dialog box. LACP messages are not sent from this port, and any received LACP messages are ignored.
- **Passive**
This mode sets a link to receive LACP messages, and responds with LACP when receiving a far-end LACP initiation.
- **Off**
This Ethernet link cannot be aggregated either manually or dynamically; LACP is not sent from this port and any received LACP messages are ignored.

The following table shows the compatibility matrix for the four settings.

Table 8: LACP compatibility matrix settings

Device one	Device two	Comments
Active	Active	Both devices are sending and receiving LACP. Recommended setting for dynamic aggregation.
Active	Passive	One side of the connection between devices attempts to negotiate a aggregated group. Functional, but not recommended.
On	On	Will make links available for manual aggregating; only recommended if the far-end device is not capable of LACP.

Prepare the uplink card for link aggregation

Link aggregation and LACP are not supported on FE/GE uplink cards running in RPR mode. If the FE/GE uplink card is running in RPR mode, the

card-profile interface for the uplink card must first be deleted, then a new card-profile interface with a linear Ethernet interface must be added.:



WARNING! Deleting the card-profile interface for the FE/GE uplink card will delete the configuration settings for all the line cards on the MALC. After adding the new card-profile interface, you must then re-configure all the line cards.

To prepare an uplink card for link aggregation the following card-profile and Ethernet port profile must have the following settings:

- For link aggregation to work, the card-line-type parameter in the card-profile interface for the FE/GE uplink card must be running in linear Ethernet mode.
- The aggregation mode parameter in the Modify Ethernet Physical Port Configuration dialog box must be set to *on* or *active* depending on the choice of manual link aggregation or LACP.

Changing the LACP aggregation mode

To activate LACP dynamic link aggregation, change the aggregation mode parameter of Gigabit Ethernet port from on to active.

- 1 From the tree view, expand an uplink card or the FE/GE uplink card that running in linear Ethernet mode, and then expand the physical interfaces.
- 2 Right-click a Ethernet port and select **Modify**.
The Modify Ethernet Physical Port Configuration dialog box appears.
- 3 Select **Active** from the Aggregation Mode parameter drop-down menu.
- 4 Click **Modify**.

Creating a link aggregation group on a uplink card

Link aggregation groups on the MALC/MXK/XP can be performed from the ZMS. You can manually create link aggregation groups only when LACP is not used or LACP is available and the aggregation mode is set to on.

To manually create a link aggregation among ethernet ports:

- 1 From the ZMS tree view, expand the device and then expand a uplink card.
- 2 Right-click the Link Aggregation Groups and select Add. The Add Link Aggregation dialog box appears.
- 3 In the **Add Link Aggregation** dialog box, enter the Name for the link aggregation group, and click **Add**. The link aggregation group name can be automatically assigned by ZMS if you didn't enter any names.
- 4 In the tree view, right-click this link aggregation group and select Modify. The Modify Link Aggregation Group dialog box appears.

- 5 To add physical ports into the link aggregation group, click Grouped Physicals and click Assign Links. A dialog appears with link assignments.
- 6 Select new link assignment and click **OK**.
- 7 The aggregated ports appear in the Grouped Physicals dialog box and tree view.
- 8 Add physical ports into a link aggregation group will automatically creates the corresponding redundant link.
- 9 Create an aggregated port on the card the MALC is connected to.

Creating a link aggregation group on a Active Ethernet card

To manually create a link aggregation on a Active Ethernet card:

- 1 From the ZMS tree view, expand the MxK and then expand a Active Ethernet line card.
- 2 Right-click the Link Aggregation Groups and select Add. The Add Link Aggregation dialog box appears.
- 3 In the Add Link Aggregation dialog box, enter the Name for the link aggregation group, and click Add. The link aggregation group name can be automatically assigned by ZMS if you didn't enter any names.
- 4 In the tree view, right-click this link aggregation group and select Modify. The Modify Link Aggregation Group dialog box appears.
- 5 To add physical ports into the link aggregation group, click Grouped Physicals and click Assign Links. A dialog appears with link assignments.
- 6 Select new link assignment and click **OK**.

Note that, the physical ports cannot be grouped if they have services configured on them.
- 7 To view the link aggregation group statistics. Right-click the desired link aggregation group and select **Statistics**. The **View LinkAgg Physical Performance Statistics** dialog appears.
- 8 To view the Ethernet physical line statistics for the Ethernet port inside of a Link Aggregation Group. Expand the link aggregation group, and expand the Physical level. Right-click on a Ethernet port, then select **Statistics**. The **View Ether Physical Performance Statistics** dialog appears.

Deleting a link aggregated group

To delete a link aggregated group, should delete the aggregated physical ports in the link aggregation group first, then delete the link aggregation group:

- 1 In the tree view, right-click the link aggregation group and select **Modify**. The Modify Link Aggregation Group dialog box appears.

- 2 To release grouped physical ports from this link aggregation group, click **Grouped Physicals** and click **Assign Links**. A dialog appears with link assignments. Uncheck the physical ports and click **OK**.
- 3 The link aggregation group has no physical ports bundled in it now. Right click the link aggregation group, and click **Delete**. The Delete confirm window appears.
- 4 In the Delete confirm window, click **OK**. The link aggregation group is removed.

Link resiliency

When an aggregated link fails, the linkagg interface remains up with the rest physical port links. If the failed link returns, the link aggregation group adds the link back without any service interruption. If all the links in a link aggregation group fail, then the link aggregation group is moved to a down state until at least one of the physical links is restored.

Configuring interfaces for link aggregation

Interfaces can be added to link aggregation ports for bridging and IP routing.

Bridge configurations

To add an bridge (with type Uplink, Downlink, or TLS) on the logical link aggregation port:

- 1 In the tree view, right-click a link aggregation group and select **Manage Bridging**. The Manage Bridge Logicals dialog box appears.
- 2 Click **Add** in the **Bridge Logical** portion of the dialog box. The Bridge Logical dialog box for adding a bridge appears.
- 3 Select a bridge logical type from the range of Uplink, Downlink, or TLS; and configure the corresponding settings; and then click **Add**.
- 4 Select the bridge logical and click **Add** in the **Bridge Path** portion of the Manage Bridge Logical dialog box. The Bridge Path dialog box appears.
- 5 Specify the desired bridge path settings, and click **Add**.
- 6 A confirmation box appears verifying that the bridge path was successfully added.

Unlearned traffic received on this interface is forwarded to the external network.

Interface configurations

To add an interface on the logical link aggregation port:

- 1 In the tree view, right-click a link aggregation group and select **Manage IP**. The IP Configuration Manager dialog box appears.
- 2 Click **Add**, the **Add IP Interfaces** dialog box appears.

- 3 Select the link aggregation port from the Select Physical dialog box.
- 4 Add IP Address and Net Mask. And then click **Add**.
- 5 Select the bridge logical and click **Add** in the **Bridge Path** portion of the Mange Bridge Logical dialog box. The Bridge Path dialog box appears.
- 6 Specify the desired bridge path settings, and click **Add**.
- 7 A confirmation box appears verifying that the bridge path was successfully added.

This creates an IP interface on the MALC link aggregation port with an IP address and a subnet mask.

Ethernet redundancy

The MXK supports Ethernet redundancy specified in the standards specification.

Ethernet redundant ports provide link protection between Ethernet cards on the MXK to subtended devices such as MXKs and MALCs as well as to Layer 2 (L2) switches.

Ethernet redundancy groups consist of two Ethernet ports. The two Ethernet ports can be on the same or different Ethernet cards. Since it is port level redundancy and not card level redundancy, the port number on one card does not need to match the port number on the second card.

A single Ethernet port cannot be configured in two groups at the same time.

Use the **Line Redundancy Dialog** box to designate which port is primary or secondary when creating a redundancy group. If you reboot the MXK system (or reboot the cards which have the redundant ports), the Ethernet port which comes up first and passes traffic becomes the active port.

In a redundancy group, one Ethernet port is always assigned as active and the other as standby. If an active Ethernet port fails, the standby takes over and becomes active. Note that Ethernet redundancy is non-revertive; that is, a previously active Ethernet port which has failed does not become active when the reason for the failover is resolved. The current active port will stay active until that port/line fails, then the standby (if the initial issue was resolved) will once again become the active port.

When a standby port is added to a redundancy group and comes up, the card with the active port copies over the configuration database and routing tables to the standby Ethernet port on the second card. As configuration changes are made to the active port, the standby port is automatically updated.



Note: Create the line redundancy before building interfaces such as bridges. If you add a port with existing interfaces as primary port of the redundant pair, you will need to perform a **slot reboot** on the Ethernet card with the secondary port after adding the redundancy.



Note: All logical interfaces *must* always be created on the *primary* port of the redundant pair.

Related topics:

[Configure GPON type B redundancy, page 204](#)

Configuring Ethernet line redundancy



Note: Ethernet port redundancy does not work on Ethernet ports that are a part of a link aggregation group.

- 1 Turn off the **Aggregation Mode** of two Ethernet ports that designated for port redundancy in the **Modify Ethernet Physical Port Configuration** dialog box, and click **Modify**.
- 2 Create line redundancy by right-clicking an MXK and selecting **Manage Line Redundancy**.

The **Line Redundancy Dialog** box appears.

- 3 Click **Add**.
- 4 Browse to and select a Primary Physical.
- 5 Click **OK**.
- 6 Browse to and select a Secondary Physical.
- 7 Click **OK**.
- 8 Click **Add**.
- 9 The redundancy lines will appear as a pair in the Line Redundancy Dialog.

Removing a redundant Ethernet port

Redundancy may be removed from an Ethernet port, however there are limitations. The original primary port cannot be removed. Active ports can also not be removed.

- 1 Right-click an MXK and select **Manage Line Redundancy**.
The **Line Redundancy Dialog** screen appears.
- 2 Highlight the redundant pair you want to remove.
- 3 Click **Delete**.
- 4 Confirm that you want to delete the pair.

Disable standby transmit on Standby AE ports

After two Active Ethernet port have been paired in the line redundancy group, you can disable the Standby Transmit on the standby Active Ethernet port to turn off the laser, in order to avoid confusing the remotely connected AE port.

To turn off the Standby Transmit on the standby Active Ethernet port, use the following procedure:

1. Right-click on an Active Ethernet port in the tree view. For example: "Ether 2 (GigE): 1-14-2-0(Secondary).

2. Select **Modify**.

The **Modify Ethernet Physical Port Configuration** window appears.

3. Select **Line Redundancy**.

4. Uncheck the **Standby Transmit** box, and click **Modify**, and then click **Close**.

Switchover from active to standby Ethernet port

A switchover from active to standby Ethernet port can be done automatically or forced manually.

Automatically switched

A switchover is automatically triggered when a Loss of Signal occurs on the primary port.

When an automatic switchover occurs, an alarm is raised.

Manually switched

A switchover also can be manually switched by the operator by setting the Admin status of the port to Down, then Up in the **Modify Ethernet Physical Port Configuration** screen.

Ethernet redundancy configuration limitations

The following limitations apply to Ethernet redundancy configurations.

- When a standby port is added, the configuration information is automatically inherited. If a port is configured as standby, logical interfaces cannot be configured on that port.
- The state of the card which has proposed secondary ports must be RUNNING.
- An Ethernet port may only be a member of one redundancy group.
- An Ethernet port may only be made redundant with another Ethernet port.

- The following rules apply to deleting ports from Ethernet redundancy groups:
 - The primary port can not be deleted from the redundancy group.
 - An active port can not be deleted from the redundancy group. If the active port is the secondary port of the redundancy group, neither port can be removed.
 - Only the secondary port of a redundancy group can be deleted and only in the standby state.
- Upgrades cannot be scheduled on standby ports.



Note: If a switchover event is triggered when an upgrade is in progress, the upgrade is re-queued.

Concurrent uplinks on the MXK 2.2.x

ZMS supports concurrent uplink on the MXK. With concurrent uplinks, the MXK provides facility protection with redundant uplinks.

With the 2.2.x release of the MXK, all of the Ethernet ports on uplink cards are redundant with the corresponding ports on paired uplink card automatically. Port 1 of the uplink card in slot a is paired with port 1 of the uplink card in slot b; port 2 of the uplink card in slot a with port 2 of the uplink card in slot b, and so on. These pairing of ports from one uplink card to the other are called line redundant groups.

The pairs of redundant uplink ports are added automatically into the **Line Redundancy Dialog**. To view this screen, right-click an MXK device, and then select **Manage Line Redundancy** menu item.

If a link on a port in Active state goes down, traffic is automatically sent to the corresponding port on the other uplink card which is in Standby state. Unlike previous versions of the MXK which required the Active uplink card to switch to the Standby uplink card when a link went down — now just the single link changes.

Uplink cards are still considered Active and Standby. The Active uplink card maintains the system databases. In the default state the active ports of the line redundant groups will all be on the uplink card in slot a.

Since both uplink cards are in the 'running' state when an active link in a group goes down, the standby link in the group takes over without a state change in the uplink cards, they both would still be in the running state. In this configuration both the Active and the Standby uplink cards could be forwarding traffic thereby providing facility protection with redundant uplinks.

If the Active uplink card fails, the Standby card, which maintains a synchronized set of system databases, becomes the Active uplink card.

ZMS indicates **Running with Traffic** and **Running without Traffic** for each Active and Standby Uplink in the tree view.

Settable alarm severity for Ethernet ports

The alarm severity for Ethernet ports can be set to the following levels: *critical*, *major*, *minor*, or *warning*. The default level is *minor*.

Changing the alarm severity level for one Ethernet port

Use the **Modify Ethernet Physical Port Configuration** dialog > **Alarm Config** window to set the severity level on an Ethernet port.

- 1 Right-click an Ethernet port in the tree view, select **Modify**.
The **Modify Ethernet Physical Port Configuration** dialog appears.
- 2 In the **Modify Ethernet Physical Port Configuration** dialog, click **Alarm Config**.
The **Alarm Config** window appears.
- 3 Select a severity level in the **Alarm Severity** drop-down menu, and click **Modify**.

Bond groups

- [EFM, N2N bond groups on page 190](#)
- [Gbond bond group on page 192](#)
- [Multiple Links for PPP \(MLPPP\) bond group on page 196](#)

EFM, N2N bond groups

Adding an EFM/N2N bond group

To add a T1/E1, G.SHDSL, or EtherXtend bond group, expand the card and then right-click Bond Group and select **Add**. The **Add Bond Group** dialog box appears.

- 1 Bond groups should be configured on the CO card and the CPE.
- 2 Configure the Bond Group Type and Name for the bond group. The bond group ID can be automatically assigned by ZMS by clicking the **Allow ZMS to assign group ID** or manually configured by user by un-checking the box.

For details on the settings, see the online help.

- 3 To modify a bond group, expand the card and then right-click the desired Bond Group and select **Modify**. The **Modify Bond Group** dialog box appears. This example shows a G.SHDSL bond group.
- 4 Modify the bond group configuration settings.

- 5 To change the physical ports in a bond group, click Grouped Physicals and click **Assign Links**. A dialog appears with link assignments.

User can select physical ports for the same EFM bond group across different cards. For N2N bond group, user can select physical ports in the same card.

Select new link assignment and click **OK**.

- 6 To change the group type for individual bond groups or all bond groups used in a specified slot. Right-click the desired bond group or the **Bond Groups** folder, and select **Change Bond Group Type**. The **Modify Bond Group Type** dialog box appears. Select a new bond group type as N2N or EFM, and click **OK**.

To view the bond group statistics. Right-click the desired bond group and select **Statistics**. The **Bond Group Physical Performance Statistics** dialog appears.

- 7 To view the bond group configuration settings. Right-click the desired bond group and select **View**. The **View Bond Group** dialog appears.
- 8 To view the DSL physical line statistics for the DSL port inside of a bond group. Expand the bond group, and expand the Physical level. Right-click on a DSL port, then select **Statistics**. The **View DSL Physical Performance Statistics** dialog appears.
- 9 To modify the configuration for a DSL physical port inside of a bond group. Expand the bond group, and expand the Physical level. Right-click on a DSL port, then select **Modify**. The **Modify DSL Port Configuration** dialog appears
- 10 To view the configuration for a DSL physical port inside of a bond group. Expand the bond group, and expand the Physical level. Right-click on a DSL port, then select **View**. The **View DSL Port Configuration** dialog appears

Gbond bond group

ZMS supports bonding on the Broadcom based MALC/MXK ADSL2+ 48-port line cards, ADSL2+ 72-port line cards, VDSL 24-port line cards, and VDSL 48-port line cards:

Bonding allows multiple lines to work together as a single line.

ADSL/VDSL bonding rules on 24-port and 48-port ADSL2+/VDSL2+ cards, 72-port ADSL2+ cards

This section describes bonding rules for ADSL2+/VDSL2+ cards:

- [24-port VDSL2+ DSP core boundaries and bonding rules, page 192](#)
- [48-port ADSL2+/ VDSL2+ DSP core boundaries and bonding rules, page 192](#)
- [72-port ADSL2+ DSP core boundaries and bonding rules, page 193](#)
- [Bonding rules common to the 24-port, 48-port, 72-port ADSL2/VDSL2 card, page 193](#)

The 24-port VDSL2 cards, 48-port ADSL2/VDSL2 cards, and 72-port ADSL2 cards support ADSL2+ or VDSL2 bonding using the **Add Bond Group** window and the **Modify Bond Group** window.

Bonding allows two lines to work together as a single line.

24-port VDSL2+ DSP core boundaries and bonding rules. The bonding rules for VDSL2 24-port VDSL2 card *gbond* groups are:

- The valid range for *gbond* groups is 1-24.
- There are two VDSL2 DSP chips per device with ports 1-12 on one chip, and ports 13-24 on the next chip. There are three ports per core and four cores per chip.

Members of *gbond* groups must be consecutive ports which do not cross chip core boundaries. For example, ports 1 and 2 can be in a bond group or ports 2 and 3 but not ports 3 and 4. Ports 4 and 5 or ports 5 and 6 can be bonded, but not ports 6 and 7, and so forth. Refer to [Figure 11](#) for chip core ports.

Figure 11: 24-port VDSL2 DSP core boundaries

48-port ADSL2+/ VDSL2+ DSP core boundaries and bonding rules. The bonding rules specific to ADSL2+ or VDSL2 48-port VDSL2 card *gbond* groups are:

- The valid range for *gbond* groups is 1-48.
- The 48-port ADSL2/VDSL2 card has four ports per core and bonded ports *must* be in the same core.

- Bonded ports must be consecutive (sequential) and only two ports per bonded groups are allowed with two bond groups allowed per core.

For example, you can bond ports 1 and 2 and 3 and 4 and have two groups. You can also bond ports 2 and 3, however you cannot bond ports 1 and 4 which means this core configuration could only have one bonded group.

72-port ADSL2+ DSP core boundaries and bonding rules. The ADSL2+ 72-port line card supports ADSL2+ bonding.

Bonding allows multiple lines to work together as a single line. Each bonding group can have:

- Two members per bond group.
- Members of a *gbond* group *must* be in a bond group that does not cross chip core boundary. There are 8 DSP cores, so 64 ports can be bonded. Each chip core has nine ports (ports 1-9, 10-18, 19-27, 28-36, and so on). You can create *gbond* groups with any combination of eight of the nine ports in a chip core, but you cannot combine ports 9 and 10 because that would cross a chip core boundary.
- The *gbond* group index *must* match the ports of the chip core.
- Bond group numbers must be in appropriate ranges. When using ZMS to create a *gbond* group the valid range is from 1-72.

Bonding rules common to the 24-port, 48-port, 72-port ADSL2/VDSL2 card. The following rules apply to all MALC/MXK ADSL2+ 48-port line cards, ADSL2+ 72-port line cards, VDSL 24-port line cards, and VDSL 48-port line cards:

- If you attempt to add more than two members, non-contiguous ports, ports which cross chip boundaries, or groups outside of the valid range the ZMS will remind you of these rules. You also cannot add the same member to different bound groups.
- Ports configured with bridges or interfaces will not be allowed to become members of a *gbond* group.
- Bridges or interfaces cannot be added/deleted to/from empty *gbond* groups.
- The last member of a *gbond* group cannot be deleted if a bridge or interface is configured on the *gbond* group.
- A *gbond* group cannot be deleted when a bridge or interface is configured on the *gbond* group.
- A bridge or interface cannot be configured on a link that is a member of a *gbond* group.

- When ADSL bonded modems are used on VDSL2 ports, the **Transmission Mode** parameter in the **Modify VDSL Port Configuration** dialog box > **Config Profile** window must be configured to either *Adsl2 Plus Mode*, *Adsl2 Mode*, or *Gdmt Mode* before the port is added to a *gbond* group.

If this does not occur, the port will not get link.

- When VDSL2 bonded modems are used on VDSL2 ports, the **Transmission Mode** parameter in the **Modify VDSL Port Configuration** dialog box > **Config Profile** window may remain at the default *Auto Negotiate Mode* or set to *Vdsl2 Mode* before the port is added to a *gbond* group.

If this does not occur, the port will not get link.

The **vdsl2 Profile** parameter in the **Modify VDSL Port Configuration** dialog box > **Config Profile** window must also be set to either *g993-2-8a*, *g993-2-8b*, *g993-2-8c*, *g993-2-8d*, *g993-2-12b*, and *g993-2-17a*.



Note: Bonded links on the VDSL2-48-V are capped in all VDSL2 profiles by the Broadcom chipset to downstream rates of 60 Mb and upstream rates of 20 Mb.

Adding a Gbond group

- 1 To add a Gbond group, expand the ADSL2+ or VDSL2+ card in the tree view.
- 2 Right-click **Bond Groups** and select **Add**. The **Add Bond Group** dialog box appears.
- 3 Assign the Name and the Bond Group ID for the bond group.
- 4 Click **Add**. The GBond group appears in the tree view.
- 5 Right-click the newly created GBond group in the tree view, and select **Modify**. The **Modify Bond Group** dialog box appears.
- 6 Click **Grouped Physicals** to open the **Grouped Physical** window.
- 7 Click **Assign Links**. A dialog appears with link assignments.
- 8 Select new link assignment and click **OK**. The GBond group members should be two contiguous ADSL ports, and these two ADSL ports should be on the same chip core (6 ports per core).

The selected ADSL ports appear in the **Grouped Physicals** window.

- 9 Click **Modify**, and then click **Close**.

The bond group members appear in the tree view.

Adding bridge on a Gbond group

- 1 To add bridge on a Gbond group, right-click a device with ADSL2+ or VDSL 2+ card inserted and select **Manage Bridging**.

The **Manage Bridge Logicals** dialog appears.

- 2 Click **Add** to open the Bridge Logical on this device.
- 3 Select the GBond group in the Select Physical box, and specify the desired bridge settings.
- 4 Click **Add**.

Multiple Links for PPP (MLPPP) bond group

Multilink PPP (MLPPP or MP) is a protocol which provides for multiple point-to-point (PPP) links (RFC 1717) to increase bandwidth. The MALC supports MLPPP bridging and routing on the MALC-EFM-T1/E1-24 line card, the MXK supports them on the ??? card, and a variety of Internet Access Devices (IADs). MLPPP on the MALC and MXK supports IADs which use Bridge Control Protocol (BCP) for bridged configurations or Internet Protocol Control Protocol (IPCP), depending upon their configuration, after successful MLPPP Link Control Protocol negotiations.

The remote end IAD sets whether the MLPPP bond group will use, BCP or IPCP mode. One can add bridges and routed interfaces to MLPPP bond groups like any other ports, following the same rules as on other appropriate physical or virtual interfaces. But, if the IAD is configured for IPCP operation, only the routed interfaces added will work, the bridge interfaces will not work.

For host based routed interfaces which use a floating IP address, the floating address becomes the local (MALC/MXK end) IP address (the combination of **interface add float** action and **host add** action). The host address is what is offered to the IAD. See [Offering an IP address to the far end IAD using host add, page 198](#).

Network based addressing (**interface add** action, not **float**) give the local IP address. The ability to offer an IP address to the remote IAD is configured by the **destination address** parameter in the **ip-interface-record** for the bond group. See [Offering an IP address to the far end using interface add, page 199](#).

The MALC-EFM-T1/E1-24 card and ?? card can bond any combination of links into Zhone Net2Net bundles or MP bundles, provided each bundle does not exceed the 8 link per group restriction. All DS0s of a T1 or E1 will be utilized in the link.

Creating MLPPP bond groups

In this example we will create a MLPPP bond group and add members to the group.

- 1** Create a MLPPP bond group.
 - a** Expand slot level.
 - b** Right-click **Bond Groups**, and select **Add**. The **Add Bond Group** dialog appears.
 - c** Specify the following fields in the **Add Bond Group** dialog:
 - Bond Group Type:** Select MLPPP.
 - Name:** Specify a bond group name. You can append default name as well.
 - Bond Group ID (25-99):** You can either allow ZMS to assign group ID or specify a group ID manually. The Bond Group ID is in the range of 25-99.

- d** Click **Add**.
- 2** Add bond members to the bond group:
 - a** Right-click the MLPPP bond group, click **Modify**. The **Modify Bond Group** dialog appears.
 - b** Select **Advanced > Grouped Physicals**.
 - c** Click **Assign Links**.
The **Select physicals for group** window appears.
 - d** Select E1 physicals that will be the members of the group.
 - e** Click **OK**.

Deleting bond groups

- 1** Remove the assigned physical ports from the bond group first.
 - a** Right-click the bond group, click **Modify**.
The **Modify Bond Group** window appears.
 - b** Select **Advanced > Grouped Physicals**.
 - c** Click **Assign Links**, the **Select physicals for group** window appears.
 - d** Un-check the physical ports, and click **OK**.
- 2** Then delete the bond group.
 - a** Right-click the bond group, and select **Delete**.
 - b** Click **OK** in the Delete confirmation window.

Remote IP address options on IADs

IPCP allows the IP address of the bond group interface to be configured locally relative to the interface, or remotely by the peer (the “other” or far end). The device (i.e. MALC, MXK) end, which we identify as the local end, will always be configured locally. The remote end, will either be configured locally relative to itself, or the device will offer an IP to the remote end during IPCP negotiations.

Depending on the type of IP interface, the far end IAD is offered an IP address by different mechanisms.

- For **interface add float, host add** combination of the actions the IP address which is offered to the far end IAD is added in the **host add** action. It is not necessary to add a remote IP address if the remote IAD already has one statically configured. The MALC/MXK does not need to know or use the remote IP address, however, the remote IP address is useful for administration purposes.

See [Offering an IP address to the far end IAD using host add](#).

- For non-float **interface add** method, you add the IP address in the **destination address** parameter of the **ip-interface-record** created by adding an MLPPP interface.

See [Offering an IP address to the far end using interface add](#).

Offering an IP address to the far end IAD using host add

- 1 Use the **Add IP Logical Configuration** dialog to create an unnumbered interface.
 - a Right-click the device, select **Manage IP**.
The **IP Configuration Manager** dialog appears.
 - b Select the **Floating IP** tab, and then click **Add**.
The **Add IP Logical Configuration** dialog appears.
 - c Enter values for the necessary fields, such as Name and IP Address, and then click **Add** to create the local IP address (the MALC/MXK end).

For example, enter mlppp2 to the name field, enter 10.97.0.1 to the IP address field.
- 2 Use the **IP Subscriber Hosts On Device** dialog to offer the IAD the far end address
 - a Right-click the device, select **Manage IP**.
The **IP Configuration Manager** dialog appears.
 - b Select the **Subscriber Hosts** tab, and then click **Add**.
The **IP Subscriber Hosts On Device** dialog appears.

- c** In the **Select Physical Ports** pane, expand the EFM bond card, and then select a MLPPP Bond group. In the **Remote Address Type** pane, select Dynamic or Static, and enter desired values to other fields as well. And then click **Add**.

For example, select Static, enter 10.92.0.2 to the IP Address field.

- 3** The IP addresses are displayed in the **Ip Configuration Manager** dialog > **Subscriber Hosts** pane.
- 4** A **IP Subscriber Hosts On Device** dialog may be used for any IP downstream of the CPE device if the host is in the same subnet as the floating IP address. Or you could use a **Add Ip Static Route Configuration** dialog to add a static route for subnets downstream from the CPE.

The following procedure describes how to use the **Add Ip Static Route Configuration** dialog.

- a** Expand the device in the NetHorizon navigation tree view, find **Routing Domains**.
- b** Expand the **Routing Domain** in the tree view, right-click the **88 Ip Routing Domain**, and then select **Modify**.

The **Modify IP Routing Domain Configuration** dialog appears.

- c** Click **Static Route** in the tree view, and click **Add**.

The **Add Ip Static Route Configuration** dialog appears

- d** Click **Static Route Configuration** in the tree view.

Enter your desired values to the fields in the **Static Route Configuration** pane and then click **Add**.

For example, enter 10.30.10.0 in the Address field, 255.255.255.0 in the Net Mask field, 10.97.0.1 in the Next Hop Router field.

In this example subnet 10.30.10.0 is downstream of the CPE.

Offering an IP address to the far end using interface add

- 1** Create the IP interface
 - a** Right-click the device, select **Manage IP**.
The **IP Configuration Manager** dialog appears.
 - b** Select the **IP Interface** tab, and then click **Add**.
The **Add IP Interface** dialog appears.
 - c** Select a MLPPP Bond group in the Physical field. And enter values for the necessary fields. And then click **Add**.
For example, enter 10.97.0.1 to the IP address field.
- 2** The IP interfaces on the system are listed in the **Ip Configuration Manager** dialog > **IP Interface** window.

- 3 Offer the far end IAD an IP address by updating the **ip-interface-record**
 - a Select the MLPPP interface in the **IP Interface** window, and click **Modify**.

The **Modify Ip Logical Configuration** dialog appears.

- b Click **Data Forwarding Configuration** in the tree view.

The **Data Forwarding Configuration** window appears.

- c Enter an IP address in the Destination Address field, and then click **Add**.

For example, enter 10.97.0.2 to the Destination Address field.

- 4 Static routes can be added for any subnets downstream of the CPE as needed.

Configuring RPR ports

- 1 From the tree view, expand the GigaMux card and then expand the physical interfaces.
- 2 Right-click a RPR physical interface and select **Modify**. The **Modify Ethernet Physical Port Configuration** dialog box appears.
- 3 Configure the settings for the RPR physical ports.

In RPR ring topologies, two physical ports on the GigE cards are used as the single logical RPR ring port. For redundant GigE cards, including as the two GigE cards used in the RPR uplink node, the physical ports labeled port 1 on the redundant cards form the single logical RPR port. For non-redundant GigE cards, the ports labeled port 1 and port 2 on the single GigE card form the single logical RPR port.

In RPR configurations, the following logical interfaces are used:

- interface 1-1-1-0 /ethernetcsmacd uses the first physical port labeled 10/100 for the 10/100 Ethernet physical interface.
- interface 1-1-1-0/rpr uses the two physical ports assigned to the logical RPR port.

In redundant GigE card configurations, the physical ports labeled port 1 on the redundant cards form the single logical RPR port. In non-redundant GigE card configurations, the physical ports labeled port 1 and port 2 on the same card form the single logical RPR port.

- interface 1-1-3-0 is assigned to physical port 2 in redundant GigE card configurations for upstream or subtended GigE connections.

To display the IP interfaces, click **IP Interfaces**.

To display RPR configuration options, click **RPR Configuration**.

To display RPR span status, click **RPR span**.

To display RPR topology, click **RPR Topo Image**.

For details on the settings, see the online help.

Configuring GigaMux ports

- 1 From the tree view, expand the RPR-GiGE card and then expand the physical interfaces.
- 2 Right-click a GigaMux physical interface and select **Modify**. The **Modify Port Configuration** dialog box appears.
- 3 Configure the settings for the GigaMux physical ports.

After completing the configuration changes, click **Modify** to apply the changes. Click **Reset** return to the default settings. Click **Close** to exit the dialog box.

For details on the settings, see the online help.

Configuring Talk Battery Disconnect on the POTS port

The talk battery disconnect feature provides a mechanism through the use of the **maintenance** setting in the POTS port **Admin Status** field to isolate both tip and ring on POTS ports from the rest of the analog circuitry with a mechanically open circuit cutoff. The mechanical open circuit cutoff provides high impedance on the circuit. In this state there will be no battery voltage applied to the line.

The **maintenance** setting is supported on the following POTS and ADSL/POTS cards's **Admin Status** field:

- MALC-ADSL+POTS-BCM-48A-RNG-2S
- MALC-ADSL+POTS-PKT-BCM-48A-2S
- MALC-ADSL+POTS-PKT-BCM-48B-2S
- MALC-ADSL+POTS-PKT-48A/M-2S
- MALC-ADSL+POTS-TDM-48A/M-2S
- MALC-POTS-EBS-TDM/PKT-24
- MALC-POTS-GBL-TDM/PKT-24

- MALC-POTS-TDM/PKT-48

To change the POTS port **Admin Status** field to maintenance, use the **Modify Pots Physical Port Configuration** dialog:

- 1 Right-click a POTS port, select **Modify**.
The **Modify Pots Physical Port Configuration** dialog appears.
- 2 Click **Status**.
The **Status** window appears.
- 3 Select Maintenance in the **Admin Status** drop-down menu.

SFP/XFP Information

Viewing SFP/XFP Info

NetHorizon supports viewing SFP/XFP info for the device through the SFP/XFP Info dialog.

- 1 Right-click the desired device and select View SFP/XFP Info.
The **SFP/XFP Info** dialog box appears with a list of all the ports with the SFP/XFP along with the Vendor Name, Vendor Oui, Part Number, Revision Level, Serial Number, DateCode, SFP GigE Compliance Code, Connector Type, Transceiver Type, Extended Identifier, Encoded Algorithm, SFP FC Link Length, SFP FC Tx Technology, SFP FC Tx Media, SFP FC Speed, 9 To 125mm Length Km, 9 To 125mm Length 100m, 50 To 125mm Length 10m, 62.5 To 125mm Length 10m, Nominal Bit Rate, Upper Bit Rate Margin %, Lower Bit Rate Margin %, Lower Bit Rate Margin %, and Copper Link Length.
- 2 To export data, select the desired port and click **Export Data**.
The Data Export Dialog appears.
- 3 Specify the desired file format, Tab or CSV. And select a folder to export the file to.
- 4 After finishing the configuration, click **Export**.
- 5 After finishing, click **Close** to exit the **SFP/XFP Info** dialog.

GPON configuration

Topics:

[Configure GPON OLT ports, page 203](#)

[Configure GPON ONU/ONT, page 203](#)

[Configure GPON type B redundancy](#)

[Activate ONT/ONUs by assigning serial number, page 207](#)

[Change ONT/ONU serial number format \(Hexa-decimal or Decimal\), page 208](#)

[Display ONT/ONU MAC address, page 208](#)

[Received Signal Strength Indication \(RSSI\) and Digital Diagnostic Monitoring \(DDM\), page 209](#)

[GPON High and Low Receive Power Threshold Alarms, page 210](#)

[Configure GPON ONT/ONU GEM Ports, page 211](#)

[Bandwidth allocation, page 216](#)

[Enable ONT/ONU web interface, page 220](#)

[View SFP presence, page 220](#)

[Rogue ONU detection and rogue ONU alarms, page 221](#)

Configure GPON OLT ports

Modifying GPON OLT ports

- 1 From the tree view, expand the GPON card and then expand the physical interfaces.

Right-click a GPON physical interface and select **Modify**. The **Modify GPON OLT Port Physical Configuration** dialog box appears.

- 2 Select the different panel to configure the settings for the GPON OLT physical ports.
- 3 After completing the configuration changes, click **Modify** to apply the changes. Click **Reset** return to the default settings. Click **Close** to exit the dialog box.

For details on the settings, see the online help.

Configure GPON ONU/ONT

This procedure describes how to configure the GPON ONT/ONUs.

To configure GPON ONT/ONUs:

- 1 From the ZMS tree, locate the desired ONT/ONU. ONT/ONUs are displayed under the GPON OLT containers.
- 2 Right-click the desired ONT/ONU and select **Modify**.
The **Modify GponOnu Physical Configuration** dialog appears.
- 3 Change the desired configuration options.

- 4 After completing the configuration changes, click **Modify** to apply the changes. Click **Reset** return to the default settings. Click **Close** to exit the dialog box.

For details on the settings, see the online help.

Configure GPON type B redundancy

The MXK supports GPON type B redundancy as specified in the ITU-T G984.1 standards specification.

Type B GPON redundancy doubles both the OLT ports on the GPON line card and the optical fiber between the OLT ports and the optical splitter which is closest to the OLTs. You must use a splitter with two input/output ports on the OLT side. Outages on fiber from the OLT to the first splitter can be recovered from; With Type B redundancy there is no redundancy from the splitter to the ONT.

With Zhone's GPON type B redundancy, a GPON redundancy group can have two GPON OLT ports and the two GPON OLT ports must be on different GPON line cards. The ports can be on a 4 port or 8 port GPON line card. So even though the cards themselves are not redundant, their ports may be. Two 4 port GPON line cards can provide redundancy for a single 8 port GPON line card. Since it is port level redundancy and not card level redundancy, the port numbers on one card do not need to match the port number on the second card.

A single GPON OLT port cannot be configured in two groups at the same time.

When the GPON OLT ports in a GPON redundancy group are added, the active and standby port are based on whether they are added as a primary or secondary interface in the **Manage Line Redundancy** screen. If you reboot the MXK system (or reboot both cards which have the redundant ports), the OLT port which comes up first and is able to pass traffic will be the active port.

In a redundancy group one OLT port is always assigned as active and the other standby. If an active OLT port fails, the standby takes over and becomes active. Note that OLT redundancy is non-revertive; that is, a previously active OLT port which has failed does not become active when the reason for the failover is resolved. The current active port will stay active until that port/line fails, then the standby (if the initial issue was resolved) will once again become the active port.

When a standby port is added to the redundancy group and comes up, the card with the active port copies over the configuration database and routing tables to the standby OLT port on the second card. As configuration changes are made to the active port, the standby port is automatically updated.

Configuring GPON line redundancy

- 1 Add line redundancy by right-clicking an MXK and selecting **Manage Line Redundancy**.

The **Line Redundancy Dialog** screen appears.

- 2 Click **Add**.
- 3 Browse to and select a Primary Physical.
- 4 Click **OK**.
- 5 Browse to and select a Secondary Physical.
- 6 Click **OK**.
- 7 Click **Add**.
- 8 The redundancy lines will appear as a pair in the Redundant Line Pairs screen.

The line redundancy does not change the **Manage Bridge Logicals** display. The name of the bridge interface is taken from the slot in which the line card resides when the bridge interface is initially created, however this name does not change as the active port (and therefore the card on which the active port resides) changes.

Removing a redundant OLT port

Redundancy pairs (or groups) may be deleted. However, the pair can not be deleted if the secondary OLT is active.

To resolve downed ports which are on the primary port, resolve the problem with the port (whether downed link or card issue). Resolving the problem can include replacing the card with a new card. When the new card comes up, the redundancy will be reestablished.

- 1 Right-click an MXK and select **Manage Line Redundancy**.

The **Line Redundancy Dialog** screen appears.

- 2 Highlight the redundant pair you want to remove.
- 3 Click **Delete**.
- 4 Confirm that you want to delete the pair.

Removing redundancy may take a few moments.

Switchover from active to standby GPON OLT port

A switchover from active and standby GPON OLT port can be done automatically or forced manually by forcing a reset of the line.

Automatically switched

A switchover can be triggered automatically when:

- Loss of signal from all ONT/ONUs connected to the active GPON OLT port occurs. This could be caused by:
 - The Fiber between the splitter and MXK is down (i.e.the fiber is cut or pulled)
 - Loss of all ONT/ONUs on this GPON OLT port
If one or more ONT/ONUs go down with still a few ONT/ONUs active, it would not indicate a fiber failure between the splitter and MXK, and hence no action is taken by the SLMS software.
 - Loss or damage of splitter
- An SFP for this GPON OLT port is damaged so it does not pass signal or the SFP is removed
- The GPON card is removed or deleted or the card is rebooted

When a switchover happens automatically, it raises an alarm.

Manually switched

A switchover also can be manually switched by the operator by setting the Admin status of the port to Down, then Up in the: **Modify GponOnu Physical Configuration** screen.

GPON redundancy configuration limitations

The following limitations apply to GPON redundancy configurations:

- When a standby port is added, the configuration information is automatically inherited. If a port is configured as standby, the user cannot enter configuration on the port.
- The card which has proposed secondary ports must be a running card.
- You cannot add a secondary OLT port which has any added ONUs/ONTs, whether active or not. The port cannot be provisioned with logical interfaces, whether bridge or IP.

If there are active ONUs/ONTs in a standalone port that is being attempted to added as a standby to a redundancy group, the command is rejected. However, a GPON OLT port with active ONUs/ONTs can be moved into a redundancy group as the primary active port.

- A GPON OLT port may only be a member of one redundancy group.
- A GPON OLT port may only be made redundant with another GPON OLT port.
- The following rules apply to deleting ports from OLT redundancy groups:
 - An active port can never be deleted from the redundancy group. If the active port is the secondary port of the redundancy group, neither port can be removed.

- Only the secondary port of a redundancy group can be deleted (and only when not active).
- The primary port can never be deleted from the redundancy group.
- Upgrades cannot be scheduled on standby ports



Note: If a switchover event is triggered when an upgrade is in progress, the upgrade is re-queued for the ONUs/ONTs that were in progress as well as the ONUs/ONTs that were currently queued.

Activate ONT/ONUs by assigning serial number

The ZMS GUI supports provisioning OLT ports on GPON cards by providing a list of unassigned serial numbers. The OLT port in the Navigation tree lists the number of unassigned serial numbers. By selecting an OLT card in ZMS and right-clicking on it, a pop-up menu appears to provide access to alarms, IP profiles, bridging profiles, statistics, and serial numbers.

By assigning a serial number to an ONT/ONU, this ONT/ONU will be activated. During activation, you can also modify upstream bandwidth and traffic class for ONT/ONU GEM ports, and associate OMCI file or OMCI profile to the ONT/ONU.



Note: MALC only supports OMCI file.
MXK supports OMCI profile.

Activating ONT/ONUs

- 1 To assign a serial number to an ONT/ONU, click on the OLT in the Navigation Tree as, then click on **Assign Serial Numbers** in the pop-up window.
- 2 The **Modify Serial Number Table** window appears.
- 3 Select an ONT/ONU port to assign this serial number to, and enter an ONT IP address and OMCI file.
- 4 Click **Apply**, then **Close**.

Viewing unassigned serial numbers on the MxK

You can view unassigned MxK OLT serial numbers in one window.

- 1 To view unassigned serial numbers, right-click an MxK and select **Assign ONU Serial Numbers**.
The **Unassigned Serial Numbers** dialog box appears.
- 2 To assign a serial number to a device, highlight an unassigned serial number.

- 3 Click the **Assign SN** button.

The **Modify Serial Number Table** dialog box appears.

- 4 Select an ONT/ONU port to assign this serial number to, and enter an ONT/ONU IP address and OMCI file.
- 5 Click **Apply**, then **Close**.

For details on the OMCI file configuration and parameter settings, refer to [Associating the OMCI file when activating the ONT/ONU](#), page 224.

For details on the GEM port upstream bandwidth and traffic class settings, refer to [Modifying GEM port upstream bandwidths and traffic class settings when activating ONT/ONU \(MALC only\)](#), page 213.

For details on the OMCI profile configuration and parameter settings, refer to [Activating ONT/ONU with OMCI profiles](#), page 229. (MXK only)

Change ONT/ONU serial number format (Hexa-decimal or Decimal)

ZMS supports one type of ONT/ONU serial number format displayed or set at a time. It could be either decimal or hexa-decimal.

To switch the ONT/ONU serial number format between decimal and hexa-decimal, use the **UseOnuFsanSN** flag in the *CS.properties* and *NetHorizon.properties*. By default, **UseOnuFsanSN** flag is true in the *CS.properties* and *NetHorizon.properties* files, and all ONT/ONU serial numbers will be displayed and set in hexa-decimal format. For the detail procedure, refer to the *ZMS Administrator's Guide*.

The activated ONT/ONUs are displayed in the navigation tree with their serial numbers. Only the serial number type specified by the **UseOnuFsanSN** flag is displayed.

The ONT Serial No Vendor Specific field in the **Modify GponOnu Physical Configuration** dialog box could be entered as hex or decimal number.

The Serial Number column in the **Modify Serial Number Table** dialog box can be displayed in hex or decimal.

This figures shows the numbers displayed in hex.

Display ONT/ONU MAC address

By default, the ONT MAC address field is not displayed in the **View/Modify GponOnu Physical Configuration** dialog.

The ONT MAC address field can be displayed in the NetHorizon by changing the **ShowOntMacAddress** flag to true in the *NetHorizon.properties* file. By default, this value is set to false. After this change, the ZMS server has to be restarted, and the NetHorizon client has to log back in to make the changes take effect.

The ONT MAC address field will display the MAC address of the connected ONTs. The calculations of the MAC addresses are different for the ONT

types. In case the ONT MAC Address field reported wrong MAC address, you can always force it matches to the ONT types by selecting the ONT type in the Device Type field in the **Modify GponOnu Physical Configuration** dialog. You can find the correct MAC address and the ONT type in the CPE WEB UI.



Note: Make sure you selected correct ONT models in the Device Type field. The Device Type field will force the ONT MAC Address field to change according to your selection.

By setting **ShowOntMacAddress** flag to true in the *NetHorizon.properties* file, the Device Type field will also be shown in the **View/Modify GponOnu Physical Configuration** dialog. The Device Type field has three radio buttons: 420x/421x, 24xx/26xx/422x/424x/9xxx, and Other. If users selected Device Type as 420x/421x, ONU MAC address is increased by 1. If users selected Device Type as other, ONU MAC address will not be calculated. After selected Device Type, click **Modify** to make the changes take effect.

For the detail step-by-step procedure of how to set **ShowOntMacAddress** flag to true in the *NetHorizon.properties* file, refer to the *ZMS Administrator's Guide*.

Received Signal Strength Indication (RSSI) and Digital Diagnostic Monitoring (DDM)

Viewing the received power on an OLT from an ONT/ONU

Received Signal Strength Indication (RSSI) is the capability of a SFP by which the SFP reads the strength of the signal received at the OLT from an ONT/ONU.

Display the received power of the SFP per ONT/ONU with the **View/ Modify GponOnu Physical Configuration** window:

- 1 From the ZMS tree, locate the desired ONT/ONU. ONT/ONUs are displayed under the GPON OLT containers.
- 2 Right-click the desired ONT/ONU and select **View** or **Modify**.
The **View / Modify GponOnu Physical Configuration** dialog appears.
- 3 Select **ONU Status** from the tree view.
The **SFP Power (dB)** field in the ONU Status window shows the value.

Viewing the transmit parameters on an OLT

With Digital Diagnostic Monitoring (DDM) function, the SFP optical transceiver with RSSI, measures the transceiver temperature, transceiver supply voltage, Tx Bias current, and Tx output power parameters on an OLT,

and also reports an End of Line status which alerts end-users when particular transmit parameters are outside of the normal range.

View DDM on the GPON OLT card with the **View / Modify Gpon Olt Physical Configuration** dialogs.

- 1 From the tree view, expand the GPON card and then expand the physical interfaces.
- 2 Right-click a GPON physical interface and select **View** or **Modify**. The **View/ Modify GPON OLT Port Physical Configuration** dialog boxes appears.
- 3 Select **Digital Diagnostic Monitoring** from the tree view to view the DDM transmit parameters on the GPON OLT physical port.

Temperature — Internally measured Transceiver Temperature of the GPON SFP in Celsius.

Voltage — Internally measured Transceiver Supply Voltage of the GPON SFP in Volts.

Tx Bias Current — Measured Tx Bias current per GPON SFP in Milli Amperes.

Tx Power — Measured Tx Output Power of the GPON SFP in dB.

Status — When the End Of Life (EOL) Alarm bit is set an alarm will be raised. Alarm is raised when the SFP reaches the end of life which is about 150% of original current. Alarm will be cleared when the SFP is connected. The alarm severity level is Major.

Configured Onu Count — Retrieve total count of configured GPON ONUs per GPON OLT port.

Active Onu Count — Retrieve total count of active ONUs on a per GPON OLT port..

GPON High and Low Receive Power Threshold Alarms

By default, the MXK will trigger a local alarm, and send trap to ZMS when GPON high/low receive power thresholds are crossed for ONU received power on the upstream. The default value of the High threshold is -10 dbm. The default value of the Low threshold is -30 dbm. Users can change the default threshold values, and choose the upstream received power monitoring mode as desired.

The **Rx Power Monitoring**, **Rx Power High Threshold**, and **Rx Power Low Threshold** fields are added into **Modify GponOnu Physical Configuration** dialog> **Configuration** window per-ONU basis.

Configuring GPON high and low received power threshold alarms

- 1 View the upstream received power level on an ONU.

From the ZMS tree, locate the desired ONT/ONU. ONT/ONUs are displayed under the GPON OLT containers.

- a Right-click the desired ONT/ONU and select **View** or **Modify**.

The **View / Modify GponOnu Physical Configuration** dialog appears.

- b Select **ONU Status** from the tree view.

The **Rx Power (dB)** field in the **ONU Status** window shows the value.

- 2 Configure the upstream ONU received power monitoring mode and threshold values.

- a Click Configuration menu item in the **View / Modify GponOnu Physical Configuration** dialog.

- b Configure the following fields in the dialog as desired:

Rx Power Monitoring

Block on Error: Monitor ONU Receive Power Level. When ONU Receive Power Level crosses either the High or Low thresholds, trigger a local alarm, send trap to ZMS, disable ONT ranging and set ONT line status to DSA.

Monitor Only: Monitor ONU Receive Power Level. When ONU Receive Power Level crosses either the High or Low thresholds, trigger a local alarm, and send trap to ZMS. This is default value.

Disabled: Disable the received power threshold alarm

Rx Power High Threshold

Upstream receive power high threshold value, in the unit of dbm, default value is -10.

Rx Power Low Threshold

Upstream receive power low threshold value, in the unit of dbm, default value is -30.

- c Click **Modify** to save the configuration.

Configure GPON ONT/ONU GEM Ports

Delivering integrated and combined services such as IPTV, video on demand, data, voice over IP etc. requires enough network resource. To maintain control and be able to prioritize traffic in service-based order, Zhone OLT line card supports GPON Encapsulation Method (GEM) ports on ONT/ONUs.

The following procedure describes how to configure the GPON ONT/ONU GEM port.

- [Configuring GEM port general settings, page 212](#)
- [Modifying GEM port upstream bandwidths and traffic class settings when activating ONT/ONU \(MALC only\), page 213](#)
- [Modifying the alloc-ID profile on the static GEM port \(MALC only\), page 213](#)
- [Creating a dynamic GEM port with a GEM traffic profile \(Smart OMCI on MXK only\), page 214](#)

Configuring GEM port general settings

To configure general settings on GPON ONT/ONU GEM ports:

- 1 From the ZMS tree, locate the desired ONT/ONU GEM port. GEM ports are displayed under the GPON ONT/ONU containers.
- 2 Right-click the desired GEM port and select **Modify**.
The **Modify GponPort Physical Configuration** dialog appears.
- 3 Click the Configuration entry to select desired configuration options. Port settings can be multicast or not, encrypted or not (default value) on bidirectional, up direction or down direction.
- 4 Click the Traffic Profile entry to modify the GPON traffic profile of the GEM port.

If you select **Use Existing Gpon Traffic Profile**, you can click the **Gpon Traffic Profile Index** browse button and select an existing GPON traffic profile that stored in this device. The settings in the GPON traffic profile will be displayed with the GTP index in the **Gpon Traffic Profile Index** field.

If you select **Use Gpon Traffic Profile Template**, you can click the **Gpon Traffic Template** browse button and select a GPON traffic profile template that stored in this ZMS server.

When modifying a GTP index of a GEM port, the CAC validation is performed.

It compares the new GTP with the GTP assigned on the GEM port. The GTP index modification is rejected when the following condition are met:

- If the DBA is disabled on both GTP profiles, and Traffic Class is changed.
- If the status of DBA is changed.

Then the CAC bandwidth validation is performed. The total available bandwidth is recalculated on the OLT interface (GPON physical port) using the newly assigned GTP index. If the CAC validation fails, the GTP index modification is rejected.

- 5 Click the Status entry to modify the GEM port administrative status and operational status.

After completing the configuration changes, click **Modify** to apply the changes. Click **Reset** return to the default settings. Click **Close** to exit the dialog box.

For details on the settings, see the online help.

Modifying GEM port upstream bandwidths and traffic class settings when activating ONT/ONU (MALC only)

The upstream bandwidths and traffic class can be modified for multiple GEM ports in the **Modify Serial Number Table** dialog box when activating the ONT/ONU. However the compensation mode (compensated) can only be modified in the **Modify Gpon AllocId** dialog box.

The following example activate ONT/ONU 1-6-1-2 with serial number 266999, and changes upstream bandwidths for GEM ports 502 and 902 to 1024 Kbps and 1536 Kbps from the default values respectively:

- 1 From the ZMS tree view, expand the MALC device and then expand the GPON card OLT level. View all the free ONT/ONUs, serial numbers under the OLT 1-6-1:
- 2 Right-click the OLT port, select **Assign Serial Numbers**.
The **Modify Serial Number Table** dialog appears.
- 3 Select 1-6-1-2 from the ONT/ONU Port pull down menu, associate it with serial number 266999. And select upstream bandwidths for GEM ports 502 and 902 to 1024 Kbps and 1536 Kbps respectively.
- 4 Click **Apply** to activate ONT 1-6-1-2 with the modified upstream bandwidth values.

Modifying the alloc-ID profile on the static GEM port (MALC only)

With static GEM ports, each ONT/ONU has been assigned a fix set of three GEM ports. And each GEM port has a GPON Alloc ID profile. In the GPON alloc-ID profile, you can specify bandwidth, traffic class, and compensation mode for the upstream traffic of the GEM port.

Note that the zNID-GPON-4200 ONT/ONU only requires one GEM port (5XX) because it can perform traffic shaping on a per VLAN basis inside of that single GEM port.

The GPON alloc-ID profile is associated with each static GEM port. In the GPON alloc-ID profile, the users can specify bandwidth, traffic class, and compensation mode for the upstream traffic of the GEM port.

To view or modify the GEM port settings in the alloc-ID profile, perform the following tasks:

- 1 Right-click a static GEM port, and select **GPON Alloc**.

The **Modify Gpon AllocId** dialog box appears.

In the **Modify Gpon AllocId** dialog box, specify the desired values for the following fields:

Guaranteed Bandwidth — The upstream bandwidth for the GEM port. The value is multiple of 512 kbps. By default, the value is 512 kbps.

Traffic Class — The upstream traffic class value is UBR (Unspecified Bit Rate) or CBR (Constant Bit Rate).

Compensated — Check or uncheck True for CBR compensation mode.

- 2 Click **Modify**.

Creating a dynamic GEM port with a GEM traffic profile (Smart OMCI on MXK only)

Dynamic GEM ports can be created during **bridge add** and **host add** operations. And it can be automatically deleted during **bridge delete** and **host delete** operations.

When creating a dynamic GEM port, a GPON Traffic Profile (GTP) must be selected, otherwise an error message will appear. The GPON traffic profile defines the upstream bandwidths, traffic class, and compensation mode for the GEM ports.

If a GTP template is selected for a GEM port, device searches all the existing GTP to see if a matching profile exists. If it does, the index of the matching GTP will be used to associated with this GEM port. If it does not, the device will automatically create a corresponding GPON traffic profile and assign a GTP index to it.

- 1 Create a bridge with GEM port, and apply a GPON traffic profile to it.
 - a Expand device> GPON line card> OLT port> ONT/ONU port level in the tree view, right-click this ONT/ONU port and select **Managing Bridge**. The **Manage Bridge Logical** window appears.
 - b In the **Manage Bridge Logical** window, click **Add**.
The **Bridge Logical on Device** dialog box appears.
 - c In the dialog box, specify the following fields and other desired settings.
 - In the **Select Physical Ports** pane, expand the tree view and select an ONT/ONU port.
 - And then in the **GPON Port ID** drop-down menu select a GPON port ID. GPON port ID is in the range of 5xx to 35xx.
By specifying the ONT/ONU port ID and GPON Port ID, it creates the GEM port ID.

GEM port ID= GPON Port ID + ONT/ONU Port ID.

For example, after you selected ONU 1: 1-13-1-1 (i.e.ONT/ONU port ID 1), and selected GPON Port ID 5xx, then the newly created GEM port ID will be 501.

- At last, in the Traffic Info pane, select whether you want to use an existing GPON traffic profile or a GPON traffic profile template.

If you select **Use Existing Gpon Traffic Profile**, you can click the **Gpon Traffic Profile Index** browse button and select an existing GPON traffic profile.

If you select **Use Gpon Traffic Profile Template**, you can click the **Gpon Traffic Template** browse button and select a GPON traffic profile template.

- d Click **Add** to create a GEM port on the ONT/ONU during bridge-add operation.
- 2** Or you can create a GEM port during host add operation, and apply a GPON traffic profile to the GEM port.
- a Expand device > GPON line card> OLT port> ONT/ONU port level in the tree view, right-click this ONT/ONU port and select **Managing IP**. The **IP Configuration Manager** window appears.
 - b In the **IP Configuration Manager** window, click **Subscriber Hosts** tab.
 - c Click **Add**. The **IP Subscriber Hosts on Device** dialog box appears.
 - d In the dialog box, specify the following fields and other desired settings:
 - In the **Select Physical Ports** pane, expand the tree view and select an ONT/ONU port.
 - And then in the **GPON Port ID** drop-down menu select a GPON port ID.
 - At last, in the VCL Info pane, select whether you want to use an existing GPON traffic profile or a GPON traffic profile template.

If you select **Use Existing Gpon Traffic Profile**, you can click the **Gpon Traffic Profile Index** browse button and select an existing GPON traffic profile.

If you select **Use Gpon Traffic Profile Template**, you can click the **Gpon Traffic Template** browse button and select a GPON traffic profile template that stored in this ZMS server.
 - e Click **Add** to create a GEM port on the ONT/ONU during host-add operation.

Related Topics:

To create the GPON traffic profile, use the **Modify Device Configuration** dialog box. For details refer to [Creating a GPON Traffic Profile on page 216](#).

To change the GPON traffic profile index of a GEM port, use the **Modify GponPort Physical Configuration** dialog box. For details refer to [Configuring GEM port general settings on page 212](#).

Bandwidth allocation

The following procedure describes how to configure the bandwidth allocation on the GPON physical port.

- [Configure GPON traffic profile, page 216](#)
- [Dynamic Bandwidth Allocation \(DBA\), page 217](#)
- [Connection Admission Control \(CAC\) validation during creation of bridge/host on the ONT/ONU GEM port, page 219](#)

Configure GPON traffic profile

The GEM port uplink parameter such as DBA enabled or disabled, upstream bandwidths, traffic class, and compensation mode etc. are defined in the GPON Traffic Profiles (GTP).

Each GEM port has one GPON traffic profile.

One GPON traffic profile could be applied to multiple GEM ports. GPON traffic profile can be created and shared in a device. If you want to share the GTP with all the devices in the same ZMS server, you can create a GTP template.

For the detail DBA configuration on the GPON traffic profile, refer to section [Dynamic Bandwidth Allocation \(DBA\) on page 217](#).

The profile validation and CAC validation are performed during the GPON traffic profile configuration.

If a GTP template is selected for a GEM port, device searches all the existing GTP to see if a matching profile exists. If it does, the index of the matching GTP will be used to associated with this GEM port. If it does not, the device will automatically create a corresponding GPON traffic profile and assign a GTP index to it.

Creating a GPON Traffic Profile

Create a GPON traffic profile or GPON traffic profile template:

- 1 To create a GPON traffic profile on a device and generate a GPON traffic profile index, perform the following task:
 - a Right-click an MXK device and select **Modify**. The **Modify Device Configuration** dialog box appears.
 - b Click **Gpon Traffic Profiles**, the **GPON Traffic Profiles** window appears.

All the existing GPON traffic profiles appear in the window.

c Click **Add**, the **Add GPON Traffic Profile** dialog box appears.

d In the **Add Gpon Traffic Profile** dialog box, specify the values.

For details on the settings, see the online help.

e Click **Add**.

2 To create a GPON traffic profile template in the ZMS server, perform the following task:

a Select **Tools > Configure Templates**.

The **Template Configuration** dialog box appears.

b Right click **Gpon Traffic Profile Templates** and select **Add**.

The **Add Gpon Traffic Profile** dialog box appears.

c In the **Add Gpon Traffic Profile** dialog box, specify the values for the following template related fields:

Template Name — The name of the template, it will appear in the template selection dialog boxes.

Description — Brief description of the template.

Name — More information for this template

For details on the GPON traffic profile settings, see the online help.

d When finished, click **Close**.

Dynamic Bandwidth Allocation (DBA)

Dynamic Bandwidth Allocation (DBA) is specified in the ITU standards 984.3. This feature is used to grant upstream bandwidth to ONT/ONUs based on their demand and service-level agreement. The OLT will grant ONT/ONUs an increase in their slot time for more bandwidth while granting a reduced slot time to others. Through DBA, a GPON link can be oversubscribed for upstream traffic, and improve bandwidth usage efficiency.

There are two types of DBA, Status Reporting (SR) and Non-Status Reporting (NSR):

- **SR:** The ONT/ONU provides the bandwidth status information as part of the upstream traffic message. SR is specified in the Dynamic Bandwidth Report upstream (DBRu).
- **NSR:** NSR is the non-status reporting option where the OLT calculates the available bandwidth. The allocation is based on monitoring ONT/ONU's bandwidth usage compared to the allocated bandwidth.

DBA type is not selected by users. The system automatically chooses SR or NSR type. The system first attempts an SR connection, if the SR connection is not able to be established, the NSR connection is used. If SR is used to

determine the DBA type, and subsequently the ONT/ONU sends error DBRu, after three consecutive DBRu received, the system switch to NSR. The only way to force back to SR is to reboot the ONT/ONU.

This section provides the following topics:

- [Configuring DBA in the GPON traffic profile, page 218](#)
- [Viewing the bandwidth allocation on a GPON physical port, page 219](#)
- [Viewing the allocation Ids information on a GPON physical port, page 219](#)

Configuring DBA in the GPON traffic profile

User can enable or disable DBA and configure the DBA bandwidth in the **Add/Modify GPON Traffic Profile** dialog boxes.

User can configure both guaranteed (i.e. Fixed Upstream UBR Bandwidth, Fixed Upstream CBR Bandwidth, and Assured Upstream Bandwidth) and non-guaranteed DBA bandwidth (i.e. Maximum Upstream Bandwidth). The non-guaranteed DBA bandwidth is always the UBR type of traffic and is non-compensated.

To configure the DBA related parameters in a GPON traffic profile, perform the following task:

- 1** Right-click an MXK device and select **Modify**. The **Modify Device Configuration** dialog box appears.
- 2** Click **Gpon Traffic Profiles**, the **GPON Traffic Profiles** window appears.
All the existing GPON traffic profiles appear in the window.
- 3** Click **Add**, the **Add GPON Traffic Profile** dialog box appears.
- 4** In the **Add Gpon Traffic Profile** dialog box, specify values for the following DBA related GPON GEM ports uplink parameters:

Profile Index

Compensated

Shared

Dynamic Bandwidth Allocation

Fixed Upstream UBR Bandwidth

Fixed Upstream CBR Bandwidth

Assured Upstream Bandwidth

Maximum Upstream Bandwidth

Extra Upstream Bandwidth Type

For details on the settings, see the online help.

- 5 Click **Add**.

Viewing the bandwidth allocation on a GPON physical port

View the bandwidth allocation on the GPON physical port in the **View/Modify Gpon Olt Physical Configuration** dialog boxes.

To view the bandwidth allocation on an GPON physical port, perform the following task:

- 1 Right-click an OLT interface and select **View** or **Modify**. The **View Gpon Olt Physical Configuration** or **Modify Gpon Olt Physical Configuration** dialog box appears.
- 2 Click **Dynamic Bandwidth Allocation**, the **Dynamic Bandwidth Allocation** window appears.

For details on the settings, see the online help.

Viewing the allocation Ids information on a GPON physical port

View the Alloc-Ids information on the GPON physical port in the **View/Modify Gpon Olt Physical Configuration** dialog boxes.

To open the dialog boxes, perform the following task:

- 1 Right-click an OLT interface and select **View/ Modify**. The **View Gpon Olt Physical Configuration** or **Modify Gpon Olt Physical Configuration** dialog box appears.
- 2 Click **Allocation Ids**, the **Allocation Ids** window appears.

For details on the settings, see the online help.

Connection Admission Control (CAC) validation during creation of bridge/host on the ONT/ONU GEM port

When using the **bridge add** or **host add** window to add a GEM port, or add a bridge/host to an existing GEM port with different VLAN, the Connection Admission Control (CAC) is performed.

If the creation of bridge/host is rejected by CAC validation, ZMS shows the message as "Unable to create Gpon Port ." along with one of the following CAC failure reasons:

"Device version does not support CAC"

"GPON CAC request approved"

"GPON CAC request has not been performed"

"Internal error. Bad pointer or index value parameter to a GPON CAC procedure call"

"Internal error. Failed to look up a config record (OLT, ONU, traffic profile, etc)"

"Internal error. Invalid value was found inside a profile so a switch statement failed"

"Each ONU supports a limited number of GEM ports"

"Each OLT supports a limited number of allocIds"

"Each OLT supports a limited number of DBA-enabled allocIds"

"There is no available total bandwidth"

"There is no available CBR bandwidth"

"The change was not allowed because the new traffic profile has a different traffic class"

"The change was not allowed because the new traffic profile has a different DBA Enabled status"

Enable ONT/ONU web interface

ZMS also provides an ONT/ONU IP address field. Providing the IP address of the ONT/ONU enables the **MANAGE ONT** menu choice on the ONT/ONU in the Navigation tree.

Enabling ONT/ONU web interface

- 1 Right-click on the assigned ONT/ONU in the Navigation tree and select Manage ONT.
- 2 ZMS will provide the ONT/ONU (zNID) web interface.

View SFP presence

The Small Form Factor Pluggable (SFP) optics is used on the GE and FE/GE uplink cards and on the Active Ethernet line card. Using an SFP gives greater flexibility to the user and allows the users to chose from many available optical options. This feature adds the ability for the users to query an installed SFP for status and diagnostics.

ZMS now supports SFP attributes in the **Modify Ethernet Physical Port Configuration** and **View Ethernet Physical Port Configuration** dialog boxes. If there is no SFP configured on a specific ethernet port, all SFP panels will be removed from the dialog.

Viewing SFP presence

To view the SFP information, perform the following tasks:

- 1 Right-click an ethernet port which is configured with SFP, and select **Modify**.
- 2 The **Modify Ethernet Physical Port Configuration** dialog box appears with SFP tabs.

For details on the settings, see the online help.

Rogue ONU detection and rogue ONU alarms

A rogue ONU is an ONU that transmits outside of its allocated bandwidth map. It can cause disruption to multiple subscribers or to all subscribers on a PON. Zhone provides versatile ways to detect a rogue ONU that is present on the PON and/or shut it down. That saves the other subscribers from experiencing any service issues.

To detect and/or shutdown a rogue ONU, use the following detection modes per OLT basis:

1. Periodical background process detection mode

Periodical background process detection mode can detect certain cases of rogue ONUs, but will not disable rogue ONUs. If a rogue ONU has been detected on the OLT, an OLT-level alarm “**OLT Status Rogue (OLT= \$\$ifAlias\$\$)**” is raised.

2. Rogue RSSI detection mode

Rogue RSSI detection mode can detect and disable rogue ONUs by using the RSSI measurement on ONUs. If a rogue ONU has been detected on an OLT, an OLT-level alarm “**OLT Status Rogue ONU Rssi (OLT= \$\$ifAlias\$\$)**” is raised. And then this rogue ONU will be identified, isolated, and disabled. An ONU-level alarm “**Rogue ONU (ONU= \$\$ifAlias\$\$)**” will be raised too.

3. Auto rogue RSSI detection mode

Auto rogue RSSI detection mode normally functions as disabled, it will be switched to the rogue RSSI detection mode only under certain circumstances.

All three kinds of rogue ONU alarms have severity levels as minor.



Note: As a rule we'd only want to use either **Disabled** or **Auto Rssi** mode under normal conditions, although we might want to set either **Rogue Rssi** or **Background Process** if we suspect a rogue ONU for some reasons that is not detected or not isolated by **Auto Rssi** mode.

Configuring ONU Detection

Users can configure the ONU detection related fields in the **Modify Gpon Olt Physical Configuration** dialog > **Rogue Onu** window:

- 1 Expand the GPON card in the tree view, right-click an OLT port, and then select **Modify**.

The **Modify Gpon Olt Physical Configuration** dialog appears.

- 2 Select **Rogue Onu**.

The **Rogue Onu** window appears.

- 3 The **Rogue Onu** window contains three rogue ONU detection related attributes:

- **Rogue Onu Detection**

Select a rogue ONU detection mode from this field:

Disable: Disable all the rogue ONU detection mode.

Background Process: Enable background process detection. When a rogue transmission is detected, trigger a local alarm and send a trap to ZMS. Certain rogue behaviors can only be detected by running the periodical background process detection mode on an OLT. This mode only detects the condition, rather than trying to disable it.

Rogue Rssi: Enable rogue RSSI detection. When a rogue ONU RSSI measurement crosses the rogue-onu-rx-power-threshold, an attempt is made to isolate the rogue ONU. If successful, disable the rogue ONU. Trigger a local alarm and send a trap to ZMS.



Caution: The rogue RSSI measurement is a semi-invasive mode. During the activation of the RSSI measurement on an OLT port it is not allowed to provision Alloc_IDs or to activate ONUs under that OLT port.

If you want to provision Alloc_IDs (by creating bridges/hosts/interfaces on ONU Gemparts), and activate ONUs (by assigning serial numbers to ONUs ports), you must change the rogue-onu-detection mode from rogue RSSI to auto RSSI mode or disabled, after clearing any disabled ONUs.

Auto Rssi: Enable auto RSSI detection. In this mode, it normally stays as disabled, it will switch to the rogue RSSI detection mode 1) if more than half the active ONUs go down within a brief interval, 2) or if BIP errors exceed threshold on any ONU. Note that the second case is a detect only measurement, no attempt to disable the rogue ONU will be automatically performed.

- **Rogue Onu Detection Frequency** (1-60) (in seconds)

How often to run a detection after enabling the detection. The default value is 10 seconds.

- **Rogue Onu Power Threshold**

Upstream Receive Power High Threshold value for detecting rogue ONU, in the unit of dbm.

RSSI upstream received power is measured on an unused ONU, which should measure zero, if the measurement exceeds the threshold, an alarm is reported and isolation is attempted. This is ignored in background process mode. The default value is 30 dbm.

4 Click **Modify** to save the configuration.

GPON OMCI configuration

Topics:

[OMCI file \(MALC only\), page 223](#)

[Smart OMCI - OMCI profiles \(MXK only\), page 225](#)

[Unified Service Provisioning - CPE profiles \(MXK, MXK 194/198 only\), page 244](#)

[Manage ONT/ONU with OMCI \(MXK, MXK 194/198 only\), page 232](#)

[OMCI Statistics \(MXK, MXK 194/198 only\), page 243](#)

Related topics:

[Configure GPON OLT ports, page 203](#)

[Configure GPON ONU/ONT, page 203](#)

[Activate ONT/ONUs by assigning serial number, page 207](#)

[Configure GPON ONT/ONU GEM Ports, page 211](#)

OMCI file (MALC only)

The OMCI file (a standards-based ONT Management and Control Interface file) is supplied by Zhone Technologies for use with the OMCI-enabled ONT/ONUs.

The OMCI file contains the commands used to configure the ONT/ONUs that are related to customer premises equipment (CPE) devices.

Prior to associate OMCI file to the ONT/ONU, the OMCI file must be downloaded to the OMCI directory from the server first, and the filename must be entered in the *gpon-olt-onu-config* file.

User can associate OMCI file with an ONT/ONU by these two methods:

- [Associating the OMCI file when activating the ONT/ONU, page 224](#)
- [Associating the OMCI file with an activated ONT/ONU, page 225](#)

Downloading an OMCI file

At first create the OMCI directory, and then download an OMCI file into this directory.

- 1 Create a directory at the root level. The name of the directory must be *omci*.

```
zSH> mkdir /omci
```

- 2 Download the OMCI file to *omci* directory, in this example the OMCI file name is *cigprov_eth3_fxs.txt*.

```
zSH> filedownload 172.16.80.201 pathname/cigprov_eth3_fxs.txt /omci/  
cigprov_eth3_fxs.txt
```

Associating the OMCI file when activating the ONT/ONU

The following example shows how to associate the OMCI file *cigprov_eth3_fxs.txt* with ONT/ONU 1-6-1-1 when activating the ONT/ONU:

- 1 From the ZMS tree view, expand the MALC device and then expand the GPON card OLT level. View all the free ONT/ONUs, serial numbers under the OLT 1-6-1:

- 2 Right-click the OLT port, select **Assign Serial Numbers**.

The **Modify Serial Number Table** dialog appears.

- 3 Select 1-6-1-1 from the ONT/ONU Port pull down menu, associate it with serial number 266999. And input OMCI file name as *cigprov_eth3_fxs.txt*.

The max length for the OMCI filename is 35 bytes (36- terminator)

- 4 Click **Apply** to activate ONT 1-6-1-1 with the associated OMCI file.
- 5 Right-click ONT 1-6-1-1, and select **View**. In the **View GponOnu Physical Configuration** dialog box verify the *Onu Added* and the *OMCI Config Filename*.

Associating the OMCI file with an activated ONT/ONU

The following example shows how to associate the OMCI file *cigprov_eth3_fxs.txt* with an activated ONT/ONU, 1-6-1-1:

- 1 From the ZMS tree view, expand the MALC device and then expand the GPON card ONT /ONU level.
- 2 Right-click ONT 1-6-1-1, and select **Modify**.
The **Modify GponOnu Physical Configuration** dialog box appears.
- 3 Click **Configuration**.
- 4 In the OMCI Configuration Filename field, input *cigprov_eth3_fxs.txt*.
The max length for the OMCI filename is 35 bytes (36- terminator)
- 5 Click **Modify**.

Smart OMCI - OMCI profiles (MXK only)

Topics:

[Configure Smart OMCI on ONU, page 225](#)

[Import and export OMCI profile file, page 230](#)

Configure Smart OMCI on ONU

Generally these are the steps to follow to configure the MXK to be able to manage ONU with Smart OMCI:

- [Creating ME profile, page 225](#)
- [Creating Generic profiles, page 226](#)
- [Creating Specific profiles on OLT level, page 227](#)
- [Creating Specific profiles on ONU level, page 228](#)
- [Activating ONT/ONU with OMCI profiles, page 229](#)

Creating ME profile

Before creating an ME profile, make sure the OMCI ME profile file exists in the ZMS server */tftpboot* directory first.

ME profile is created from the ME profile file. One ME profile is created for each ONT/ONU model.

- 1 To create an ME profile, right-click a device in the tree view, select **Manage ME Profile**. The **Manage ME Profile** dialog box appears.
- 2 Click **Add**. The **Add ME Profile** dialog box appears.
- 3 In the **Add ME Profile** dialog box, specify ME profile name, and the ME profile file name. And then click **Add**.

The newly created ME profile appears in the **Manage ME Profile** dialog box.

- 4 If you want to delete an ME profile, select this ME profile and click **Delete**.

Note that an ME profile can only be removed if it does not have any Generic profiles associated with it, and the associated ONT/ONU (if any) is not activated.

Related topics:

[Downloading files to a single or multiple devices, page 70.](#)

Creating Generic profiles

The Generic profile defines the values of parameters that define service plans. It also contains values of system information. The system parameters, service plan values are entered by the service provider as part of system commissioning.

If the service provider intend to offer 3 different service plans that are supported on 5 different ONT/ONU hardware models, service provider should create 5 ME profiles and 15 Generic profiles in the system.

To create, modify, and view a Generic profile:

- 1 There are two ways to create a Generic profile:

Use the **Add Generic Profile on ME profile** dialog box.

- a Right-click a device in the tree view, select **Manage ME Profile**. The **Manage OMCI ME Profile** dialog box appears.
- b In the **Manage OMCI ME Profiles** dialog box, select an ME profile, and click **Details**. The **ME Details** dialog box appears.
- c In the **ME Details** dialog box, click **Add**. The **Add Generic Profile on ME Profile** dialog box appears.
- d In the **Add Generic Profile on ME Profile** dialog box:

Generic Profile Name — enter a name for the Generic Profile.

Import contents of profile from a file — If you want to import the contents from a file, check this box, and enter the file's name in the **Profile File Name** field. This file must exist in the */tftpboot* directory in the ZMS server

Click **Add**.

The newly created Generic profile appears in the **ME Details** dialog box.

You can also use the **Add Generic Profile on Device** dialog box.

- a Right-click a device in the tree view, select **Manage Generic Profile**. The **Manage OMCI Generic Profile** dialog box appears.

- b** In the **Manage OMCI Generic Profiles** dialog box, click **Add**. The **Add Generic Profile on Device** dialog box appears.
- c** In the **Add Generic Profile on Device** dialog box:

Parent ME Profile Name — select the name of the ME Profile.

Generic Profile Name — enter a name for the Generic Profile that related to the selected ME profile.

Import contents of profile from a file — If you want to import the contents from a file, check this box, and enter the file's name in the **Profile File Name** field. This file must exist in the */tftpboot* directory in the ZMS server

Click **Add**.

The newly created Generic profile appears in the **Manage OMCI Generic Profile** dialog box.

- 2** When a Generic profile is created, no values are assigned to the variables in the profiles. The variables are typically parameters that associated with the specific service plan. For example, voice vlan. The variables can also be parameters that are generic to the system. For example, Softswitch IP address (i.e. the parameter SIP Proxy IP in the following generic profile example).

To assign values to desired variables in the Generic profile, select this Generic profile in the **ME Details** or **Manage OMCI Generic Profile** dialog box, and click **Modify**.

The **Modify Generic Profiles** dialog box appears.

Specify the desired value and then click **Close**.

- 3** To view a Generic profile, select a Generic profile in the **ME Details** dialog box or **Manage OMCI Generic Profile** dialog box, and click **View**. The **Modify Generic Profiles** dialog box appears.
- 4** If you want to delete a Generic profile, select it in the **ME Details** dialog or **Manage OMCI Generic Profiles** dialog and click **Delete**.

Note that a Generic profile can only be removed if it does not have any Specific profiles associated with it, and the associated ONT/ONU (if any) is not activated.

Creating Specific profiles on OLT level

For each end-user, the service provider creates a Specific profile. The Specific profile is similar to the Generic profile, it is also a collection of parameters that are used by an ME profile. But the Specific profile provides values for information fields that are very specific to the ONT/ONU.

Every Specific profile is associated with only one ME and one Generic profile to define the supported ONT/ONU hardware model and service plan.

- 1** To create an end-user based Specific profile in the ZMS tree view, right-click an OLT port, and then select **Manage Specific Profile**.

The **Manage OMCI Specific Profiles** dialog box appears. It shows all the existing Specific profiles.

- 2 Click **Add**, the **Add Specific Profile on OLT** dialog box appears.
- 3 In the **Add Specific Profile on OLT** dialog box, specify the following values:

Parent Generic Profile Name — Select a Generic profile by clicking the browser button.

Create Mode — Select creating a Specific profile on one ONT/ONU or all ONT/ONUs under this OLT. Each ONT/ONU can only create one Specific profile.

Unused ONU ID — If Only One Unused ONT/ONU is selected in the Create Mode, this field will be enabled. Specify an ONT/ONU ID to create the Specific profile on.

Import contents of profile from a file — If you want to import the contents from a file, check this box, and enter the file's name in the **Profile File Name** field. This file must exist in the `/tftpboot` directory in the ZMS server.

- 4 Click **Add**.

The newly created Specific profile appears in the **Manage OMCI Specific Profiles** dialog box.

The newly created Specific profile also appears in the **Generic Details** dialog box. The **Generic Details** dialog box can be opened after selecting its associated Generic profile in the **ME Details** dialog box and click **Details**.

- 5 After creating Specific profile, select this Specific profile in the **Manage OMCI Specific Profiles** dialog box or the **Generic Details** dialog box, and click **Modify**. The **Modify Specific Profiles** dialog box appears. User can assign values to the parameters that are unique to the end-user, such as user's IP address and telephone number etc. And then, click **Modify** to save the change.
- 6 To view the specific profile, select this Specific profile in the **Manage OMCI Specific Profiles** or **Generic Details** dialog box, click **View**:
- 7 To delete the Specific profile, select this Specific profile in the **Manage OMCI Specific Profiles** or **Generic Details** dialog box, click **Delete**.

Click **Ok** in the confirm window.

Creating Specific profiles on ONU level

The Specific profile can be created on ONU level too.

Every Specific profile is associated with only one ME and one Generic profile to define the supported ONT/ONU hardware model and service plan.

- 1 To create an end-user based Specific profile in the ZMS tree view on the ONU level, right-click an ONU port, and then select **OMCI ONT Configuration**, and then click **Configure Specific Profile**.
- 2 If there is no Specific Profile exist in this ONU, the **Add Specific Profile on physical** dialog box appears.
- 3 In the **Add Specific Profile on physical** dialog box, specify the following values:

Parent Generic Profile Name — Select a Generic profile by clicking the browsing button.

Import contents of profile from a file — If you want to import the contents from a file, check this box, and enter the file's name in the **Profile File Name** field. This file must exist in the */tftpboot* directory in the ZMS server.

- 4 Click **Add**.

The **Modify Specific Profiles** dialog box appears automatically.

In the **Modify Specific Profile** dialog box, user can assign values to the parameters that are unique to the end-user, such as user's IP address and telephone number etc.

Click **Modify** to save the change.

- 5 The newly created Specific profile appears in the **Generic Details** dialog box. The **Generic Details** dialog box can be opened after selecting its associated Generic profile in the **ME Details** dialog box and click **Details**.
- 6 To view the specific profile, select this Specific profile in the **Manage OMCI Specific Profiles** or **Generic Details** dialog box, click **View**:
- 7 To delete the Specific profile, select this Specific profile in the **Manage OMCI Specific Profiles** or **Generic Details** dialog box, click **Delete**.

Click **Ok** in the confirm window.

Activating ONT/ONU with OMCI profiles



Note: Make sure to provision the logical connections for data, video, and voice services in the MXK and ONT/ONUs before activating the ONT/ONUs in order to avoid having to re-sync or reboot the ONT/ONUs eventually.

After a specific profile is created on an ONT/ONU, you can activate this ONT/ONU with serial number and OMCI profiles association.

During activation process, when the OLT communicates with the ONT/ONU, the OLT retrieves the current variable settings on this ONT/ONU.

To activate an ONT/ONU, perform the following tasks:

- 1 After a Specified profile is created on an ONT/ONU, the names of the associated ME and Generic profiles will be displayed in the **Modify GponOnu Physical Configuration** dialog box.
- 2 Right-click an OLT port, select **Assign Serial Numbers**:
The **Modify Serial Number Table** dialog appears.
- 3 Select an ONT/ONU port from the pull-down menu to associate with a serial number. And click **Apply**.
- 4 Verify this ONT/ONU is activated with serial number and OMCI profiles.
Right-click this ONT/ONU port in the tree view, select **Modify**. The **Modify GponOnu Physical Configuration** window appears. And then click **Configuration** tab.
ONT Serial No Vendor Specific field shows the associated serial number.
OMCI ME file name shows the associated ME profile name.
OMCI Generic file name shows the associated Generic profile name.
Onu Added is True shows this ONT/ONU is activated.
- 5 If you want to disable an ONT/ONU and clear the serial number for this ONT/ONU, uncheck the **Onu Added** field and then click **Modify**.

Import and export OMCI profile file

The OMCI profile import feature allows user to overwrite the contents in an existing OMCI profile with a new OMCI profile file. The OMCI profile file must exist in the ZMS server */tftpboot* directory.

Any changes in the OMCI profile file, such as adding or deleting OMCI commands in ME profile file, will cause the variables in the OMCI profile to be added, deleted, or remain the same. After importing the OMCI profile file to the existing OMCI profile, system will reconcile the associated Generic profile and Specific profile. User can update the variables in the Generic and Specific profile as needed.

The OMCI profile export feature allows user to copy the contents of an OMCI profile to a new OMCI profile file, and store this file into the ZMS server */tftpboot* directory. Later this OMCI profile file could be shared with other devices.

Importing and exporting ME profile file

The following example shows how to import and export an ME profile file:

- 1 Right-click a device, and select **Manage ME Profile**.
The **Manage OMCI ME Profiles** dialog appears.
- 2 To import the contents of an ME profile, select this ME profile in the **Manage OMCI ME Profiles** dialog, then click **Import**.

The **Import Profile On Device** dialog appears.

- 3 Enter the profile file name to which you want to import the ME profile. Make sure this profile file exists in the ZMS server */tftpboot* directory. And then click **Apply**.
- 4 To export the contents of an ME profile, select this ME profile in the **Manage OMCI ME Profiles** dialog, then click **Export**.
The **Export Profile On Device** dialog appears.
- 5 Enter the profile file name to which you want to export the ME profile. The correspondent profile file will be stored in the device. And then click **Apply**.

Importing and exporting Generic profile file

The following example shows how to import and export a Generic profile file:

- 1 Right-click a device, and select **Manage Generic Profile**.
The **Manage OMCI Generic Profiles** dialog appears.
- 2 To import the contents of a Generic profile, select this Generic profile in the **Manage OMCI Generic Profiles** dialog, then click **Import**.
The **Import Profile On Device** dialog appears.
- 3 Enter the profile file name to which you want to import the Generic profile. Make sure this profile file exists in the ZMS server */tftpboot* directory. And then click **Apply**.
- 4 To export the contents of a Generic profile, select this Generic profile in the **Manage OMCI Generic Profiles** dialog, then click **Export**.
The **Export Profile On Device** dialog appears.
- 5 Enter the profile file name to which you want to export the Generic profile. The correspondent profile file will be stored in the ZMS server */tftpboot* directory. And then click **Apply**.

Importing and exporting Specific profile file

The following example shows how to import and export a Specific profile file:

- 1 Right-click an OLT port, and select **Manage Specific Profile**.
The **Manage Specific Profiles** dialog appears.
- 2 To import the contents of a Specific profile, select this Specific profile in the **Manage OMCI Specific Profiles** dialog, then click **Import**.
The **Import Profile On Device** dialog appears.

- 3 Enter the profile file name to which you want to import the Specific profile. Make sure this profile file exists in the ZMS server */tftpboot* directory. And then click **Apply**.
- 4 To export the contents of a Specific profile, select this Specific profile in the **Manage OMCI Specific Profiles** dialog, then click **Export**.
The **Export Profile On Device** dialog appears.
- 5 Enter the profile file name to which you want to export the Specific profile. The correspondent profile file will be stored in the ZMS server */tftpboot* directory. And then click **Apply**.

Manage ONT/ONU with OMCI (MXK, MXK 194/198 only)

The GPON ONT/ONUs are managed through OMCI (standard G983.1 - 983.4).

Topics:

- [Viewing or changing trap reporting status on ONT/ONU on page 233](#)
- [Retrieving alarm information on ONT/ONU on page 234](#)
- [Viewing the ONT/ONU specific OMCI alarms on page 234](#)
- [Viewing OMCI alarms on the ONT/ONU subscriber ports on page 234](#)
- [Viewing OMCI status on ONT/ONU on page 234](#)
- [Configuring subscriber ports on ONT/ONU on page 235](#)
- [Re-syncing changes to a single ONT/ONU on page 236](#)
- [Re-syncing changes to ONT/ONUs on page 236](#)
- [Applying changes to a single ONT/ONU \(Smart OMCI Only\) on page 236](#)
- [Applying changes to multiple ONT/ONUs \(Smart OMCI Only\) on page 237](#)
- [Rebooting a single ONT/ONU on page 237](#)
- [Performing immediate upgrade on a single ONT/ONU on page 237](#)
- [Performing immediate/scheduled upgrade on multiple ONT/ONUs on page 239](#)
- [Viewing or deleting scheduled ONT upgrades on page 241](#)
- [Performing auto upgrade on an ONT/ONU on page 241](#)
- [Viewing ONT/ONU upgrade status on an OLT on page 242](#)
- [Enabling upstream multicast video support on page 243](#)

Viewing or changing trap reporting status on ONT/ONU

User can control the conditions that cause asynchronous reporting traps from the OLT via SNMP. The purpose of these controls is to reduce trap traffic between the MXK and ZMS, while allowing the user to get more information about critical or failing ONT/ONUs.

To view or change the reporting status of traps on ONT/ONU(s), perform the following steps:

- 1 To view the current reporting status of traps on an ONT/ONU, right-click on this ONT/ONU in the tree view, and click **Modify**.

The **Modify GponOnu Physical Configuration** dialog appears. And then click **Configuration** tab.

Three types of traps could be reported on ONT/ONU, they are:

- **OMCI ONT Physical Traps** — It includes the power status, battery status, and physical intrusion conditions, as reported from the ONT/ONU via OMCI.

The options for the OMCI ONT Physical Traps are:

enable: This is the default value. The OMCI ONT Physical Traps are sent.

disable: The OMCI ONT Physical Traps are not sent.

- **OMCI ONT Traps** — It is the status of subscriber ports on the ONT/ONU (e.g. ethernet port LanLos).

The options for the OMCI ONT Traps are:

enable: The OMCI ONT Traps are sent.

disable: This is the default value. The OMCI ONT Traps are not sent.

- **Line Status Change Traps** — It is originated on the MXK, and reports the ONT/ONU line going up or down.

The options for the Line Status Change Traps are:

enable: The linkUp, linkDown, and Line Status Change Traps are sent.

disable: The Line Status Change Traps are not sent.

auto: This is the default value. In this setting, the linkUp or linkDown traps are not sent, only the Line Status Change Traps trap is sent if the line is going down with dying gasp (presumably powered down), or if the line is coming up (which may or may not be clearing a dying gasp condition).

- 2 To change the current reporting status of traps on the ONT/ONU, select the desired reporting option for traps, and click **Modify**.

Retrieving alarm information on ONT/ONU

To force ZMS to verify that the alarms ZMS has for the ONT/ONU are up-to-date:

Right-click an ONT/ONU in the tree view, and select **OMCI ONT Configuration > Synchronize Alarms**.

Viewing the ONT/ONU specific OMCI alarms

To view some ONT/ONU specific OMCI alarms, use the following procedure:

- 1 Right-click an ONT/ONU in the tree view, and click **Modify**.
The **Modify GponOnu Physical Configuration** dialog appears.
- 2 Click **Alarm Status**. The status of supported alarms are displayed in the window.
Yes indicates this alarm is currently raised on this ONT/ONU, **No** means not.

Viewing OMCI alarms on the ONT/ONU subscriber ports

From MXK user can view all the OMCI alarms generated on the ONT/ONU subscriber ports.

To view those alarms, right-click an ONT/ONU, and select **Manage ONT > Current Conditions**.

The **Current ONT Condition List** dialog appears.

The following fields are displayed in the dialog:

Class — This field indicates the class objects that defined in the standard 984.4.

Entity ID — This field indicates the ONT/ONU subscriber port ID used in SNMP.

Logical Port ID — This field indicates the actual subscriber port number on the ONT/ONU.

Description — This field gives the brief description for OMCI alarm that generated on the ONT/ONU subscriber ports.

Viewing OMCI status on ONT/ONU

From MXK user can view the OMCI status of an ONT/ONU.

To view the OMCI of an ONT/ONU, right-click this ONT/ONU, and select **Manage ONT > Status**.

The **View OMCI Ont Status** dialog appears.

The following fields are displayed in the dialog:

Administrative State — This field indicates the administrative state of the ONT/ONU. Up or Down.

Operational State — This field indicates the operational state of the ONT/ONU. Active or Inactive.

Battery Backup — This field indicates the ONT/ONU has battery backup or not. True or False.

Omcc Version — This field indicates the OMCC/ OMCI version used by the ONT/ONU.

Security Capability — This field indicates the AES capability on the GPON ONT/ONU.

Security Mode — This field indicates the AES encryption mode on the GPON ONT/ONU.

Configuring subscriber ports on ONT/ONU

From MXK user can set the administrative state, operational state, and auto-detect settings of ONT/ONU subscriber ports.

The port type could be Eth (ethernet port), POTS (POTS port), RF (RF port), and CES (T1/E1 port). User can also enable or disable the port by changing the admin state of it.

- 1 To change the admin state of a subscriber ports on an ONT/ONU, right-click this ONT/ONU, and select **Manage ONT> Manage Ports**.

The **OMCI Port Status** dialog appears.

- 2 Select a port, and click **Admin Up** button to enable it, or click **Admin Down** button to disable it.
- 3 To specify the auto detect setting, click the **Auto Detect** column and specify the auto detect setting
 - None: auto detect off.
 - Auto: auto-detect
 - Ten-Full: 10 Mbps, full duplex only
 - Hundred-Full: 100 Mbps, full duplex only
 - Thousand-Full: 1000 Mbps, full duplex only
 - Ten-Half: 10 Mbps, half duplex only
 - Hundred-Half: 100 Mbps, half duplex only
 - Thousand-Half: 1000 Mbps, half duplex only
 - Ten-Full-Auto: 10 Mbps full duplex and auto
 - Thousand-Auto: 1000 Mbps auto
- 4 Click the **Modify Auto Detect** button.

Re-syncing changes to a single ONT/ONU

Synchronizing an ONT/ONU causes the MXK to break and re-establish linkage with ONT/ONU, and send the latest OMCI commands to the ONT/ONU. It could be used after an ME profile change.

- 1 To re-sync an OMCI enabled ONT/ONU, right-click on this ONT/ONU in the tree view, and click **Manage ONT > Resync**.

A Confirm window appears.

- 2 Click **Yes**.

Re-syncing changes to ONT/ONUs

- 1 To resync changes to all ONTs, right-click a device, slot, OLT and select **Manage ONT > Resync ONTs**.

The **Resync** dialog box appears.

- 2 Specify the following fields in the dialog:

Once— Check this field to resync the ONTs at a scheduled time. You also need to select the time (in the format of HH, MM, Date in the week) to initiate the upgrade process.

Immediate— Check this field to resync the ONTs immediately.

- 3 Click **Resync**.

Applying changes to a single ONT/ONU (Smart OMCI Only)

Adding new services to an existing subscriber does not require a resync of the ONT/ONU. For example, if a user has High Speed Internet Access (HSIA) on Ethernet port 1, and requests HSIA on Ethernet port 2, this can be achieved without doing a resync of the ONT/ONU. The user can modify the Specific profile or Generic profile and issue the following command:

The **apply ONT** option issues the OMCI configuration command in the ME profile. This command does not force a resync of the ONT/ONU. If the user makes modifications to the Specific profile and adds new services, then these commands take effect in the ONT/ONU without affecting other services on the same or other ports.

To add new services to an OMCI enabled ONT/ONU without effecting other existing services:

- 1 Right-click on this ONT/ONU in the tree view, and click **Manage ONT > Apply**.

A Confirm window appears.

- 2 Click **Yes**.

Applying changes to multiple ONT/ONUs (Smart OMCI Only)

To apply changes to all the ONTs in a device, slot, or OLT:

- 1 Right-click a device, slot, or OLT, and select **Manage ONT > Apply ONTs**.

The **Apply** dialog box appears.

- 2 Specify the following fields in the dialog:

Once— Check this field to apply the changes to the ONTs at a scheduled time. You also need to select the time (in the format of HH, MM, Date in the week) to initiate the upgrade process.

Immediate— Check this field to apply the changes to the ONTs immediately.

- 3 Click **Apply**.

Rebooting a single ONT/ONU

To reboot the remote ONT/ONU from MXK:

- 1 Right-click this ONT/ONU, and select **Manage ONT> Reboot**.

A **Confirm** window appear.

- 2 Click **Yes** on the **Confirm** window. This ONT/ONU will be rebooted.

Rebooting multiple ONT/ONUs

To reboot multiple ONT/ONUs:

- 1 Right-click a device, slot, or OLT, and select **Manage ONT > Reboot ONTs**.

The **Bulk Reboot ONT** dialog box.

- 2 Specify the following fields in the dialog:

Once— Check this field to reboot the ONTs at a scheduled time. You also need to select the time (in the format of HH, MM, Date in the week) to initiate the upgrade process.

Immediate— Check this field to perform upgrading on the ONTs immediately.

- 3 Click **Reboot**.

Performing immediate upgrade on a single ONT/ONU

The OMCI image upgrade feature enables MXK user to upgrade firmware on an ONT/ONU via ZMS immediately. Before downloading the image file to the ONT/ONU, make sure the ONT/ONU image file is downloaded in the MXK /card1 directory first.

To upgrade the image on an OMCI based GPON ONT/ONU, use the **Modify Upgrade ONT** dialog box:

- 1 Right-click this ONT/ONU, and select **Manage ONT > Upgrade**.

The **Modify Upgrade ONT** dialog box appears.

- 2 Specify the following fields in the dialog:

Action —This field indicates the action you want to perform for the image upgrading. It contains the following combinations:

- **Download:** Download an image file to the ONT/ONU from OLT. An image file will be downloaded to either an inactive partition or an uncommitted partition. After downloading, ONT/ONU validates the file.
- **Activate:** Bootup a valid file in the inactive partition immediately in ONT/ONU. Only one partition at a time could be active.
- **Commit:** Specify a default file to bootup when next time this ONT/ONU is powered up. It will commit the file in the uncommitted partition. Only one partition at a time could be committed.
- **Download and Activate:** Perform the download action, and then if the file passed validation check, perform the activate action.
- **Download, Activate and Commit:** Perform the download and activate actions, and then if the ONT/ONU ranges, perform the commit action.
- **Abort Download:** Terminate the queued download.
- **None:** No actions are performed.

File Name —This field indicates the name of the image file that you want to download to the ONT/ONU from MXK OLT. This file must exist in the MXK.

Partition —This field is optional. It indicates which partition you want to perform the action on. Partition 0, Partition 1, or None. None means use the inactive partition for download or activate action, or the uncommitted partition for commit action.

- 3 Click **Apply**. The dialog shows the download status.

Download Status —The values of the download status could be:

- **None:** ONT/ONU is not running, or not OMCI-provisioned.
- **No Upgrade:** ONT/ONU is running, but hasn't been upgraded yet.
- **Queued:** An Image download has been requested, and has been queued by the system for download.
- **Downloading:** Downloading the image to the ONT/ONU is in progress or validating the downloaded image is in progress.
- **Downloaded:** The software has been downloaded to the ONT/ONU but not activated yet. One possible reason is the ONT/ONU is rebooting.

- **Complete:** Successfully completed downloading, activating, and committing the software to the ONT/ONU.
- **Error:** Failed to upgrade due to some errors.
- **Aborted:** The ONT/ONU queued to be upgraded was aborted by request.
- **FileErr:** The software file to be upgraded does not exist, or has errors

Partition 0 Version —This field indicates the version of the image file stored in Partition 0. None, True, or False.

Partition 0 Valid —This field indicates whether the image file stored in Partition 0 is valid. None, True, or False.

Partition 0 Activated —This field indicates whether the image file stored in Partition 0 is activated. None, True, or False.

Partition 0 Committed —This field indicates whether the image file stored in Partition 1 is committed. None, True, or False.

Partition 1 Version —This field indicates the version of the image file stored in Partition 1. None, True, or False.

Partition 1 Activated —This field indicates whether the image file stored in Partition 1 is valid. None, True, or False.

Partition 1 Committed —This field indicates whether the image file stored in Partition 1 is committed. None, True, or False.

ONT Model—This field indicates ONT model.

Last Upgrade Start Time—This field indicates the date-time when last upgrade was started.

Upgrade will be activated—This field indicates whether the activate action will be taken.

Upgrade will be committed—This field indicates whether the commit action will be taken.

Upgrade type—This field indicates whether the upgrade is auto upgrade or manual upgrade.

4 Click **Refresh** will update all the read-only fields.

Related topics:

[Downloading files to a single or multiple devices, page 70.](#)

Performing immediate/scheduled upgrade on multiple ONT/ONUs

The bulk ONT upgrade feature allow you to perform immediate or scheduled upgrade tasks on all OMCI ONT/ONUs under an OLT, slot, or a device node. Same as the single ONT/ONU upgrade, before downloading a ONT/ONU image file to the ONT/ONU, make sure the file is downloaded in the *MXK / card1* directory first.

The bulk ONT upgrading actually combine the actions of download, activate, and commit together. The inactive partition is always used to perform those actions.

To upgrade the image on multiple OMCI based GPON ONT/ONUs managed by a device, use the **Upgrade ONT** dialog box:

- 1 Right-click a device, slot, or OLT, and select **Manage ONT > Upgrade ONTs**.

The **Upgrade ONT** dialog box appears.

- 2 Specify the following fields in the dialog:

Action —This field indicates the action you want to perform for the image upgrading. It contains the following combinations:

- **Activate and Commit:** Perform activate action, and then if the ONT/ONU ranges, perform the commit action.
- **Abort Download:** Terminate the queued download.
- **Download, Activate and Commit:** Perform the download and activate actions, and then if the ONT/ONU ranges, perform the commit action.
- **Download and Activate:** Perform the download action, and then if the file passed validation check, perform the activate action.
- **Commit:** Specify a default file to bootup when next time this ONT/ONU is powered up. It will commit the file in the uncommitted partition. Only one partition at a time could be committed.
- **Activate:** Bootup a valid file in the inactive partition immediately in ONT/ONU. Only one partition at a time could be active.
- **Download:** Download an image file to the ONT/ONU from OLT. An image file will be downloaded to either an inactive partition or an uncommitted partition. After downloading, ONT/ONU validates the file.
- **None:** No actions are performed.

File Name —This field indicates the name of the image file that you want to download to the ONT/ONUs from MXK OLT. This file must exist in the MXK.

Once— Check this field to perform scheduled upgrading on the ONTs, you also need to select the time (in the format of HH, MM, Date in the week) to initiate the upgrade process.

Immediate— Check this field to perform upgrading on the ONTs immediately.

- 3 Click **Upgrade**.

Related topics:

[Downloading files to a single or multiple devices, page 70.](#)

Viewing or deleting scheduled ONT upgrades

You can view and delete any scheduled OMCI ONT upgrades in the **Manage ONT/ONU Schedules** dialog. Any future scheduled ONT actions will also be managed from this dialog.

- 1 Select **Tools > Manage ONT Schedules**.

The **Manage ONT Schedules** dialog box appears.

All the scheduled OMCI ONT upgrades are displayed in this dialog box.

- 2 If you want to delete a schedule OMCI ONT upgrade task, select this task and click **Delete**.

Performing auto upgrade on an ONT/ONU

The OMCI ONT/ONU auto upgrade feature allows MXK user to automatically upgrade ONT/ONUs which are installed with the outdated software images when they are ranging.

If the OMCI auto-upgrade is enabled, when an ONT/ONU ranges, MXK searches an auto-upgrade template for this ONT/ONU model. The auto-upgrade template is pre-defined by the user for each ONT/ONU model. It contains the auto-upgrade enable status, model name, allowed software version, and the image file to be downloaded. If the matching template is found for the specific ONT/ONU model, the MXK compares the ONT/ONU software version with the allowed software version defined in the template. If they are same, then the auto-upgrade is interrupted, otherwise the MXK automatically upgrades the ONT/ONU.

The actions to automatically upgrade an ONT/ONU software through OMCI are Download->Activate->Commit.

The download is always performed on the standby partition. If the download is successful, then the standby partition is made the active and then the image is committed to the partition. After the image is committed, the auto-upgrade is finished.

The download task in queue will be aborted if disabling the auto-upgrade.

- 1 Create an auto-upgrade template for an ONT/ONU model.

- a Right-click the device, and select **Modify**:

The **Modify Device Configuration** dialog box appears.

- b Select **Remote Software Upgrade Profiles** from the tree view.

The **Remote Software Upgrade Profile** window appears.

- c Click **Add** button to open the **Add Remote Software Upgrade Profile** window.

- d Specify the following parameters in the window:

ONT Model — The ONT/ONU model to be upgraded

ONT SW Version — Allowed software version on this ONT/ONU.

ONT SW Filename — The image file to be downloaded.



Note: When creating the template, the image file must already exist in the device flash, otherwise an error message displays. Not specifying the directory in the *fileName* field indicates the file is stored under the root directory, */card1*.

Enabled — Enable or disable auto-upgrade on this ONT/ONU model. By default, it is disabled.

e Click **Add** to confirm the change.

2 Enable ONT/ONU auto-upgrade.

By default, ONT/ONU auto-upgrade is disabled. In order to perform ONT/ONU auto upgrade, the following two places should be both enabled:

a Enable auto-upgrade on an ONT/ONU model in the **Add/ Modify Remote Software Upgrade Profile** window.

b Enable auto-upgrade for an ONT/ONU ID in the **Modify GponOnu Physical Configuration** window:

Right-click on the ONT/ONU, select **Modify**.

In the **Modify GponOnuPhysical Configuration** dialog box select **Configuration** in the tree view.

At last select **Enabled** in the **Auto Upgrade Enabled** field.

Click **Modify**.

3 View the ONT/ONU auto-upgrade status.

Right-click this ONT/ONU, and select **Manage ONT> Upgrade**.

The **Modify Upgrade ONT** dialog box appears.

Related topics:

[Downloading files to a single or multiple devices, page 70.](#)

Viewing ONT/ONU upgrade status on an OLT

User can view all the ONT/ONU upgrade status on an OLT in the **ONT Upgrade Status** window.

This window shows current ONT/ONU upgrade status such as ONT/ONU upgrade status, ONT/ONU model ID, the date-time when last upgrade was started, active state, commit state, type of upgrade (Manual or Auto), and which partition is used.

Right-click an OLT, select **Manage ONT > Upgrade ONT Status**.

The **ONT Upgrade Status** window appears:

The possible values of the Upgrade Status field are:

- **None:** ONT/ONU is not running, or not OMCI-provisioned.
- **No Upgrade:** ONT/ONU is running, but hasn't been upgraded yet.
- **Queued:** An Image download has been requested, and has been queued by the system for download.
- **Downloading:** Downloading the image to the ONT/ONU is in progress or validating the downloaded image is in progress.
- **Downloaded:** The software has been downloaded to the ONT/ONU but not activated yet. One possible reason is the ONT/ONU is rebooting.
- **Complete:** Successfully completed downloading, activating, and committing the software to the ONT/ONU.
- **Error:** Failed to upgrade due to some errors.
- **Aborted:** The ONT/ONU queued to be upgraded was aborted by request.
- **FileErr:** The software file to be upgraded does not exist, or has errors

Enabling upstream multicast video support

The upstream multicast video feature are supported on some OMCI-based zNIDs (e.g. zNID-GPON-2520) for applications like video surveillance.

The upstream multicast video feature can be turned on on the OLT side by enabling the Flood Multicast field in the **Modify Logical Bridge Configuration** dialog box.

The following example turns on the upstream multicast video on a downlink bridge that was created on 1-7-2-909-gponport-300 for video services:

- 1 In the Manage Bridge Logicals dialog box, select the downlink bridge that created on 1-7-2-909-gponport-300 and click **Modify**.
- 2 In the **Modify Logical Bridge Configuration** dialog box, select Bridge Logical Configuration tab, and select **True** in the **Flood Multicast** field.
- 3 Click **Modify**.

OMCI Statistics (MXK, MXK 194/198 only)

The MXK obtains ONT/ONU statistics from the ONT/ONU using OMCI. The MXK sends standards based OMCI commands to retrieve statistics information. The statistics are maintained on the ONT/ONU in 15-minute intervals. There are 2 intervals of statistics that is stored in the ONT/ONU, current and previous. When an ONT/ONU is activated, the ONT/ONU starts storing statistics. This statistics is stored under the current category of statistics. After a 15 minute time period, the statistics value are reset. The statistics tracked during the past 15 minute period are stored as the previous interval. A new set of current interval statistics is tracked. After every

15-minute period the current interval is saved as previous and a new current category is created with zeroed out values.

To display OMCI statistics for selected ONT/ONU(s), right-click an ONT/ONU in the tree view, and select **Manage ONT > Statistics**.

The **OMCI Statistics** window appears.

For details on the settings, see the online help.

Unified Service Provisioning - CPE profiles (MXK, MXK 194/198 only)

Building on Dynamic OMCI to provide automatic software downloads, pre-provisioning support, and zNID configuration “master” in MXK — Unified Service Provisioning provides a single provisioning method for Zhone GPON zNIDs via the MXK and ZMS.

Unified Service Provisioning accesses all the management interfaces, now extending to work with features that were only accessible through SNMP or the CPE device’s Residential Gateway web based user interface.

Unified Service Provisioning section includes the following topics:

- [Dynamic OMCI, page 244](#)
- [Residential Gateway \(RG\) Features Provisioning, page 270](#)
- [CPE Management Templates, page 299](#)
- [Post Configuration in USP, page 301](#)
- [CPE LLDP-MED configurations, page 302](#)

Dynamic OMCI

In an effort to improve the MXK user experience Zhone has added enhanced functionality to provision CPE devices. The user is now able to use a single screen to provision a bridge on the MXK and the attached CPE at the same time. Voice, Video, and Data services are configured on the MXK and flow through to the CPE.

Note that MXK 194 and MXK 198 support Dynamic OMCI feature too. This section uses “MXK” to represent all the devices (MXK, MXK 194, MXK 198) that support dynamic OMCI feature.

Generally these are the steps to follow to configure the MXK to be able to manage ONU with Dynamic OMCI:

- [Provision MXK upstream services, page 245](#)
- [Create service related GPON additions, page 245](#)
- [Provision Dynamic OMCI GPON with internal ME profile, page 245](#)
- [Provision per subscriber downstream MXK bridges and CPE connections with Dynamic bridging, page 246](#)
- [Provision services with CPE Profiles, page 251](#)
- [Activate ONT/ONU in Dynamic OMCI, page 269](#)

Provision MXK upstream services

As shown in the **Step 2a**, an uplink bridge must be created with the **Bridge Logical on Device** window. To access to this window, right-click the device, select **Manage Bridging**, and then click **add**.

For details refer to [Bridge configuration on page 403](#).

Create service related GPON additions

As shown in the **Step 2b**, GPON Traffic Profile must be created before creating a MXK downlink bridge on GPON. It contains the bandwidth allocation information for the T-cont. To create the GPON traffic profile, use the **Modify Device Configuration** dialog box. For details refer to [Creating a GPON Traffic Profile on page 216](#).

Provision Dynamic OMCI GPON with internal ME profile

Zhone provides internal ME profiles for supported Zhone GPON ONTs. The format of a internal ME profile name is *zhone-ZnidModel*.

Internal ME profiles are the indicator of Dynamic OMCI provisioning.

As shown in the flowchart **Step 2c**, by specifying an internal ME profile name in the initial setup on an ONU, the MXK knows the model of this ONU, and will provision that ONU with Dynamic OMCI. For example, internal ME profile **zhone-5114** defines there are 4 Ethernet ports, 2 POTS ports, and 4 PWE ports on the ZNID-GPON-5114, which supports both SIP and H.248 VoIP signaling.

Zhone also provides a universal ME profile for any zNIDs: *zhone-default*.

Specifying internal ME profile for the ONU

Based on the ONU model, assign the matching internal ME profile to this ONU. In this way it indicates this ONU is provisioned by dynamic OMCI.

There are two ways to specify internal ME profile for the ONU:

- 1 The first method is specifying internal ME profile while creating ONU connection in the **CPE Connection On Device** dialog box.
 - a Right-click a MXK in the tree view, select **Manage USP Services**. The **Manage CPE Services dialog box** appears.
 - b Click **CPE Connection** tab. And then click **Add**.
The **CPE Connection On Device** dialog box appears. Its **Select Port** pane shows all the connected ONUs and their assigned serial numbers and specified internal ME profiles.
 - c While you creating CPE connection on an ONU, you can select an internal ME profile name in the **ME Profile** field.
Note that Internal ME will only be set for the ONUs that do not have internal ME specified.
- 2 The second method is using the **Modify GponOnu Physical Configuration** dialog box.
 - a To specify an internal ME profile for an ONU, right-click an ONU in the tree view, select **Modify**. The **Modify GponOnu Physical Configuration** dialog box appears.
 - b Click **Configuration**. The **Configuration** dialog box appears.
 - c In the **OMCI ME Profile** field, select an internal ME profile name. And then click **Modify**.

Provision per subscriber downstream MXK bridges and CPE connections with Dynamic bridging

Dynamic bridging is only applicable to the Unified Provisioning. It appears as **Step 4a** in the flowchart. It uses a single dialog box “**CPE Connection On Device**” to create both MXK bridge and CPE connections, and define the bridge-related parameters for service types.

The MXK bridge and CPE connection can have one-to-one and one-to-many mappings. Dynamic OMCI provisioning usually use one-to-one mapping. RG provisioning can have one-to-one and one-to-many mappings.

The one-to-one mapping is one MXK bridge created on a GEM port that maps to one CPE connection created on an ONU UNI port.

Before creating the MXK bridges and CPE connections. Check if you have the following profiles:

1. GPON Traffic Profile (mandatory)

For details about creating GTPs, refer to [Creating a GPON Traffic Profile on page 216](#).

2. CPE traffic management profile (optional)

For details about creating CPE TMs, refer to the next section [Creating CPE traffic management profiles on page 247](#).

Creating CPE traffic management profiles

You can use the CPE traffic management profile to configure the bandwidth shaping on GEM ports and Ethernet UNI ports (i.e. the Ethernet subscriber facing ports on an ONU). It is optional.

Note that the support of traffic management is ONU model dependent. Not all the ONU models support traffic management.

- For GEM ports:

You can use the CPE Traffic Management profile to configure rate control on upstream, priority control on both upstream and downstream direction, and weight control parameters on both direction.

To assign a CPE traffic management profile index to a GEM port, use the **CPE Connection On Device** dialog. For details, refer to the next section [Creating MXK bridge and CPE connections for different services on page 249](#).

- For CPE Ethernet UNI ports:

You can use the CPE Traffic Management profile to configure rate control on upstream and downstream directions of the Ethernet UNI port by using the Upstream SIR, Upstream PIR, Downstream SIR, and Downstream PIR fields.

To assign a CPE traffic management profile index to a CPE Ethernet UNI port, use the **Ethernet Service on Device** dialog. For details, refer to the section [Creating CPE Ethernet subscriber profile \(optional\) on page 262](#).



Note: Rate control and Priority (weight) control cannot be used on the same ONU. If rate control is applied to one GEM port, it will be enabled for the whole ONU, the other GEM ports in the same ONU must use rate control too. Same for Priority (Weight) control.



Note: Rate control on the downstream direction (i.e. ds-sir and ds-pir field in the CPE traffic management profile) only apply to Ethernet UNI ports. They do not apply to GEM ports.

The following example shows how to create a CPE traffic management profile.

- 1 Right-click an MXK, and select **Manage USP System**.

The **Manage CPE System** dialog box appears.

- 2 Click **Traffic Management** tab, and click **Add**.

The **Add Traffic Management** dialog box appears.

- 3 In the **Configuration** window, specify the desired values for the following fields.

Traffic Management Index: CPE traffic management profile index.

Profile Name: CPE traffic management profile name.

Upstream SIR (in kbps): Upstream sustained information rate, in kilobits per second. Value range is 0 to 1310720.

Upstream PIR (in kbps): Upstream peak information rate, in kilobits per second. Value range is 0 to 1310720.

Upstream Priority: Upstream priority, for the strict priority scheduling policy. Value range is 0 to 7 where 0 is the highest priority.

Upstream Weight: Upstream weight, for the weighted round robin scheduling policy. Value range is 0 to 255 where 0 is the lowest weight.

Downstream SIR (in kbps): Downstream sustained information rate, in kilobits per second. Value range is 0 to 1310720. Only for Ethernet UNI ports.

Downstream PIR (in kbps): Downstream peak information rate, in kilobits per second. Value range is 0 to 1310720. Only for Ethernet UNI ports.

Downstream Priority: Downstream priority, for the strict priority scheduling policy. Value range is 0 to 7 where 0 is the highest priority.

Downstream Weight: Downstream weight, for the weighted round robin scheduling policy. Value range is 0 to 255 where 0 is the lowest weight.

- 4 Click **Add**, the new CPE traffic management profile appears in the **Manage CPE System** dialog > **Traffic Management** pane.
- 5 If users want to modify a CPE traffic management profile, select it and then click **Modify**.
- 6 If users want to delete a CPE traffic management profile, select it and then click **Delete**.

Creating MXK bridge and CPE connections for different services

Use the following procedure to create MXK bridges and CPE connections.

Note that the following procedure is used to create a downlink bridge and CPE connection. You need to create an uplink bridge with the **Bridge Logical on Device** window as well.

- 1 Right-click an MXK, and select **Manage USP Service**.

The **Manage CPE Services** dialog box appears.

- 2 Click **CPE Connection** tab, and click **Add**.

The **CPE Connection On Device** dialog box appears.

- 3 In the **Select Port** pane, expand the tree, and then select an ONU port.

Only the ONU with the internal ME profile specified will be displayed in the tree view, otherwise it will be greyed out.

- 4 In the **GEM Port Id** field, enter a GEM port ID. The GEM port ID could be any number in the range of 257 to 3828.

- 5 In the **GTP Information** pane,

- a Select a GTP index or GTP Template. (mandatory)

GTP is a mandatory field when creating a downlink MXK bridge on the GEM port. It contains the bandwidth allocation information for the T-cont. For details about creating GTPs, refer to [Creating a GPON Traffic Profile on page 216](#).

- b Select a traffic management profile index. (optional)

Traffic management profile is optional when creating a downlink MXK bridge on the GEM port. It contains the traffic shaping information for the GEM port. For details about creating CPE TMs, refer to [Creating CPE traffic management profiles on page 247](#).

- c Select a multicast control list index and the max number of multicast streams.



Note: The maximum number of multicast streams must be specified for video bridges.

The max number of multicast streams are required when creating a downlink MXK bridge on the GEM port for video service. The bridge will fail to pass any video traffic if multicast-control-list is specified but has no entries.

If you want to control multicast control list checking on the MXK bridge, pick a multicast control list in the Multicast Control List field in this dialog. For creating multicast control list on MXK side, refer to [Configuring multicast control lists](#).

If you want to control multicast control list checking on the CPE connection, use the CPE Video ACL profile. For details, refer to [Creating CPE video access control \(optional\)](#).

- 6 In the **Select Bridge Template** field, select a bridge template based on the bridge type and the tag mode. It is recommended to use downlinkSingleTagged.

- 7 Specify the following bridge-related parameters for the MXK downlink bridge:

VLAN ID (0..4096): The VLAN ID the ONU inserted, translated or passed through.

SLAN ID (0..4096): The Service-provider VLAN ID the ONU inserted, translated or passed through.

VLAN COS (0..8): The Class of Service (COS) value used for VLAN tag insertion. 0 is default value.

SLAN COS (0..8): The COS value used for SLAN tag insertion. 0 is default value.

VLAN TP ID: The value of the tag protocol identifier that is being used for VLAN ID. 0x8100 is default value.

SLAN TP ID: The value of the tag protocol identifier that is being used for SLAN ID. 0x8100 is default value.

MVR Vlan Id: The value of the VLAN ID that is being used for MVR. 0x8100 is default value.

- 8 Specify the following CPE connection related parameters for the ONU UNI port:

Type: The type of the termination point (i.e. ONU UNI port) associated with the MXK bridge. It could be Ethernet UNI, IPTV UNI, PWE, SIP PLAR, SIP, or H248.

UNI Port: The index of termination point associated with the MXK bridge. It varies depends on the ONU model. For VoIP (e.g. SIP PLAR, SIP, H248) or PWE services, TP index do not need to be specified, the CPE connection is created on all the service-related UNI ports on this ONU.

UNI VLAN: The original VLAN ID of the ONU for VLAN tag insertion or passthrough.

UNI SLAN: The original Service provider LAN (SLAN) ID of the ONU for SLAN tag insertion or passthrough.

UNI VLAN COS: The Class of Service (COS) value used for P-Bit insertion or replacement. 0 is default value.

UNI SLAN COS: The COS value used for P-Bit insertion or replacement. 0 is default value.

UNI VLAN TP ID: The value of the tag protocol identifier that is being used for VLAN ID. 0x8100 is default value.

UNI SLAN TP ID: The value of the tag protocol identifier that is being used for SLAN ID. 0x8100 is default value.

DSCP To Cos Index: Assign DSCP to COS mapping to this port or not. 0 means not assigned, 1 means assigned and using dscpToCos index 1.

RG Mode: Select Not Applicable to use Dynamic OMCI. Select other modes to use Residential Gateway feature.

9 Select Using Existing Packet Rules or Use Packet Rule Templates.

10 Specify Ingress or Egress Packet Rule Group Index or Templates.

11 Click **Add**.

A CPE connection and a MXK bridge are created.

The CPE connection can be viewed in the **Manage CPE Services** dialog, under the **CPE Connection** tab.

The MXK bridge can be viewed in the **Manage Bridge Logicals** dialog.

12 To view the details on a CPE connection, select it in the **Manage CPE Services** dialog and click **View**.

To modify the CPE connection, select it and click **Modify**.

To delete the CPE connection, select it and click **Delete**.

Deleting a MXK bridge and associated CPE connections

By deleting the MXK bridge, you could remove the MXK bridge and all the associated CPE connections.

1 Right-click the device, select **Manage Bridging**.

2 In the **Bridge Logical** window, select the bridge, and click **Delete**.

3 In the **Delete confirmation** dialog, click **OK**.

Provision services with CPE Profiles

CPE profiles define the different services that are provisioned on CPEs. As shown in the flowchart, there are two kinds of CPE profiles:

- CPE shared profiles (used in **Step 4b**)

CPE shared profiles contain the common service information which is used by multiple ONU UNI ports.



Note: The CPE shared profile can only be deleted if it is not associated with any other CPE profiles.

- CPE subscriber profiles (used in **Step 4c**)

CPE subscriber profiles contain the information for an individual ONU UNI port. When creating a CPE subscriber profile on an ONU UNI port, based on different services, you can associate related CPE shared profiles with it.

For example, when creating a CPE IP subscriber profile for VoIP service, a CPE IP server profile is required to be associated with it, if there is no CPE IP server profile index specified, the default CPE IP server profile will be used.

Table 9 listed how to use CPE shared profiles and CPE subscriber profiles to provision different services (Data, Video, VoIP, PWE, RF).

As shown in the table, for Data or Video service, the creation of the CPE shared profiles and CPE subscriber profiles are not necessary, unless users want to change the default settings of those profiles. Creation of MXK downlink bridges and CPE connections (with the **CPE Connection On Device** dialog) and creation of MXK uplink bridge (with the **Bridge Logical on Device** dialog) are sufficient for creating a Data or Video service.

Table 9: Service provisioning with Dynamic OMCI

Services	MXK bridges and CPE connections	CPE Shared Profiles	CPE Subscriber Profiles
Data	Create uplink/downlink MXK bridge, and CPE connections	N/A	CPE Eth profile (Optional)
Video	Create uplink/downlink MXK bridge, and CPE connections	CPE video access profile (Optional) CPE video profile (Optional)	CPE Eth profile (Optional)
VoIP	Create uplink/downlink MXK bridge, and CPE connections	CPE VoIP server profile CPE VoIP feature profile (Default profile provided. Only for SIP or SIP PLAR) CPE VoIP media profile (Default profile provided) CPE VoIP SIP dialplan profile (Optional. Only for SIP)	CPE VoIP profile (Requires CPE VoIP server profile, CPE VoIP feature profile, and CPE VoIP media profile)
		CPE IP server profile (Default profile provided)	CPE IP profile (Requires CPE IP server profile)
PWE	Create uplink/downlink MXK bridge, and CPE connections	CPE PWE common profile (Default profile provided)	CPE PWE profile (Requires CPE PWE common profile)
		CPE IP server profile (Default profile provided)	CPE IP profile (Requires CPE IP server profile)
RF	N/A	N/A	CPE RF profile

The following sections described how to create CPE shared profiles:

- [Creating CPE video access control \(optional\)](#)
- [Creating CPE video profile and associate it with a CPE video access control list \(optional\)](#)
- [Creating a CPE IP server profile \(i.e. CPE IP common profile\)](#)
- [Creating CPE VoIP server profiles](#)
- [Creating CPE SIP dial plans for a SIP VoIP server \(optional\)](#)
- [Creating CPE VoIP features profile for SIP or SIP PLAR](#)
- [Creating CPE VoIP media profile](#)
- [Creating a CPE PWE common profile](#)

The following sections described how to create CPE subscriber profiles:

- [Creating CPE Ethernet subscriber profile \(optional\)](#)
- [Creating CPE VoIP subscriber profile and associate it with a VoIP server, a VoIP features profile, and a media profile](#)
- [Creating a CPE IP profile and associate it with a CPE IP server profile](#)
- [Creating PWE service on ONU CES ports and associate it with a CPE PWE profile](#)
- [Creating RF service on ONU RF ports](#)

Creating CPE video access control (optional)

CPE video access control profile creates an access control list, which defines which multicast addresses the remote-end video can access. That access control list can be specified later in the CPE video profile. If there is no CPE video access control profiles specified in the CPE video profile, there will be no control on the multicast addresses.



Note: The CPE video access control profile can not be deleted if this profile is the only entry in an access control list that is being associated with a CPE video profile.

To create CPE video access control profiles:

- 1** Right-click an MXK, and select **Manage USP System**.
The **Manage CPE System** dialog box appears.
- 2** Click **Video ACL** tab, and click **Add**.
The **Add CPE Video ACL** dialog box appears.
- 3** In the **Configuration** window, specify the desired values for the following fields.
ACL Index: CPE video access control list index.

ACE Index: CPE video access control entry index.

Profile Name: CPE video access control profile name.

ACL Type: Defines the video stream type. Possible values are normal (default), always-on, periodic.

Source IP: Source IP address. The default value is 0.0.0.0, that indicates that source IP address is to be ignored.

Destination Start IP: Destination IP address of the start of the multicast range.

Destination End IP: Destination IP address of the end of the multicast range.

Imputed Group Bandwidth: Imputed group bandwidth. In the unit of bytes/second. The imputed group bandwidth is used to decide whether or not to honor a join request in the presence of a max multicast bandwidth limit. The default value 0 effectively allows this table entry to avoid maximum bandwidth limitations.

- 4 Click **Add**, the new CPE video access control profile appears in the **Manage CPE System** dialog > **Video ACL** pane.
- 5 If users want to modify a CPE video access control profile, select it and then click **Modify**.
- 6 If users want to delete a CPE video access control profile, select it and then click **Delete**.

Note that if users want to delete the last CPE video access control profile in an access control list that is being associated with a CPE video profile. Users have to remove the reference in the CPE video profile first, and then delete the CPE video access control profile.

Creating CPE video profile and associate it with a CPE video access control list (optional)

This step is optional. Creation of Video bridge and CPE connections is sufficient for creating a video service. You can use the cpe-video-access-control profile and cpe-video profile, if you want to add some common video service attributes.



Note: CPE video profile can only be deleted when it is not associated with any CPE video subscriber profiles.

- 1 Right-click an MXK, and select **Manage USP System**.
The **Manage CPE System** dialog box appears.
- 2 Click **Video** tab, and click **Add**.
The **Add Video** dialog box appears.
- 3 In the **Configuration** window, specify the desired values for the following fields.

Video Index: CPE video profile index.

Profile Name: Specifies a unique CPE video profile name. 36 characters string.

Maximum Simultaneous Groups: Specifies the maximum number of dynamic multicast groups that may be joined by at any one time.

Default value 0 specifies that no administrative limit is to be imposed.

Maximum Multicast Bandwidth: Specifies the maximum imputed dynamic bandwidth, in bytes per second, that may be delivered to the client port at any one time.

Default value 0 specifies that no administrative limit is to be imposed.

Bandwidth Enforce: Value True specifies that such attempts be counted and denied. The imputed bandwidth value is taken from the dynamic access control list table, both for a new join request and for pre-existing groups. Value False specifies that attempts to exceed the max multicast bandwidth be counted but honored. By default, value is False.

ACL Index: This attribute points to a access control group list. Default value is 0. It indicates no control list is used.

- 4 Click **Add**, the new CPE video profile appears in the **Manage CPE System** dialog > **Video** pane.
- 5 If users want to modify a CPE video profile, select it and then click **Modify**.
- 6 If users want to delete a CPE video profile, select it and then click **Delete**.
- 7 Users can go to the **Manage CPE Service** dialog > **CPE Ethernet Subscriber** pane to find if any CPE video profiles are associated with a CPE Ethernet Subscriber profile.

Creating a CPE IP server profile (i.e. CPE IP common profile)

The default CPE IP server profile specified the DHCP as the host IP option. It indicates CPE will get the host IP address automatically from the DHCP server.



Note: CPE IP server profile can only be deleted when it is not associated by any CPE IP profiles.

To create a CPE IP server profile:

- 1 Right-click an MXK, and select **Manage USP System**.
The **Manage CPE System** dialog box appears.
- 2 Click **IP Common** tab, and click **Add**.
Select a template, then the **Add CPE IP Common** dialog box appears.
- 3 In the **Configuration** window, specify the desired values for the following fields.

Server Index: CPE IP server profile index.

Profile Name: Specifies a unique CPE IP server profile name. 36 characters string.

Host IP Option: Selects an IP related option. DHCP is the default value. It indicates CPE will get the host IP address automatically from the DHCP server.

Net Mask: Specifies the subnet mask for IP host services.

Gateway: Specifies the default gateway address used for IP host services, this attribute has default value 0.0.0.0.

Primary DNS: Specifies the primary DNS IP address. If this value is 0.0.0.0, no primary SIP DNS is defined. The default value is 0.0.0.0.

Secondary DNS: Specifies the secondary DNS IP address. If this value is 0.0.0.0, no second SIP DNS is defined. The default value is 0.0.0.0.

NAT: Specifies NAT, NAPT or Disable. The default value is NAT.

Secure Forward: Specifies the secure forwarding is disabled or enabled. The default value is Disable.

IGMP Function: Specifies the secure forwarding is disabled or enabled. The default value is Disable.

Default Face: Specifies the secure forwarding is disabled or enabled. The default value is Disable.

Secure Forward: Specifies the secure forwarding is disabled or enabled. The default value is Disable.

Secure Forward: Specifies the secure forwarding is disabled or enabled. The default value is Disable.

Secure Forward: Specifies the secure forwarding is disabled or enabled. The default value is Disable.

- 4 The **Firewall Access Bits** window shows the protocols allowed on the CPE WAN or LAN interfaces. It requires firewall feature to be enabled.

The protocols are listed below:

HTTP: Web Browser Traffic.

PING: ICMP Echoes used to test for connectivity.

SNMP: Simple Network Management Protocol.

SNMPTRAP: Alarms for Simple Network Management Protocol.

SSH: Secure Shell.

TELNET: Remote Terminal support.

By default, those protocol are all enabled.

- 5 Click **Add**, the new CPE IP server profile appears in the **Manage CPE System** dialog > **IP Server** pane.

- 6 If users want to modify a CPE IP server profile, select it and then click **Modify**.
- 7 If users want to delete a CPE IP server profile, select it and then click **Delete**.

Creating CPE VoIP server profiles

This section will create a CPE VoIP server profile. Each CPE VoIP server profile specifies the IP addresses or names of the primary and secondary VoIP servers, and the VoIP signalling protocol. The VoIP signalling protocol could be SIP, SIP PLAR, or H.248. This example sets it to SIP.



Note: CPE VoIP server profile can only be deleted when it is not associated by any CPE VoIP subscriber profiles.

To create VoIP server profiles.

- 1 Right-click an MXK, and select **Manage USP System**.

The **Manage CPE System** dialog box appears.

- 2 Click **VOIP Server** tab, and click **Add**.

The **Add CPE VOIP Server** dialog box appears.

- 3 In the **Configuration** pane, specify the desired values for the following fields.

Server Index: CPE VoIP server profile index.

Profile Name: Specifies a unique CPE VoIP server profile.

Primary Server: Contains the name (IP address or resolved name) of the primary MGCP or SIP proxy server that controls the signalling messages.

Secondary Server: Contains the name (IP address or resolved name) of the secondary or backup MGCP proxy server that controls the signalling messages.

Signalling Protocol: Specifies the VoIP signalling protocol. SIP, SIPLAR, or H248.

SIP Domain: Contains the host or domain part of the SIP address of record for users connected to this ONT.

SIP Registrar: Contains the name (IP address or resolved name) of the registrar server for SIP signalling messages.

Signal Reg Head Start Time (in seconds): Time in seconds prior to timeout that causes the SIP agent to start the re-registration process. Default is 360.

Signal Reg Expiry Time(in seconds): SIP registration expiration time in seconds. If 0, no expiration and no re-registration. Default is 3600.

Soft Switch: Defines the SIP gateway softswitch vendor. The format is four ASCII coded alphabetic characters[A..Z] as defined in ANSI T1.220. A value of four null characters indicates no particular vendor.

Release Timer (in seconds): Release timer in seconds. The value 0 specifies that the ONT is to use its internal default. Default is 10.

Roh Timer(in seconds): This attribute defines the time in seconds for the receiver off hook condition before ROH tone is applied. The value 0 disables ROH timing. Default value is 15.

OOB DTMF Events: Enables or disables handling of DTMF via RTP DTMF events per RFC 4733.

OOB CAS Events: Enables or disables handling of Channel-Associated Signaling (CAS) signals via RTP.

OutBound Server: Contains the name (IP address or resolved name) of the outbound proxy server for SIP signalling messages.

Port ID: Specifies the TCP/UDP port number of the VoIP protocol. The default value -1 selects the default port number for the VoIP protocol. It is 2944 for H.248 and 5060 for SIP.

MGC Termination Id Base: Specifies the base string for the H.248 physical termination id's for this ONT. This string is intended to uniquely identify an ONT. Vendor specific termination identifiers are optionally added to this string to uniquely identify a termination on a specific ONT.

DTMF Events Passing Method: If OOB DTMF Events is disabled, dtmf digits are carried along the voice path. If OOB DTMF Events is enabled, we look at the **DTMF Events Passing Method**. If **DTMF Events Passing Method** is rfc4733, dtmf digits are carried in the RTP payload. If **DTMF Events Passing Method** is sip-info, dtmf digits are carried along the signaling path in the INFO messages.

Cas Events Passing Method: If OOB CAS Events is disabled, dtmf digits are carried along the voice path. If OOB CAS Events is enabled, we look at the Cas Events Passing Method. If **Cas Events Passing Method** is rfc4733, dtmf digits are carried in the RTP payload. If **Cas Events Passing Method** is sip-info, dtmf digits are carried along the signaling path in the INFO messages.

RTP DSCP: Set the Differentiated services codepoint value for RTP streams associated with the VoIP server.

Signaling DSCP: Set the Differentiated services codepoint value for signalling messages associated with the VoIP server.

SIP Registration Retry Time (in seconds): SIP registration retry time in seconds. Default is 60.

- 4 Click **Add**, the new CPE VoIP server profile appears in the **Manage CPE System** dialog > **VOIP Server** pane.
- 5 If users want to modify a CPE VoIP server profile, select it and then click **Modify**.

- 6 If users want to delete a CPE VoIP server profile, select it and then click **Delete**.

Creating CPE SIP dial plans for a SIP VoIP server (optional)

CPE SIP dialplans are only for SIP. You can create up to 30 CPE SIP dialplans for each CPE SIP VoIP server.

- 1 Right-click an MXK, and select **Manage USP System**.

The **Manage CPE System** dialog box appears.

- 2 Click **SIP Dial Plan** tab, and click **Add**.

The **Add SIP Dial Plan** dialog box appears.

- 3 In the **Configuration** pane, specify the desired values for the following fields.

VOIP Server Index: Specifies a CPE VoIP server profile index.

Dial Plan Index: Specifies a unique CPE SIP dial plan index.

Dial Plan Format: Defines the dialplan format standard that is supported on the ONT for VoIP service. It could be h248, nsc, or vendor-specific. The default value is h248.

Dial Plan String: Defines the dialplan used by the VoIP service.

- 4 Click **Add**, the new CPE SIP dialplan profile created for SIP VoIP server appears in the **Manage CPE System** dialog > **SIP Dial Plan** pane.
- 5 If users want to modify a CPE SIP Dial Plan profile, select it and then click **Modify**.
- 6 If users want to delete a CPE SIP Dial Plan profile, select it and then click **Delete**.

Creating CPE VoIP features profile for SIP or SIP PLAR

Create a CPE VoIP features profile for the VoIP service.



Note: The CPE VoIP features profile is only applicable for SIP or SIP PLAR VoIP server.



Note: CPE VoIP feature profile can only be deleted when it is not associated by any CPE VoIP subscriber profiles.

- 1 Right-click an MXK, and select **Manage USP System**.

The **Manage CPE System** dialog box appears.

- 2 Click **VOIP Features** tab, and click **Add**.

The **Add SIP Dial Plan** dialog box appears.

- 3 In the **Configuration** pane, specify the desired values for the following fields.

Feature Index: a CPE VoIP feature profile index.

Profile Name: By only specifying profile-name field, the profile will be created with all the default settings.

Announce Type: Specifies the treatment when a subscriber goes off hook but does not attempt a call. Silence, Recorder Tone, Fast Busy, Voice, or Not Applicable.

- 4 You can change the default settings of the CPE VoIP features.
Click **CID** to show default settings of the caller ID features.
Click **Call Waiting** to show default settings of the call waiting features.
Click **Progress Or Transfer** to show default settings of the call processing features.
Click **Presentation** to show default settings of the call presentation features.
Enable or disable the above CPE VoIP feature settings as you desired.
- 5 Click **Add**, the new CPE VoIP feature profile appears in the **Manage CPE System** dialog > **VOIP Features** pane.
- 6 If users want to modify a CPE VoIP feature profile, select it and then click **Modify**.
- 7 If users want to delete a CPE VoIP feature profile, select it and then click **Delete**.

Creating CPE VoIP media profile

Create a CPE VoIP media profile for the VoIP service.



Note: CPE VoIP media profile can only be deleted when it is not associated by any CPE VoIP subscriber profiles.

- 1 Right-click a device, and select **Manage USP System**.
The **Manage CPE System** dialog box appears.
- 2 Click **VOIP Media** tab, and click **Add**.
The **Add CPE VOIP Media** dialog box appears.
- 3 In the **Configuration** pane, specify the desired values for the following fields.

Media Index: a CPE VoIP media profile index.

Profile Name: Specifies a unique CPE VoIP media profile name.

Echo Cancel: Turns on or off echo cancellation.

Fax Mode: Selects the fax mode.

Codec First/Second/Third/Fourth Order: Specifies the codec selection as defined by RFC 3551. There are four orders.

Period First/Second/Third/Fourth Order: Packet period selection interval in milliseconds. There are four orders.

Silence Suppression First/Second/Third/Fourth Order: Specifies whether silence suppress is on or off. There are four orders.

Minimum HookFlash Timer(in milli seconds): The Minimum Hookflash Timer specifies the minimum timer that qualifies for a hookflash. Any loop open below this time will be ignored as a glitch. The Default value is 100.

Maximum HookFlash Timer (in milli seconds): The Maximum Hookflash Timer specifies the maximum timer that qualifies for a hookflash. Any loop open more than this timer will be considered as a onhook. The default value is 1550.

- 4 Click **Add**, the new CPE VoIP media profile appears in the **Manage CPE System** dialog > **VOIP Media** pane.
- 5 If users want to modify a CPE VoIP media profile, select it and then click **Modify**.
- 6 If users want to delete a CPE VoIP media profile, select it and then click **Delete**.

Creating a CPE PWE common profile

Create a CPE PWE common profile for the common PWE service or use the default CPE PWE profile.



Note: CPE PWE common profile can only be deleted when it is not associated by any CPE PWE subscriber profiles.

- 1 Right-click an MXK, and select **Manage USP System**.
The **Manage CPE System** dialog box appears.
- 2 Click **PWE Common** tab, and click **Add**.
The **Add PWE** dialog box appears.
- 3 In the **CPE PWE Common** window, specify the desired values for the following fields.

PWE Common Index: a CPE PWE profile index.

Profile Name: Specifies a unique CPE PWE profile name.

Line Type: Specifies the line type used. DS1 or E1. Default value is E1.

Encoding: Specifies the line coding scheme. B8ZS is used for DS1 line-type, HDB3 is used for E1 line-type. Default value is HDB3.

Timing Mode: Selects the timing mode of the TDM service. If RTP is used. Default value is network.

Payload Size: Specifies the number of payload bytes per packets. Valid only if service-type is unstructured or octetalignedunstruct (unstructured octet aligned). Valid choices depend on the TDM service, but must include the following. Other choices are at the vendor's discretion.

Values:

192: For DS1 service

200: For DS1 service, required only if service-type octetalignedunstruct is selected

256: For E1 service

1024: For DS3 and E3 service.

Jitter Buffer Max: Specifies the desired maximum depth of the playout buffer in the PSN to TDM direction. The value is expressed as a multiple of the 125 microseconds frame rate. The value 0 selects the ONT's internal policy.

Jitter Buffer Desired: Specifies the desired nominal fill depth of the playout buffer in the PSN to TDM direction. The value is expressed as a multiple of the 125 microseconds frame rate. The value 0 selects the ONT's internal policy.

Differentiated Services Code Point (DSCP): Set the DSCP value for cpe pwe.

- 4 Click **Add**, the new CPE PWE profile appears in the **Manage CPE System** dialog > **PWE** pane.
- 5 If users want to modify a CPE PWE profile, select it and then click **Modify**.
- 6 If users want to delete a CPE PWE profile, select it and then click **Delete**.

Creating CPE Ethernet subscriber profile (optional)

By default, the admin-state of the CPE Ethernet UNI port is up after creation of CPE connection on that CPE Ethernet UNI port. Because of that, the Data and Video traffic can run on this Ethernet UNI port without further configuration.

You could change the default Ethernet physical configurations as you desired in the **Ethernet Subscriber on Device** dialog. With this dialog, the CPE Ethernet subscriber profile is created *manually*. The Ethernet UNI port ID specified in this command must match the one assigned in the **CPE Connection On Device** dialog when creating downlink bridge and CPE connection.

Note that a CPE ethernet subscriber profile will also be created *automatically* if users set the ONU UNI ethernet port's admin-state or modify the port speed with the **OMCI Port Status** dialog. For the details, refer to [Configuring subscriber ports on ONT/ONU on page 235](#)

To create a CPE Eth subscriber profile manually:

- 1 Right-click an MXK, and select **Manage USP Service**.
The **Manage CPE Services** dialog box appears.
- 2 Click **Ethernet Service** tab, and click **Add**.
The **Ethernet Service on Device** dialog box appears.
- 3 In the **Select ONU Physical** pane, expand the tree, and then select an ONU port.
- 4 In the CPE ETH Subscriber pane, specify the desired values for the following fields.

Port number: Ethernet UNI port ID of the physical subscriber-facing interface on the ONU.

Admin Status: Activates or deactivates the functions performed by the Ethernet port for this subscriber. Possible values are up, down. Default value is up.

Description: Describes the CPE Ethernet subscriber profile instance.

Rate: Sets the Ethernet port rate. Possible values are auto (default), 10, 100, 1000.

Duplex: Sets the Ethernet port duplex. Possible values are auto (default), full, half.

Line Status: This field is for enabling/disabling alarm reporting from this CPE UNI.

In order for ZMS to synchronize the new alarms, the **OMCI ONU Physical Traps** field in the **Modify GponOnu Physical Configuration** window must be Enabled. Note that enabling or disabling OMCI ONU physical traps will increase ZMS alarm refresh time, and require significant system resources. Therefore, we recommend that it only be used for premium customers.

Alarm Severity: This field is for specifying the severity level of all the alarms from this CPE UNI. Once the **Line Status** is enabled, the setting in the alarm severity will take effect too. By default, the alarm severity is Major, you can change it to Warning, Minor, or Critical.

Power Shed: The Power shedding enable/disable per Port feature is only for zNIDs that support Power Over Ethernet(PoE).

In order to extend battery life on the ONU during AC power outages, some services may be shutdown, and some services maybe kept such as VoIP services for emergency contact or data services on an important computer, etc.

When power shedding is enabled at the CPE system level and the CPE is operating on battery power during an AC power outage, Power Shed controls the enable/disable state of each Ethernet port. Ports with power shedding enabled will remain operational on battery power, while disabled ports will be shut down to conserve battery power. Power shedding for the Ethernet ports are disabled by default.

Power shedding in the CPE system level is controlled by the Power Shutdown Delay field in the CPE system common profile. The Power Shutdown Delay is 0 means disabled; the Power Shutdown Delay in the range of 1 to 60 means enabled and defines the amount of time in minutes the ONU waits after an AC power outage before shut-down.

The Power Restore Delay in the CPE system level determines the amount of time in minutes the ONU will wait after AC power is restored before reactivating services. The value is in the range of 0 to 10.

Power Range: The maximum PoE power allowed per port is defined in the Power Range field for each Ethernet port. The choices of this field are High, Low, Medium, Disabled (no PoE Power will be provided), and Custom. The actual values of the High, Low, Medium choices are defined at the CPE side based on the CPE model. The Custom is the recommended value for users. After specified Custom in the Power Range field, users can customize the value of the maximum PoE power in the Custom Power Range field. The value of the Custom Power Range is in the range of 0.0 to 30.8, in the unit of 0.1 watts.

Custom Power Range: Customize the value of the maximum PoE power. The value is in the range of 0.0 to 30.8, in the unit of 0.1 watts.

Video Index: Associated CPE video profile. Note: The video-profile field is only for video service.

Traffic Management Index: Associated CPE Traffic Management Profile.

- 5 Click **Add**, the new CPE Ethernet Subscriber profile appears in the **Manage CPE Services** dialog > **Ethernet Service** pane.
- 6 To change the settings in that profile, you can select it and click **Modify**.

Creating CPE VoIP subscriber profile and associate it with a VoIP server, a VoIP features profile, and a media profile

Create a CPE VoIP subscriber profile on ONU POTS ports. When creating a CPE VoIP subscriber profile, user must specify a VoIP server profile, associate the VoIP server information to the POTS port. There is no default VoIP server profile. A VoIP features profile and a VoIP media profile are also required when creating the CPE VoIP subscriber profile, if users do not specify these two profiles, then the default profiles are used.

Note that a CPE VoIP subscriber profile will also be created *automatically* if users set the ONU UNI POTS port's admin-state with the **OMCI Port Status** dialog. For the details, refer to [Configuring subscriber ports on ONT/ONU on page 235](#).

To create a CPE VoIP subscriber profile on an ONU manually:

- 1 Right-click an MXK, and select **Manage USP Service**.
The **Manage CPE Services** dialog box appears.
- 2 Click **VOIP Service** tab, and click **Add**.

The **VOIP Service on Device** dialog box appears.

- 3 In the **Select ONU Physical** pane, expand the tree, and then select an ONU port.
- 4 In the CPE VOIP Subscriber pane, specify the desired values for the following fields.

Port number: POTS UNI port ID of the physical subscriber-facing interface on the ONU.

Admin Status: Activates or deactivates the functions performed by the POTS port for this subscriber. Possible values are up, down. Default value is up.

Dial Number: Specifies the subscriber directory number.

Note: The dial-number field is only used with SIP.

User Name: Defines the customer id used for the display attribute in outgoing SIP messages.

Note: The username field is only used with SIP.

Password: Contains the SIP user identification used for authentication.

Note: The password field is only used with SIP

Rx Gain (-12 to 6) (in dB): Specifies a gain value for the received signal in the form of a 2s complement number. Valid values are -12 (-12.0 dB) to 6 (+6.0 dB).

Tx Gain (-12 to 6) (in dB): Specifies a gain value for the transmit signal in the form of a 2s complement number. Valid values are -12 (-12.0 dB) to 6 (+6.0 dB).

Service Index: Associated cpe-voip-feature profile.

Features Index: Associated cpe-voip-feature profile. If user specify profile index 1 or omit this field, a default profile is used.

Note: The voip-features-profile field is only used with SIP.

Media Index: Associated cpe-voip-media profile. If user specify profile index 1 or omit this field, a default profile is used.

- 5 Click **Add**, the new CPE VOIP Subscriber profile appears in the **Manage CPE Services** dialog > **VOIP Service** pane.
- 6 If users want to modify a CPE VoIP Subscriber profile, select it and then click **Modify**.
- 7 If users want to delete a CPE VoIP Subscriber profile, select it and then click **Delete**.

Creating a CPE IP profile and associate it with a CPE IP server profile

Create a CPE IP profile and associate it with a CPE IP server. If there is no CPE IP server specified, the default CPE IP server will be used.

- 1 Right-click an MXK, and select **Manage USP Service**.
The **Manage CPE Services** dialog box appears.
- 2 Click **IP** tab, and click **Add**.
The **IP on Device** dialog box appears.
- 3 In the **Select ONU Physical** pane, select an ONU interface ID.
- 4 In the **CPE IP** pane, specify the desired values for the following fields.
Server Type: Specifies a service type. VOIP, PWE, or WIFI.
Host IP: Specifies the address used for IP host services. The default value is 0.0.0.0.
IP Server Index: Associates a CPE IP server profile with this host IP. If this field is not specified or is 1, the default CPE IP server profile (index 1) with DHCP enabled will be used.
- 5 Click **Add**, the new CPE IP profile appears in the **Manage CPE Services** dialog > **IP** pane.
- 6 If users want to modify a CPE IP profile, select it and then click **Modify**.
- 7 If users want to delete a CPE IP profile, select it and then click **Delete**.

Creating PWE service on ONU CES ports and associate it with a CPE PWE profile

Create a CPE PWE subscriber profile on ONU CES ports *manually* and associate it with a CPE PWE profile. If there is no CPE PWE profile specified, the default CPE PWE profile will be used.

Note that a CPE PWE subscriber profile will also be created *automatically* if users set the ONU UNI CES port's admin-state with the **OMCI Port Status** dialog. For the details, refer to [Configuring subscriber ports on ONT/ONU on page 235](#)

To create a CPE PWE subscriber profile with the **cpe pwe add** command:

- 1 Right-click an MXK, and select **Manage USP Service**.
The **Manage CPE Services** dialog box appears.
- 2 Click **PWE Service** tab, and click **Add**.
The **PWE Service on Device** dialog box appears.
- 3 In the **Select ONU Physical** pane, expand the tree, and then select an ONU port.
- 4 In the **CPE PWE Subscriber** pane, specify the desired values for the following fields.
Port Number: CES UNI port ID of the physical interfaces.
Admin State: Activates or deactivates the functions performed by the CES port for this subscriber. Possible values are up, down. Default value is up.

Description: Describes the CPE pwe subscriber profile instance.

Near End Port: When the pseudowire service is transported via IP, this attribute specifies the port number of the near-end TCP/UDP service. Default is 57000 + port number.

Far End IP: When the pseudowire service is transported via IP, this attribute specifies the IP address or resolved name of the far-end termination point.

Far End Port: When the pseudowire service is transported via IP, this attribute specifies the port number of the far-end TCP/UDP service. Default is 57000 + port number.

Line Length (in Feet): Specifies the length of the twisted pair cable from a DS1 physical UNI to the DSX-1 cross-connect point. In the unit of feet. Default is 0.

PWE Common Index: Points to the associated CPE PWE profile. If this field is not specified or is 1, the default CPE PWE profile (index 1) will be used.

Line Status: This field is for enabling/disabling alarm reporting from this CPE UNI.

In order for ZMS to synchronize the new alarms, the **OMCI ONU Physical Traps** field in the **Modify GponOnu Physical Configuration** window must be Enabled. Note that enabling or disabling OMCI ONU physical traps will increase ZMS alarm refresh time, and require significant system resources. Therefore, we recommend that it only be used for premium customers.

Alarm Severity: This field is for specifying the severity level of all the alarms from this CPE UNI. Once the **Line Status** is enabled, the setting in the alarm severity will take effect too. By default, the alarm severity is Major, you can change it to Warning, Minor, or Critical.

Destination MAC Address: Each connection requires the configuration of the MAC Address of the peer Ethernet bridged device. If the destination MAC address is incorrectly configured, all PWE packets will be discarded by the remote PWE device. If the field is empty, MAC address Mode is dynamic. The destination MAC address is determined from ARP.

Outer MPLS Label: The outer MPLS label identifies the MPLS LSP, used to tunnel the TDMoMPLS packets through the MPLS network. It is also known as the tunnel label or the transport label.

Inner MPLS Label: Inner MPLS label is also known as the PW label or the interworking label, which contains the bundle identifier used to multiplex multiple bundles within the same tunnel. It is used for all packets transmitted to and received from the remote PWE device

Emulated Circuit ID: Emulated Circuit ID (ECID) defines the destination that will be used for all packets transmitted to and received from the remote PWE device

- 5 Click **Add**, the new CPE PWE Subscriber profile appears in the **Manage CPE Services** dialog > **PWE Service** pane.
- 6 If users want to modify a CPE PWE Subscriber profile, select it and then click **Modify**.
- 7 If users want to delete a CPE PWE Subscriber profile, select it and then click **Delete**.

Creating RF service on ONU RF ports

This section provide procedure to create a CPE RF subscriber profile on ONU RF ports *manually*.

Note that a CPE RF subscriber profile will also be created *automatically* if users set the ONU UNI RF port's admin-state with the **OMCI Port Status** dialog. For the details, refer to [Configuring subscriber ports on ONT/ONU on page 235](#)

To create a CPE RF subscriber profile:

- 1 Right-click an MXK, and select **Manage USP Service**.
The **Manage CPE Services** dialog box appears.
- 2 Click **RF Service** tab, and click **Add**.
The **RF Service on Device** dialog box appears.
- 3 In the **Select ONU Physical** pane, expand the tree, and then select an ONU port.
- 4 In the **CPE RF Subscriber** pane, specify the desired values for the following fields.

Port Number: RF UNI port ID of the physical interfaces.

Admin Status: Activates or deactivates the functions performed by the RF port for this subscriber. Possible values are up, down. Default value is up.

Line Status: This field is for enabling/disabling alarm reporting from this CPE UNI.

In order for ZMS to synchronize the new alarms, the **OMCI ONU Physical Traps** field in the **Modify GponOnu Physical Configuration** window must be Enabled. Note that enabling or disabling OMCI ONU physical traps will increase ZMS alarm refresh time, and require significant system resources. Therefore, we recommend that it only be used for premium customers.

Alarm Severity: This field is for specifying the severity level of all the alarms from this CPE UNI. Once the **Line Status** is enabled, the setting in the alarm severity will take effect too. By default, the alarm severity is Major, you can change it to Warning, Minor, or Critical.

- 5 Click **Add**, the new CPE RF Subscriber profile appears in the **Manage CPE Services** dialog > **RF Service** pane.

- 6 If users want to modify a CPE RF Subscriber profile, select it and then click **Modify**.
- 7 If users want to delete a CPE RF Subscriber profile, select it and then click **Delete**.

Activate ONT/ONU in Dynamic OMCI

As shown in the **Step 6**, only need to activate ONU once to add the ONU to the system. Note that in Dynamic OMCI, after changing the service configuration on an activated ONU, the services configuration will be updated automatically. Thus you can activate the ONU at any time after specifying this ONU is provisioned by Dynamic OMCI, it is not necessary to do it after performing all the service provisioning.

Activating ONT/ONU in Dynamic OMCI

After specifying internal ME profile for the ONT/ONU, you can activate this ONT/ONU with serial number.

During activation process, when the OLT communicates with the ONT/ONU, the OLT retrieves the current variable settings on this ONT/ONU.

To activate an ONT/ONU, perform the following tasks:

- 1 After an internal ME profile is assigned on an ONT/ONU, the names of the internal ME profile name will be displayed in the **Modify GponOnu Physical Configuration** dialog box.

- 2 Right-click the OLT port this ONU belongs to, select **Assign Serial Numbers**:

The **Modify Serial Number Table** dialog appears.

- 3 Select the ONT/ONU port from the pull-down menu to associate with a serial number. And click **Apply**.
- 4 Verify this ONT/ONU is activated with serial number and internal ME profile.

Right-click this ONT/ONU port in the tree view, select **Modify**. The **Modify GponOnu Physical Configuration** window appears. And then click **Configuration** tab.

ONT Serial No Vendor Specific field shows the associated serial number.

OMCI ME file name shows the associated internal ME profile name.

Onu Added is True shows this ONT/ONU is activated.

- 5 If you want to disable an ONT/ONU and clear the serial number for this ONT/ONU, uncheck the **Onu Added** field and then click **Modify**.

Residential Gateway (RG) Features Provisioning

There are GPON zNIDs where ONU and RG functions are physically integrated into the same device - these ONTs are referred to as Dual-Managed ONTs. Two Configuration Modes exist to facilitate the provisioning of Dual-Managed ONTs under the Unified Service Provisioning umbrella.

This section provides information on how to install and provision Dual-Managed GPON zNIDs with Unified Service Provisioning using ZMS on the MXK.

Dual-Managed GPON zNIDs may be provisioned via the ONT-Only Configuration Mode or by the ONT+RG Configuration Mode. With the ONT-Only mode, the zNID is managed via OMCI (as described in [Dynamic OMCI, page 244](#) *Dynamic OMCI*) and this is useful where services are limited to L2 Data and Video, or VoIP in simpler bridging cases. The vast majority of GPON zNIDs have been deployed in this configuration, with OMCI used exclusively for configuration and control. The provisioning requirements for this operating mode are defined by the ITU-T G.988 Standard.

However, provisioning RG capabilities on the Dual-Managed GPON zNIDs requires the use of the ONT+RG Configuration Mode. With this Mode an ONT+RG connection is managed through a combination of OMCI and SNMP. (Note that the users do not have to know what management protocols are used underneath when you provision the zNIDs.) Here, SNMP complements OMCI by being responsible for the configurations and management of the RG functions.

Both configuration modes allow for pre-provisioning, where the GPON zNIDs will be automatically configured once they are connected to the PON and come on-line.

This chapter describes the following topics:

- [RG modes in RG provisioning, page 271](#)
- [OMCI GPON zNID with RG features installation for Triple services, page 272](#)
- [CPE System Level Default Settings on page 286](#)
- [Static Configuration on the WAN side interfaces \(without DHCP\) on page 288](#)
- [Static configuration on the LAN side interfaces with a new DHCP server on page 290](#)
- [Configuration of Static Routes on page 291](#)
- [Configuration of Firewall on page 293](#)
- [Configuration of DHCP server on page 297](#)
- [Configuration of PPPoE username and password on page 298](#)

- [Configuration of TR-069 on page 298](#)

RG modes in RG provisioning

In RG provisioning, the MXK bridge and CPE connection can have one-to-one and one-to-many mappings.

The one-to-many mapping is one MXK bridge created on a GEM port that maps to multiple CPE connections created on multiple ONU UNI ports.

Creation of RG enabled CPE connections is very similar to Dynamic OMCI CPE connection creation with the following exceptions:

- **RG Mode** shall be set to Brouted, Bridged, or Bridged PPPOE. Not specifying the **RG Mode** will make the CPE connection add request to be treated as dynamic OMCI type connection
- TR-69 **Type** option is only applicable for RG enabled CPE connections

In ZMS, RG mode can be set by setting the **RG Mode** field in the **CPE Connection On Device** window:

- Bridged

The LAN-side interfaces and Wireless LAN interfaces can be a member of a bridged VLAN. A bridged VLAN can optionally have an IP address assigned to it for the purpose of enabling management, or supporting VoIP clients or PWE.

A RG bridge is created if Bridged mode is specified in the **CPE Connection On Device** window. In the case of an ONU model only support ONU+RG configuration mode, does not support ONU-Only configuration mode(e.g. zNID 26xx, 42xx, 9xxx), a RG bridge is still created even without Bridged mode is explicitly specified.

- Brouted

The Brouted mode operates like a bridged VLAN for all LAN-side interfaces, and as a routed VLAN for the WAN-side interface. In rg-brouted mode, there are only two IP interfaces: one for the routed WAN-side interface, and another for the bridged LAN-side interfaces.

A Brouted VLAN may have multiple LAN ports as members of the VLAN, and all ports will use the same IP subnet, and therefore the same DHCP server and IP server.

- Bridged PPPOE

The PPPoE/Bridged VLANs are similar to Brouted VLANs, but the WAN interface is a PPPoE client that establishes a PPPoE tunnel to an upstream BRAS. On the LAN side of a PPPoE/Bridged VLAN, all ports will be members of the same IP Subnet.

If it is not a PPPoE connection, after creating bridges and CPE connections in the **CPE Connection On Device** window, the zNid is ready to provide service. For PPPoE, the users have to set PPPoE user-ID and password too. (Refer to [Configuration of PPPoE username and password on page 298.](#))

[Table 10](#) provides a summary on how to add bridges for supported services in different RG operating modes.

Table 10: Creating services in RG by using the CPE Connection On Device window

Services	RG Mode field	Type field
Data	Brouted (preferred mode for Data)	Ethernet UNI
	Bridged	Ethernet UNI
	Bridged PPPOE	Ethernet UNI
Video (When creating Video service, you also need to specify Multicast Control List field and Max Number of Multicast Streams field)	Bridged (preferred mode for Video)	IPTV UNI
	Brouted	IPTV UNI
	Bridged PPPOE	IPTV UNI
Voice	Bridged (preferred mode for Voice)	SIP
	Brouted	SIP
	Bridged PPPOE	SIP
TR-069	Bridged (preferred mode for TR-069)	TR69
	Brouted	TR69
	Bridged PPPOE	TR69

OMCI GPON zNID with RG features installation for Triple services

In this section, we will provision Data service, Video service, VoIP service on the same ONU, just the MXK bridge interface, GEM port setup, GPON traffic profile, VLAN, UNI ports are different. For ease of discussion each of the applications is described separately in this section.

Generally these are the steps to follow to configure the MXK to be able to manage OMCI GPON zNIDs with RG features:

Creation of Data service in RG

This section shows how to create Data service on a zNID Ethernet Uni-port with Brouted mode in the **CPE Connection On Device** window.

- [Associating a GPON traffic profile to the ONU, page 273](#)
- [Specifying internal ME profile for the ONU, page 273](#)

Only need to specify the internal ME profile once for each ONU.

- [Creating uplink/downlink MXK bridges, and CPE connections in RG-brouted mode for data service, page 273](#)
- [Activating the ONU, page 275](#)

Only need to activate the ONU once.

Associating a GPON traffic profile to the ONU

In the **CPE Connection On Device** window:

- 1 If you select **Use GTP Index**, you can click the **GTP Index** browse button and select an existing GPON traffic profile that stored in this device. The settings in the GPON traffic profile will be displayed with the GTP index in the **Select Gpon Traffic Profile Index** field.
- 2 If you select **Use GTP Template**, you can click the **GTP Template** browse button and select a GPON traffic profile template that stored in this ZMS server.
- 3 If you want to create a new GPON traffic profile, refer to [Configure GPON traffic profile, page 216](#).

Specifying internal ME profile for the ONU

By specifying the ONU internal ME profile in the initial setup on an ONU, the MXK knows this ONU model is provisioned by RG.

You only need to specify the ME profile once.

To specify an internal ME to the ONU in the **CPE Connection On Device** window, select the ONU in the tree view, and then click the **ONU Internal ME** browsing button, and then select an internal ME profile, at last click **OK**.

Creating uplink/downlink MXK bridges, and CPE connections in RG-brouted mode for data service

In the example below, Ethernet Uni-port 1 in the RG is member of the Brouted VLAN 100. NAT is enabled on the WAN side. When creating the LAN-side interfaces in the same RG VLAN, one DHCP server and IP common server will be assigned to all interfaces. By default, the first assigned index number is 100001, and the IP subnet is 192.168.1.1.

The DHCP server index and IP server index number will be increased automatically if you created new CPE connection in another RG VLAN.

You can use the default DHCP server and IP server or create and assign another DHCP server and IP common server to the LAN-side interface as you desired. For the details, refer to [Configuration of DHCP server on page 297](#).

- 1 Create an uplink bridge interface on the MXK.
 - a Right-click the MXK, and then select **Manage Bridging**.

The **Manage Bridge Logicals** window appears.

- b** In the **Bridge Logical** pane, click **Add**.

The **Bridge Logical on Device** window appears.

- c** Select an uplink port, select **Uplink (802.1 q)** type, specify the tag mode, and then specify the VLAN ID, and other uplink bridge related parameters. Click **Add**.

- 2** Create a downlink MXK bridge, and a connection between an ONT 1-4-1-1 GEM port 303 and a CPE UNI Ethernet port 1 on a VLAN 100.

- a** Right-click the MXK, and then select **Manage USP Services**.

The **Manage CPE Services** window appears.

- b** In the **CPE Connection** pane, click **Add**.

The **CPE Connection On Device** window appears.

- c** Select the ONU port that you specified internal ME profile. This example selects 1-4-1-1.

- d** Select **Manual Select GEM port** (default) or **Auto Select GEM port**.

If you select **Manual Select GEM Port**, then specify the GEM port ID in the **GEM Port Id** field within the range of 257 to 3828. This example specifies 303.

Make sure the GTP is specified on this GEM port.

- e** Specify the bridge related parameters:

Select the Bridge type after browsing the bridge templates. This example selects DownlinkSingleTagged.

Specify VLAN ID. This example uses 100.

And other downlink bridge related parameters.

- f** Specify the CPE connection related parameters:

Specify the UNI port type, for data it must be Ethernet UNI.

Specify UNI port ID. This example uses 1.

Specify RG Mode. Note: RG Mode must be specified for RG provisioning. This example uses BRouted.

And other Ethernet UNI port related parameters.

- 3** View the bridges.

You can view the uplink and downlink bridges in the **Manage Bridge Logicals** window > **Bridge Logical** pane.

- 4** View the CPE connection, WAN interface, and LAN interface.

You can view them in the **Manage CPE Services** window > **CPE Connection** pane.

Note: If this is a PPPoE connection, you can view PPPoE parameters in this pane too.

Activating the ONU

Activate the ONU to add it to the system. In Unified Service Provisioning, after changing the service configuration on an activated ONU, the services configuration will be updated automatically.

For details, refer to [Activate ONT/ONUs by assigning serial number, page 207](#).

Creation of Video service in RG

This section shows how to create Video service on a zNID Ethernet Uni-port with rg-bridged mode.

- [Associating a GPON traffic profile to the ONU, page 273](#)
Same as in the **Creation of Data service in RG** section.
- [Creating uplink/downlink MXK bridges, and CPE connections in RG-bridged mode for Video service, page 275](#)

Creating uplink/downlink MXK bridges, and CPE connections in RG-bridged mode for Video service

In the example below, Ethernet Uni-port 2 in the RG is member of the RG-bridged VLAN 200.

- 1 Create an uplink bridge interface on the MXK.
 - a Right-click the MXK, and then select **Manage Bridging**.
The **Manage Bridge Logicals** window appears.
 - b In the **Bridge Logical** pane, click **Add**.
The **Bridge Logical on Device** window appears.
 - c Select an uplink port, select **Uplink (802.1 q)** type, specify the tag mode, and then specify the VLAN ID, and other uplink bridge related parameters. Click **Add**.
- 2 Create a downlink MXK bridge, and a connection between the ONT 1-4-1-1 GEM port 403 and the CPE untagged UNI Eth 2 on VLAN 200.
 - a Right-click the MXK, and then select **Manage USP Services**.
The **Manage CPE Services** window appears.
 - b In the **CPE Connection** pane, click **Add**.
The **CPE Connection On Device** window appears.
 - c Select the ONU port that you specified internal ME profile. This example selects 1-4-1-1.

- d** Select **Manual Select GEM port** (default) or **Auto Select GEM port**.

If you select **Manual Select GEM Port**, then specify the GEM port ID in the **GEM Port Id** field within the range of 257 to 3828. This example specifies 403.

Make sure the GTP is specified on this GEM port.

- e** Specify the bridge related parameters:

Select the Bridge type after browsing the bridge templates. This example selects DownlinkSingleTagged.

Specify VLAN ID. This example uses 200.

And other downlink bridge related parameters.

- f** Specify the CPE connection related parameters:

Specify the UNI port type, for video it must be IPTV UNI.

Specify UNI port ID. This example uses 2.

Specify RG Mode. Note: RG Mode must be specified for RG provisioning. This example uses Bridged.

And other IPTV UNI port related parameters.

Creation of Voice service in RG

This section shows how to create Voice service on all the POTS ports in a zNID with Bridged mode.

- [Associating a GPON traffic profile to the ONU, page 273](#)
Same as in the **Creation of Data service in RG** section.
- [Creating uplink/downlink MXK bridges, and CPE connections in RG-bridged mode for Voice service, page 276](#)
- [Creating IP Common profile for Voice service \(Optional\), page 277](#)

Creating uplink/downlink MXK bridges, and CPE connections in RG-bridged mode for Voice service

In the example below, POTS ports in the RG are members of the RG-bridged VLAN 300.

- 1** Create an uplink bridge interface on the MXK.
 - a** Right-click the MXK, and then select **Manage Bridging**.
The **Manage Bridge Logicals** window appears.
 - b** In the **Bridge Logical** pane, click **Add**.
The **Bridge Logical on Device** window appears.

- c Select an uplink port, select **Uplink (802.1 q)** type, specify the tag mode, and then specify the VLAN ID, and other uplink bridge related parameters. Click **Add**.
- 2 Create a downlink MXK bridge, and a connection between the ONT 1-4-1-1 GEM port 503 and the CPE UNI POTS ports on VLAN 300.
 - a Right-click the MXK, and then select **Manage USP Services**.
The **Manage CPE Services** window appears.
 - b In the **CPE Connection** pane, click **Add**.
The **CPE Connection On Device** window appears.
 - c Select the ONU port that you specified internal ME profile. This example selects 1-4-1-1.
 - d Select **Manual Select GEM port** (default) or **Auto Select GEM port**.
If you select **Manual Select GEM Port**, then specify the GEM port ID in the **GEM Port Id** field within the range of 257 to 3828. This example specifies 503.
Make sure the GTP is specified on this GEM port.
 - e Specify the bridge related parameters:
Select the Bridge type after browsing the bridge templates. This example selects DownlinkSingleTagged.
Specify VLAN ID. This example uses 300.
And other downlink bridge related parameters.
 - f Specify the CPE connection related parameters:
Specify the UNI port type, this example selects SIP.
Specify RG Mode. Note: RG Mode must be specified for RG provisioning. This example uses Bridged.
And other Voice UNI port related parameters.

Creating IP Common profile for Voice service (Optional)

This step is optional. If zNID is using DHCP (default setting) to get voice host IP address, you can skip this step.

If you want to assign static IP address to the zNID, you need to create a static IP common profile on WAN interface and assign the static IP address to the WAN interface. For the detail configuration, see [Static Configuration on the WAN side interfaces \(without DHCP\)](#), page 288.

Creation of Data service on Wireless interfaces

This section shows how to create Data service on a zNID Wireless interface with rg-brouted mode.

- [Creating uplink/downlink MXK bridges, and CPE connections in RG-brouted mode, page 278](#)
- [Creating CPE WLAN subscriber profile and associate it with a CPE WLAN common profile or CPE WLAN common advance profile \(optional\), page 279](#)
- [Creating CPE WLAN common profile \(optional\), page 280](#)
- [Creating CPE WLAN common advance profile \(optional\), page 282](#)

Creating uplink/downlink MXK bridges, and CPE connections in RG-brouted mode

This example creates the data service on WLAN 1 interface (i.e. SSID 0 in the ONT WebUI). This WLAN interface is using same VLAN and GEM port used when we created data service on Uni Ethernet 1.

- 1 Do not need to create uplink interface. This example uses the VLAN that was already created on the uplink for data service.
- 2 Create a downlink MXK bridge, and a connection between the ONT 1-4-1-1 GEM port 303 and the CPE LAN side wireless interface 1 (i.e. SSID 0 in the ONT WebUI) on VLAN 100 for untagged packets.

- a Right-click the MXK, and then select **Manage USP Services**.

The **Manage CPE Services** window appears.

- b In the **CPE Connection** pane, click **Add**.

The **CPE Connection On Device** window appears.

- c Select the ONU port that you specified internal ME profile. This example selects 1-4-1-1.

- d Select **Manual Select GEM port** (default) or **Auto Select GEM port**.

If you select **Manual Select GEM Port**, then specify the GEM port ID in the **GEM Port Id** field within the range of 257 to 3828. This example specifies 303.

Make sure the GTP is specified on this GEM port.

- e Specify the bridge related parameters:

Select the Bridge type after browsing the bridge templates. This example selects DownlinkSingleTagged.

Specify VLAN ID. This example uses 100.

And other downlink bridge related parameters.

- f Specify the CPE connection related parameters:

Specify the UNI port type, this example selects WLAN (802.11).

Specify RG Mode. Note: RG Mode must be specified for RG provisioning. This example uses BRouted.

And other Wireless UNI port related parameters.

3 View the bridges.

You can view the uplink and downlink bridges in the **Manage Bridge Logicals** window > **Bridge Logical** pane.

4 View the CPE connection, WAN interface, and WLAN interface.

You can view them in the **Manage CPE Services** window> **CPE Connection** pane. WLAN interface details are shown in the LAN Interface pane.

Creating CPE WLAN subscriber profile and associate it with a CPE WLAN common profile or CPE WLAN common advance profile (optional)

By default, the admin-state of the CPE Wireless LAN (WLAN) UNI port is up after creation of CPE connection on that CPE WLAN UNI port. Because of that, the Data and Video traffic can run on this WLAN UNI port without further configuration.

If you want to change the default WLAN physical configurations, you can use the **WLAN Service on Device** window. With this window, the CPE WLAN subscriber profile is created *manually*. The WLAN UNI port ID specified in this window must match the one assigned in the **CPE Connection On Device** window when creating downlink bridge and CPE connection.

After a CPE WLAN subscriber profile is created, if you want to change the settings in that profile, you can use the **Modify WLAN Service** window, which has the same command syntax as the **WLAN Service on Device** window.

To create a CPE WLAN subscriber profile with the **WLAN Service on Device**:

1 Right-click the MXK, and then select **Manage USP Services**.

The **Manage CPE Services** window appears.

2 Select **WLAN Service** pane, and click **Add**.

The **WLAN Subscriber on Device** window appears.

3 In the **WLAN Subscriber on Device** window, specify the desired values for the following fields:

Select Physicals: Pick the ONU that used in the **CPE Connection On Device** window when creating downlink bridge and CPE connection.

Use Template: you can either select template or specify the values manually.

WLAN: WLAN UNI port ID of the physical interfaces.

SSID: Assigns the Service Set Identifier (SSID) to the wireless LAN interface. An SSID is the public name of a wireless local area network. All wireless devices on a wireless local area network must employ the same SSID in order to communicate with each other. It could be 32 characters string or less.

Admin Status: Activates or deactivates the functions performed by the wireless port for this subscriber. Possible values are up, down. Default value is up.

Encryption Key / Passphrase: Sets the wireless encryption key on the wireless network to increase the security. The two standard types of wireless keys support Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) encryption:

If it is a WEP 64-bit encryption key: the value could be 5 ASCII characters or 10 hexadecimal digits

If it is a WEP 128-bit encryption key: the value could be 13 ASCII characters or 26 hexadecimal digits

If it is a WPA Passphrase: the value could be 64 characters.

Device PIN: Sets the device pin only when Wi-Fi Protected Setup (WPS) security method is enabled. Device pin is only used on WLAN UNI port 1.

Radius Key: Sets the Remote Authentication Dial In User Server (RADIUS) authentication key. This field cannot contain a SPACE and is returned as a string of asterisks.

WLAN Profile Index: Associated CPE WLAN common profile with this WLAN UNI port. 1 (Default_CPE_Wlan) indicates the default WLAN common profile is used.

WLAN Advanced Profile Index: Associated CPE WLAN common advance profile with this WLAN UNI port. 1 (Default_CPE_Wlan) indicates the default WLAN common advance profile is used.

- 4 Click **Add**, the new CPE WLAN Subscriber profile appears in the **Manage CPE Services** dialog > **WLAN Service** pane.
- 5 If users want to modify a CPE WLAN Subscriber profile, select it and then click **Modify**.
- 6 If users want to delete a CPE WLAN Subscriber profile, select it and then click **Delete**.

Creating CPE WLAN common profile (optional)

This step is optional. Creation of Data bridge in step [Creating uplink/downlink MXK bridges, and CPE connections in RG-brouted mode on page 278](#) is sufficient for creating a data service. You can use the CPE WLAN common profile if you want to add some common data service attributes.

The CPE WLAN common profile in this section covers the common settings would be used for all WLAN ports. The CPE WLAN common advance

profile in the next section covers the advanced settings that could be used only for WLAN port 1.



Note: CPE WLAN common profile can only be deleted when it is not associated with any CPE WLAN subscriber profiles.

- 1 Right-click the MXK, and then select **Manage USP System** .

The **Manage CPE System** window appears.

- 2 Select **WLAN** pane, and click **Add**.

The **Add WLAN** window appears.

- 3 In the **Add WLAN** window, specify the desired values for the following fields:

Name: Specifies a unique CPE WLAN common profile name. 36 characters string.

Hide Access Point: Enable or disable the suppression of the advertising of the access point's SSID. If enabled, clients will need to configure the SSID to associate. Default is Disable.

Isolate Clients: Isolate clients within the wireless network from communicating directly with each other. Default value is Disable.

Wireless Multi Media Advertise: Wireless Multi Media (WMM) provides a subset of the IEEE 802.11e QoS standard, which adds prioritization to wireless to optimize their performance. When multiple concurrent applications are on the wireless network each application may have different latency and throughput needs. WMM provides for this optimization, however WMM may provide slower.

Possible values are Enabled or Disable. Default value is Disable.

Multicast Forward: Wireless Multicast Forwarding enables the ability to send wireless packets to be intercepted by all nodes in the transmission range of the sender. Possible values are Disable, Enable. Default value is Disable.

Maximum Number of Clients: The maximum number of wireless client devices that may be simultaneously connected to the wireless network.

Possible values are 1-50. Default value is 16.

Net Authentication: Configure the network authentication method.

Possible Values:

open

shared

Dot1x

WPA

Wpapsk

WPA2

WPA2psk

MixedWpa2Wpa

MixedWpa2WpaPsk.

Wi-Fi Protected Access(WPA) Group-Rekey Interval: Specifies WPA Group Rekey Interval.

Possible Values are 0-9999999999. Default Value is 0.

WPA Encrypt: WPA encryption mode.

Possible Values are AES, Tkipaes. Default Value is AES.

Wired Equivalent Protection (WEP) Encrypt: WEP encryption mode.

Possible Values are Enable, Disable. Default Value is Disable.

WEP Encryption Strength: WEP encryption strength.

Possible Values are Bit128, Bit64. Default Value is Bit128.

Radius Server IP: IP address of the Remote Authentication Dial In User Server (RADIUS) used for 802.1x authentication.

Default Value is 0.0.0.0.

Radius Port: UDP port to use for accessing the Remote Authentication Dial In User Server (RADIUS).

Possible Values are 0-9999999999. Default Value is 1812.

WPA2 Pre Authentication: Enable or disable WPA2 pre-authentication.

Possible Values are enable, disable. Default Value is disable.

Network Re-Authentication Interval (Sec): WPA2 network re-authentication time, in seconds.

Possible Values are 0-9999999999. Default Value is 36000.

- 4 Click **Add**, the new CPE WLAN Common profile appears in the **Manage CPE System** dialog > **WLAN** pane.
- 5 If users want to modify a CPE WLAN Common profile, select it and then click **Modify**.
- 6 If users want to delete a CPE WLAN Common profile, select it and then click **Delete**.

Creating CPE WLAN common advance profile (optional)

This step is optional. Creation of Data bridge in step [Creating uplink/downlink MXK bridges, and CPE connections in RG-brouted mode on page 278](#) is sufficient for creating a data service.

The CPE WLAN common profile in the previous section covers the common settings would be used for WLAN ports 1 to 4. The CPE WLAN common

advance profile in this section covers the advanced settings that could be used only for WLAN port 1.



Note: CPE WLAN common advance profile can only be deleted when it is not associated with any CPE WLAN subscriber profiles.

- 1 Right-click the MXK, and then select **Manage USP System**.

The **Manage CPE System** window appears.

- 2 Select **WLAN Advanced** pane, and click **Add**.

The **Add WLAN Advanced** window appears.

- 3 In the **Add WLAN Advanced** window, specify the desired values for the following fields:

Name: Specifies a unique CPE WLAN Common Advanced profile name. 36 characters string.

Channel: Defines which channel to use, or 'auto' for automatic selection of a channel with low interference. 802.11b and 802.11g use channels to limit interference from other devices.

Possible Values are Auto, c1-c13. Default is Auto.

Auto-Channel Timer (Minutes): When configured for auto mode, this timer value specifies how often (in minutes) to re-analyze the spectrum to select a low interference channel. Note: auto channel rescan will only occur when there are no actively connected devices.

Possible Values are 0-2147483647. Default value is 15.

802.11n Multi-input Multi-output Mode: 802.11n MIMO EWC modes of operation. 802.11n improves data rates via MIMO (multiple-input, multiple-output) using spatial streams which each have a channel width of 40 MHz or 20 MHz. Usage of 802.11n in the 2.4 and 5GHz modes should depend on interference with other 802.11 or bluetooth systems on the same frequency. Enhanced Wireless Consortium (EWC) provides extra enhancements (adding the ability to define 20 MHz channels).

Possible values are Auto, Disable, Enable. Default value is Auto.

802.11n Multi-input Multi-output Rate: Supported 802.11n MIMO rates, in Mbps.

Possible values are Auto, Usage54G, Rate6Dot5M, Rate13M, Rate19Dot5M, Rate26M, Rate39M, Rate58Dot5M, Rate65M, Rate78M, Rate104M, Rate117M, Rate130M. Default value is Auto.

802.11n Protection Mode: 802.11n MIMO protection modes.

Possible values are Auto, Disabled. Default value is Auto.

802.11n Client Only: Enable or disable the restriction of access to 802.11n clients only. When enabled, prevent 802.11b/g clients from connecting.

Possible Values are Disable, Enable. Default Value is Disable.

Rate54G: The rate when the radio is operating in 802.11g mode. This parameter only applies when the Multiple Input Multiple Output (MIMO) 802.11n Rate is set to use54g.

Possible Values are Auto, Rate1M, Rate2M, Rate5Dot5M, Rate6M, Rate9M, Rate11M, Rate12M, Rate18M, Rate24M, Rate36M, Rate48M, Rate54M. Default Value is Rate1M.

Multicast Rate: The rate for multicast traffic.

Possible Values are Auto, Rate1M, Rate2M, Rate5Dot5M, Rate6M, Rate9M, Rate11M, Rate12M, Rate18M, Rate24M, Rate36M, Rate48M, Rate54M. Default Value is Auto.

Basic Rate: The rate when the radio is operating in basic 802.11b/g mode.

Possible Values are Default, All, Rate1n2m, StdRates. Default Value is Default.

Request-To-Send (RTS) Threshold: The packet size of a request-to-send (RTS) transmission. A low threshold implies RTS packets are sent more frequently, thus requiring more bandwidth but ensuring packet transmission on a busy network.

Possible Values are 0-2347. Default Value is 2347.

Fragmentation Threshold: The threshold at which packets are fragmented.

Possible Values are 256-2346. Default Value is 2346.

Delivery Traffic Indication Message (DTIM) Interval: The interval at which Delivery Traffic Indication Messages (DTIM) are generated. A DTIM message notifies a wireless client that a packet is waiting for transmission.

Possible Values are 1-255. Default Value is 1.

Beacon Interval: The interval at which Beacons are generated.

Possible Values are 1-65535. Default Value is 100.

Global Max. Clients: The maximum number of wireless client devices that may be simultaneously connected to the radio. This value should include the sum total of all active SSIDs.

Xpress Technology: Enable or disable the XPress(TM) Technology.

Possible Values are Disable, Enable. Default Value is Disable.

Transmit Power: The percentage of total power that should be used for data transmissions.

Possible Values are 0-100. Default Value is 100.

Wireless Multi Media(WMM): Enable or disable Wifi Multimedia. If it is enabled, audio, video and voice application data is prioritized over other network traffic.

Possible Values are Enable, Disable. Default Value is Enable.

WMM No-Ack: Enable or disable the suppression of acknowledgements for frames that do not require a QOS Acknowledgement. This avoids the unnecessary transmission of acknowledgements for highly time-critical data.

Possible Values are Enable, Disable. Default Value is Disable.

WMM Automatic Power Save Delivery(APSD): Enable or disable the Automatic Power Save Delivery (APSD) power management method. This feature is useful for bi-directional applications, such as VoIP phones.

Possible Values are Enable, Disable. Default Value is Enable.

Access Point Mode: Wireless access point modes of operation: access point and WDS or WDS only.

Possible Values are AccessPoint, WirelessBridge. Default Value is AccessPoint.

Bridge Restriction Mode: Wireless Bridge Restriction Modes of operation.

Possible Values are Enable, Disable, EnableScan. Default Value is Disable.

Wifi Protected Setup(WPS): Enable or disable WiFi Protected Setup (WPS) security method. If WPS is enabled, the network authentication method, the data encryption, and network key should also be configured in order to authenticate to this wireless network. It is available for WPA-PSK, WPA2-PSK, Mixed WPA2/WPA-PSK and Open Network Authentication methods.

Possible Values are Enable, Disable, EnableScan. Default Value is Disable.

WPS Add Client Method: A client can be added via three different methods: push button, station pin or access point pin.

Possible Values are PushButton, StaPin, ApPin. Default Value is PushButton.

WPS AP-Mode: If the provider is using an external registrar for security, select "Configured". The PIN for AP mode is specified by the registrar. Provide this PIN to the client. Issue "Config AP" to begin the registration process with the client.

Dual Band Cfg Bands: This feature is for the Dual Radio Wifi zNIDs.

Possible Values are 2.4GHz, Undefined, 5GHz. Default Value is 2.4GHz.

Cfg Bandwidth: Aggregate radio bandwidth setting selection. The value of cfg-bandwidth depends on the the different combinations of zNID models and the band values.

Possible Values: 20MHz, 40MHz, 20MHz in 2G and 40MHz in 5G, 80 MHz.

- 4 Click **Add**, the new CPE WLAN Common Advanced profile appears in the **Manage CPE System** dialog > **WLAN Advanced** pane.
- 5 If users want to modify a CPE WLAN Common Advanced profile, select it and then click **Modify**.
- 6 If users want to delete a CPE WLAN Common Advanced profile, select it and then click **Delete**.

CPE System Level Default Settings

The CPE system level default settings on a CPE include:

- firewall settings
- sync-cookie-protection settings
- cross VLAN routing settings
- static route list profile settings
- TR-069 settings, include Username, Password, ACS URL, and etc.
- Passwords of CPE login accounts: Admin, Support, User.

They are listed in the CPE system level common profile. There is a default CPE system common profile that applied to all CPEs in the system. You can modify the default settings as you desired, or create a new CPE system common profile then apply to a CPE.



Note: CPE system common profile can only be deleted when it is not applied to any CPE.

To create a CPE system common profile, use the **Add System Common** window. To apply the new CPE system common profile to a CPE, use the **CPE System on Device** window.

Configuring CPE system common profile

- 1 Right-click the MXK, and then select **Manage USP System**.
The **Manage CPE System** window appears.
- 2 Select **System Common** pane, and click **Add**.
The **Add System Common** window appears.
- 3 In the **Add System Common** window, specify the desired values for the following fields:

Name: The name of the CPE system common profile.

Firewall: Enable or disable firewall. Enabling firewall can protect the CPE from unwanted intrusion. When firewall is enabled, incoming connections can still be selectively allowed through firewall access and port forwarding settings.

Possible Values are Enable, Disable. Default is Enable.

Sync. Cookie Protection: Protects against malicious attackers attempting to exploit TCP handshaking.

Possible Values are Enable, Disable. Default is Enable.

Cross Vlan Routing: If " enabled" is selected, routing between VLANs is allowed. Route table lookups ignore the VLAN ID of the ingress and egress ports. If there is a match, the packet is routed out the interface specified in the Route table, regardless of which VLAN it is a member of.

If “disabled” is selected, packets will be forwarded to the configured Default Route for the VLAN that they arrived on, unless there is a Route Table match within that same VLAN. Routing of packets across VLANs is prevented, providing traffic isolation.

Possible Values are Enable, Disable. Default is Disable.

Static Route List Name: Address of the static-route-list profile associated with this CPE.

By default, there are non static-route-list profile created.

ACS URL: Contains the web site address of the TR-069 ACS (e.g. http://zhone.com:6050). If the URL includes a domain name, a DNS must be reachable to resolve the domain name.

ACS User Name: User name required to access the TR-069 ACS.

ACS Password: User password required to access the TR-069 ACS.

DNS Host List Index: Address of the dns-host-list profile associated with this CPE. Unit32, quick access.

TR69 Inform: Enable or Disable the generation of Inform messages to the TR-069 ACS.

Possible Values are Enable, Disable. Default Value is Enable.

Inform Interval: Periodic interval (in seconds) at which Inform messages will be generated. This is a TR-069 related parameter.

Unit32, Default is 300.

Admin Password: Password for “admin” account on the CPE. Default is blank, that means it won’t overwrite the existing default value on the CPE. 16-char string.

Support Password: Password for “support” account on the CPE. Default is blank. 16-char string.

User Password: Password for “user” account on the CPE. Default is blank.16-char string.

- 4 Click **Add**, the new CPE Common profile appears in the **Manage CPE System** dialog > **System Common** pane.
- 5 If users want to modify a CPE System Common profile, select it and then click **Modify**.

- 6 If users want to delete a CPE System Common profile, select it and then click **Delete**.

Applying a CPE system common profile to a CPE

- 1 Right-click the MXK, and then select **Manage USP Service**.
The **Manage CPE Services** window appears.
- 2 Select **CPE System** pane, and click **Add**.
The **CPE System on Device** window appears.
- 3 In the **CPE System on Device** window>**Select Port** pane, select the ONU that you want to apply the CPE system common profile to.
- 4 In the **CPE System on Device** window>**CPE System** pane, click the browsing button to open the CPE System Common Profile list.
- 5 In the list select a CPE system common profile, then click **OK**.
- 6 In the **CPE System on Device** window, click **Add**.
The CPE system common profile and associated CPE appear in the **Manage CPE Services** window> **CPE System** pane.
- 7 If users want to apply another CPE System Common profile to the CPE, select the item and then click **Modify**.
- 8 If users want to remove a connection between CPE and CPE System Common profile, select it and then click **Delete**.

Static Configuration on the WAN side interfaces (without DHCP)

This section describes how to assign a static IP address to the WAN side interfaces on a zNID.

Assigning a Static IP address to the WAN side interface on the zNID

This example is the continuance of the triple-play services that created in the section [Creation of Voice service in RG, page 276](#).

To assign a static IP address to the WAN side interface, use the following procedure:

- 1 Create services on one ONT with the **CPE Connection On Device** window (using system defaults).
Refer to [Creation of Voice service in RG, page 276](#).
- 2 View the voice bridges in the **Manage Bridge Logicals** window.
- 3 View the CPE connections for voice service in the **Manage CPE Services** window > **CPE Connection** pane.

- 4 Verify the default settings of the above voice connections on the WAN interface.

In the **Manage CPE Services** window > **CPE Connection** pane. Select the CPE connection, the **WAN Interface** pane displays its default settings.

- 5 Create a new IP Server profile with system wide static IP configuration in the **Add CPE IP Server** window.

For how to access the **Add CPE IP Server** window and parameter description, refer to [Creating a CPE IP server profile \(i.e. CPE IP common profile\)](#) on page 255.

- a This example specified the following parameters in the **Add CPE IP Server** window:

Profile Name: static-ip-config-1

Host IP Option: Static

Net Mask: 255.255.255.0

Gateway: 10.1.1.254

Primary DNS: 172.16.1.5

Secondary DNS: 172.16.5.11

- b Click **Add**.

A new IP server profile is created with an index.

- 6 Apply those custom ip-config setting on the WAN interface:

- a In the **Manage CPE Services** window > **CPE Connection** pane. Select the CPE connection, its WAN interface info will appear in the **WAN Interface** pane.

- b Select the WAN interface, and click **Modify**.

The **Modify Interface VLAN** window appears.

- c In the **Modify Interface VLAN** window, specify the static custom ip-config setting.

This example specified the following parameters:

IP Common Profile Index: select “static-ip-config-1” from the browsing menu.

IP Address: 10.1.1.5

- d Click **Modify**.

The new settings appear in the WAN Interface pane.

Static configuration on the LAN side interfaces with a new DHCP server

This example is the continuance of the triple-play services that created in the section [OMCI GPON zNID with RG features installation for Triple services, page 272](#).

This section configures the following settings on the Brouted LAN interfaces those has same VLAN:

- Assigns a static IP address as the local IP address of the LAN interfaces
- Changes the IP address range for the DHCP server
- Changes the firewall access settings on the LAN interfaces

Assigning a Static IP address to the LAN side interface on the ONU

- 1 Create services on one ONT with the **CPE Connection On Device** window (using system defaults). This example creates data service on Eth 1 and WLAN 1 with brouted connections, and both ports are in VLAN 100.

Refer to [OMCI GPON zNID with RG features installation for Triple services, page 272](#).

- 2 Create a new IP Server profile for LAN side interface in the **Add CPE IP Server** window.

Refer to [Creating a CPE IP server profile \(i.e. CPE IP common profile\)](#).

- a This example specified the following parameters in the **Add CPE IP Server** window > **Configuration** Pane:

Profile Name: hsi-lan

Host IP Option: Static

Net Mask: 255.255.255.0

Make sure all the options in the **Firewall Access Bits** Pane are enabled.

- b Click **Add**.

A new IP server profile is created with an index.

- 3 Create a DHCP server profile in the **Add DHCP Server** window.

Refer to [Configuration of DHCP server, page 297](#).

This example specifies the following parameters in the **Add DHCP Server** window:

Name: hsi-dhcp

Start Address: 192.168.10.50

End Address: 192.168.10.200

- 4 Assign a new IP address, IP common profile, and a DHCP server profile to the LAN interface in the **Modify Interface VLAN** window:
 - a In the **Manage CPE Services** window > **CPE Connection** pane. Select the CPE connection, its LAN interface info will appear in the **LAN Interface** pane.
 - b Select the LAN interface, and click **Modify**.
The **Modify Interface VLAN** window appears.
 - c This example specified the following parameters:
IP Address: 192.168.10.54
IP Common Profile Index: Select hsi-lan
DHCP Server Profile Index: Select hsi-dhcp
 - d Click **Modify**.

Configuration of Static Routes

To add static routes to the zNID, user need to create a static route list, and then associate this static route with a CPE system common profile, at last apply this system common profile to the zNID.

Adding a Static Route to the ONU

Use the following procedure to add a static route to the ONU:

- 1 Create services on one ONU (using system defaults) with the **CPE Connection On Device** window:
Refer to [OMCI GPON zNID with RG features installation for Triple services, page 272](#)
- 2 Add a static route.
 - a Right-click the MXK, and then select **Manage USP System**.
The **Manage CPE System** window appears.
 - b In the **Manage CPE System** window, select **Static Route List** pane.
 - c In the **Static Route List** pane, click **Add**.
The **Add Static Route List** window appears.
 - d In the **Add Static Route List** window, you can specify the following parameters:
Static Route List Index: The list index of the static route
Name: The list name of the static route
 - e Click **Add**.
The Static Route list appears in the **Manage CPE System** window > **Static Route List** pane.

f In the **Manage CPE System** window, select **Static Route** pane.

g In the **Static Route** pane, click **Add**.

The **Add Static Route** window appears.

h In the **Add Static Route** window, you can specify the following parameters:

Static Route List Name: Select a static route list

Static Route List Entry: Specify the static route entry index in this static route list

Destination IP: The IP address of the destination network or host. Host portion of the destination address must be zero. Default value is 0.0.0.0.

Net Mask: Destination subnet mask. An value of 0.0.0.0 indicates no destination subnet mask is specified. Default value is 255.255.255.0.

Gateway: Next hop IP address. The next hop must be reachable. Default is 0.0.0.0.

Metric: Number of hops to reach destination. A value of 0 indicates this metric is not used. Possible Values are 0 - 2147483647. Default Value is 1.

i Click **Add**.

The Static Route entry is added to the Static Route List, and appears in the **Manage CPE System** window > **Static Route** pane.

3 Associate this static route with the CPE system common profile. You can either modify an existing CPE system common profile or create a new CPE system common profile. This example creates a new one:

a In the **Manage CPE System** window, select **System Common** pane.

b In the **System Common** pane, click **Add**.

The **Add System Common** window appears.

c In the **Add System Common** window, you can specify the following parameters:

System Common Index: Specify an unique index for System Common profile

Name: Specify the name of the System Common profile

Static Route List Name: Select static route list by its name.

Cross Vlan Routing: The cross VLAN routing is disabled by default. This example enables the crossing VLAN routing on the static route.

If "enabled" is selected for cross VLAN routing, routing between VLANs is allowed. Route table lookups ignore the VLAN ID of the ingress and egress ports. If there is a match, the packet is routed out the interface specified in the Route table, regardless of which VLAN it is a member of.

If "disabled" is selected for cross VLAN routing, packets will be forwarded to the configured Default Route for the VLAN that they arrived on, unless there is a Route Table match within that same VLAN. Routing of packets across VLANs is prevented, providing traffic isolation.

d Click Add.

The System Common profile appears in the **Manage CPE System** window > **System Common** pane

4 Apply static route to a ONU.

If this CPE does not have system common profile assigned to it, you can use the **CPE System on Device** window. If there is a system common profile already exists, use the **Modify CPE System** window.

Refer to [Applying a CPE system common profile to a CPE on page 288](#).

Configuration of Firewall

User can enable or disable firewall on the CPE. Enabling firewall can protect the CPE from unwanted instruction. When firewall is enabled, incoming connections can still be selectively allowed through firewall access and port forwarding settings. The firewall is enabled by default.

Enabling or disabling firewall

Use the CPE system common profile to enable or disable firewall settings.

1 Verify the firewall setting in the CPE.

In the **Manage CPE Services** window> **CPE System** pane, find the ONU and its associated CPE System Common Profile index.

In the **Manage CPE System** window > **System Common** pane, find the CPE System Common Profile and its Firewall settings.

2 By default, the Firewall is enabled, you can modify firewall setting in the **Modify System Common window.**

Configuring firewall access

Firewall access control manages the protocols allowed on the CPE WAN or LAN interfaces. It requires firewall feature to be enabled.

The protocols are listed below:

- HTTP: Web Browser Traffic.
- PING: ICMP Echoes used to test for connectivity.
- SNMP: Simple Network Management Protocol.
- SNMPTRAP: Alarms for Simple Network Management Protocol.
- SSH: Secure Shell.

- TELNET: Remote Terminal support.

By default, those protocol are all enabled in the CPE IP Server profile.



Note: Modifying a CPE IP server profile will trigger a partial reconfiguration on each of the CPEs that depend on this profile and may cause service interruptions on these CPEs.

To modify the default firewall settings, use the following procedure:

- 1 Make sure the CPE has the firewall setting enabled.
Refer to Section [Enabling or disabling firewall](#), page 293.
- 2 Change the firewall access settings on the CPE WAN interface:
 - a View the current firewall access settings on the CPE WAN interface.
In the **Manage CPE Services** window > **CPE Connection** pane> **WAN Interface** pane, find the IP Server profile (i.e IP Common profile) Index that associated with the CPE WAN interface.
In the **Manage CPE System** window > **IP Server** pane, find and select this IP Server profile, and then click **View**. The **View CPE IP Server** window appears.
In the **View CPE IP Server** window > **Firewall Access Bits** pane, view the firewall access settings.
 - b If the existing firewall access settings are not desired, you can create a new CPE IP server profile. Note that the IP Server profile is shared across other profiles. If you modify an IP Server profile, the other profiles it associated to will get new settings too.
In the **Manage CPE System** window > **IP Server** pane, click **Add**.
In the **Add CPE IP Server** window > **Firewall Access Bits** pane, select the desired firewall access settings, and then click **Add**.
 - c Apply the new firewall access settings to the WAN interface.
In the **Manage CPE Services** window > **CPE Connection** pane> **WAN Interface** pane, select the WAN interface, and click **Modify**. The **Modify Interface VLAN** window appears.
In the **Modify Interface VLAN** window, click the **IP Common Profile Index** browsing button, pick the new IP server profile (i.e. IP common profile). And then click **Modify**.
- 3 Change the firewall access settings on the CPE LAN interface (the procedure is similar to the CPE WAN interface):
 - a View the current firewall access settings on the CPE LAN interface.
In the **Manage CPE Services** window > **CPE Connection** pane> **LAN Interface** pane, select the LAN interface, and then click **View**.

In the **View Interface VLAN** window, find the IP Server profile (i.e IP Common profile) Index that associated with the CPE LAN interface.

In the **Manage CPE System** window > **IP Server** pane, find and select this IP Server profile, and then click **View**. The **View CPE IP Server** window appears.

In the **View CPE IP Server** window > **Firewall Access Bits** pane, view the firewall access settings.

- b** Create a new CPE IP server profile.

In the **Manage CPE System** window > **IP Server** pane, click **Add**.

In the **Add CPE IP Server** window > **Firewall Access Bits** pane, select the desired firewall access settings, and then click **Add**.

- c** Apply the new firewall access settings to the LAN interface.

In the **Manage CPE Services** window > **CPE Connection** pane> **LAN Interface** pane, select the LAN interface, and click **Modify**. The **Modify Interface VLAN** window appears.

In the **Modify Interface VLAN** window, click the **IP Common Profile Index** browsing button, pick the new IP server profile (i.e. IP common profile). And then click **Modify**.

Configuring port forwarding

The CPE port forwarding list reflects the existing port forwarding rules. The port forwarding list only can be created on a WAN interface that has NAT or NAT enabled. By default, there is no port-forwarding list associated to the WAN interface.

Port forwarding list requires firewall feature to be enabled.

You can use the **Add Cpe Port Fwd List** window to create CPE port forwarding list. Use the **Add Port Forward** window to create CPE port forward entries into the list.

To configure port forwarding on CPE, use the following procedure:

- 1** Make sure the CPE has the firewall setting enabled. By default, firewall is enabled.

Refer to Section [Enabling or disabling firewall, page 293](#).

- 2** Create a port forwarding list:

- a** In the **Manage CPE System** window > **Port Forward List** pane, click **Add**.

The **Add Cpe Port Fwd List** window appears.

- b** In the **Add Cpe Port Fwd List** window, specify an unique Port Forward List Index, and specify the name of the Port Forward List.
- c** Click **Add**.

The new list appears in the **Manage CPE System** window > **Port Forward List** pane.

3 Add port forwarding entries into the list:

- a** In the **Manage CPE System** window > **Port Forward** pane, click **Add**.

The **Add Port Forward** window appears.

- b** In the **Add Port Forward** window, you can specify the following fields:

Port Forward List Name: The list name of the port forwarding rules. Click the browsing button to select the desired Port Forward List.

Port Forward List Entry: The name of the port forwarding rule.

Type: Type of the port forwarding. When DMZ is chosen it is the only rule allowed on that interface. A DMZ rule is effectively the same as a rule with all ports included. Range rules are more secure than setting a DMZ rule, because Range rules allow ports or groups of ports to be opened up. Remap indicates that any traffic on those ports will be sent to the private IP address at the private port. Range indicates that any traffic on those ports will be sent to the private IP address.

Possible Values are DMZ, Port Re-Map, and Port Range. Default Value is DMS.

Port Start: Lowest value port number for the range.

Possible Values are 0-65535. Default Value is 0.

Port End: Highest value port number for the range. This can be equal to port-start if there is only one port. Possible Values are 0-65535, end-port must be larger or equal to start-port. Default Value is 0.

Protocol: Indicate which protocols to monitor for the port numbers.

Possible Values are TCP, UDP, TCP-UDP, ICMP, ICMP V4, None. Default Value is None.

Private Port: The port number with which to send the traffic.

Possible Values are 0-65535. Default Value is 0.

Private IP: The port IP Address with which to send the traffic.

Default Value is 0.0.0.0.

- c** Click **Add**.

The new entry appears in the **Manage CPE System** window > **Port Forward** pane.

4 Associate the WAN interface with the port forwarding list.

- a** In the **Manage CPE Services** window > **CPE Connection** pane> **WAN Interface** pane, select the WAN interface, and click **Modify**.

The **Modify Interface VLAN** window appears.

- b** In the **Modify Interface VLAN** window, click the **Port Forward Profile Index** browsing button, pick the desired Port Forwarding List.
- c** Click **Modify**.

Configuration of DHCP server

DHCP server configuration is only for rg-brouted or rg-bpppoe mode connection. The rg-bridged mode connection does not need it.

After creating the connection between the MXK GEM port and CPE UNI port with the **CPE Connection On Device** window, a default DHCP server with index 100001 is automatically created for the LAN side devices.

The default DHCP server has the following settings:

Profile Name= default-dhcp-server10001

Start Address= 192.168.1.10

Stop Address= 192.168.1.100

Lease Time= 86400 seconds

If you don't want to use the default DHCP server, you can create a new DHCP server for the LAN-side devices with the following procedure.

Creating a new DHCP server for the LAN interface

- 1** Create the LAN-side interfaces in RG for the RG-brouted or RG-bpppoe connection.

Refer to [Creating uplink/downlink MXK bridges, and CPE connections in RG-brouted mode for data service, page 273](#).

- 2** Create a DHCP server profile for the LAN-side devices:

- a** In the **Manage CPE System** window > **DHCP Server** pane, click **Add**.

The **Add DHCP Server** window appears.

- b** In the **Add DHCP Server** window, specify the following fields:

DHCP Server Index: Specify an unique index for DHCP server

Name: Specify an unique name for DHCP server

Start Address: Start IP address in this range.

End Address: End IP address in this range.

Lease Time: The amount of time the address is leased for. The unit is second.

- c** Click **Add**.

The new DHCP server appears in the **Manage CPE System** window > **DHCP Server** pane.

- 3 Use the new DHCP server profile in the brouted or the bpppoe connection:
 - a In the **Manage CPE Services** window > **CPE Connection** pane. Select the CPE connection, its LAN interface info will appear in the **LAN Interface** pane.
 - b Select the LAN interface, and click **Modify**.
The **Modify Interface VLAN** window appears.
 - c In the **Modify Interface VLAN** window, select the new DHCP server profile index.
 - d Click **Modify**.

Configuration of TR-069

TR-069(Technical Report 069) is a management protocol which allows an Auto-Configuration Server (ACS) to auto-configure, provision, collection, and provide diagnostics to the zNID.

After a TR-069 connection is created on ONU GEM port in the **CPE Connection On Device** window, users can configure TR-069 client settings and then apply to the ONU. (Note that when creating TR-069 connection, the **Type** must be specified to TR69.)

TR-069 client settings are contained in the CPE system common profile.

Configuring TR-069 client settings on the ONU

The following procedure shows how to configure the TR-069 client:

- 1 Create a CPE system common profile in the **Add System Common** window for TR-069 clients, and set the ACS URL, ACS User name, and ACS Password to match the ones pre-configured on the TR-069 server (i.e.ACS).

Note that in the CPE system common profile, ACS URL, ACS User name, and ACS Password parameters are required for TR-069 configuration, and the tr69-inform and inform-interval parameters are optional.

Refer to [Configuring CPE system common profile, page 286](#).

- 2 Apply the new TR-069 client settings to the ONU, use the **CPE System on Device** window.

Refer to [Applying a CPE system common profile to a CPE, page 288](#).

Configuration of PPPoE username and password

Specifying a PPPoE username and password

The Point-to-Point Protocol over Ethernet (PPPoE) encapsulates PPP frames inside Ethernet frames to create a PPPoE tunnel between hosts connected to

the zNID and other devices out in the cloud. While Ethernet is packet-based (so no direct connection is opened), PPP is a direct connection where one device directly connects to another using the protocol. PPPoE is a virtual connection (usually called tunnel) between two devices.

By specifying Bridged PPPoE mode in the **CPE Connection On Device** window, you can add a PPPoE on an Uni-port by VLAN. PPPoE/Bridged VLANs are similar to Brouted VLANs, but the WAN side interface is a PPPoE client that establishes a PPPoE tunnel to an upstream BRAS. On the LAN side of a PPPoE/Bridged VLAN, all ports will be members of the same IP subnet.

To configure the PPPoE session, use the **Modify PPPOE** window.

- 1 Right-click the MXK, and then select **Manage USP Services**.

The **Manage CPE Services** window appears.

- 2 In the **CPE Connection** pane, select a Bridged PPPOE CPE connection.

The **PPPOE** pane shows the default settings.

- 3 In the **PPPOE** pane, select the entry, and click **Modify**.

The **Modify PPPoE** window appears.

- 4 In the **Modify PPPoE** window, you can specify the following PPPoE related parameters:

User Name: The login user name to be used for PPPoE authentication. It must be an unique 25-char string. (required)

Password: The login password to be used for PPPoE authentication. It is an encrypted 25-char string. (required)

Authentication: Indicates the PPP authentication protocol to be used for PPPoE authentication. Possible Values are Auto, Chap, MsChap, Pap. Default Value is Auto.(optional, it has default value)

Retry Interval (Sec): Specifies the time in seconds before retrying connection. (optional, it has default value)

- 5 Click **Modify**.

CPE Management Templates

ZMS supports CPE system templates and CPE service templates for Unified Service Provisioning profiles.

CPE system templates provide following templates for the profiles that could be configured in the **Manage CPE System** window:

- CPE IP Common Templates
- CPE PWE Templates
- CPE SIP Dial Plan Templates
- CPE Traffic Management Templates

- CPE Video Templates
- CPE Video Access Control Templates
- CPE VOIP Features Templates
- CPE VOIP Media Templates
- CPE VOIP Server Templates
- CPE System Common Templates
- CPE DHCP Server Templates
- CPE WLAN Templates
- CPE Port Forward Templates
- CPE Static Route Templates

CPE service templates provide following templates for the profiles that could be configured in the **Manage CPE Service** window:

- CPE VOIP Subscriber Templates
- CPE Ethernet Subscriber Templates
- CPE PWE Subscriber Templates
- CPE RF Subscriber Templates
- CPE IP Templates
- CPE Interface VLAN Templates
- CPE PPPOE Templates
- CPE WLAN Subscriber Templates

Each above CPE management template has a system default template. You can create user-defined templates too.

If there is more than one CPE management template created for a profile type, you can select a desired template when you creating this type of the profile.

Adding a user-defined CPE management template

To create a CPE management template in the ZMS server, perform the following task:

- 1** Select **Tools > Configure Templates**.

The **Template Configuration** dialog box appears.

- 2** Expand the **CPE Management Templates** level.

CPE System Templates and **CPE Service Templates** levels appear.

- 3** Expand the **CPE System Templates** level or the **CPE Service Templates** level.

- 4** Right click a template and select **Add**.

The **Add CPE xxx** dialog box appears.

- 5 In the **Add CPE xxx** dialog box, enter the template name and description. Select the desired values.
- 6 When finished, click **Add**.

Selecting a CPE system template

- 1 Select **Tools > Configure Templates**.
The **Template Configuration** dialog box appears.
- 2 Expand the **CPE Management Templates** level.
CPE System Templates and **CPE Service Templates** levels appear.
- 3 Expand the **CPE System Templates** level or the **CPE Service Templates** level.
- 4 Right click a template and select **Add**.
The **Add CPE xxx** dialog box appears.
- 5 In the **Add CPE xxx** dialog box, enter the template name and description. Select the desired values.
- 6 When finished, click **Add**.

Post Configuration in USP



Note: Post configuration requires a post configuration script from Zhone. Please contact Zhone GSS to obtain a post configuration script suited to your needs.

After the CPE has been configured with Unified Service Provision, if users want to configure some extra features on this CPE, and those features do not have profile support, a post configuration script can be used to post-configure the CPE. The post configuration scripts are created by Zhone as needed without upgrading the MXK software.

Appending post script file to the ME Profile

To append supplemental post configuration script to the ME profile, use the **Append Profile** window.

- 1 Add the post configuration script file into the ZMS server file */tftpboot* directory.
- 2 Right-click a device in the tree view, select **Manage OMCI ME Profile**. The **Manage OMCI ME Profile** dialog box appears.
- 3 Select an internal “Zhone-” ME profile in the list, and click **Append** button.

The **Append Profile** dialog box appears.

- 4 In the **Append Profile** dialog box, specify the post configuration script name in the **Profile File Name** field. And then click **Apply**, and then click **Close**.



Note: If the post configuration script file contains variables, follow the procedure to add Generic and Specific profiles as needed.

Removing post configuration script file from the ME profile

To remove post configuration script from the internal “Zhone-” ME profile, use the **Revert Profile** window.

- 1 Right-click a device in the tree view, select **Manage OMCI ME Profile**. The **Manage OMCI ME Profile** dialog box appears.
- 2 Select an internal “Zhone-” ME profile from the list, and click **Revert** button.
The **Revert Profile** dialog box appears.
- 3 In the **Revert Profile** dialog box, click **Apply**, and then click **Close**.

CPE LLDP-MED configurations

Link Layer Discovery Protocol and its extension Media endpoint Discovery. The LLDP packets will include information about the zNID device, including Manufacturer, Model Number, Asset ID, Serial Number, MAC Address, Port Description, System Name, System Location, System Description, HW Rev, FW Rev, Linux SW Rev, PoE Power Capabilities, Ethernet Link Speed and Duplex mode. In addition, when an attached device responds with an LLDP packet that indicates support for the Media Endpoint Discovery (MED) extensions to LLDP, then the zNID will also send LLDP-MED packets.

To configure CPE LLDP-MED, use the LLDP Med Policy List and the LLDP Med Policy in the **Manage CPE System** window.

Use the **Add LLDP Med Policy List** window to configure the following information for a LLDP Med Policy List Profile.

1. LLDP Med Policy List Profile Name: The name of the profile. 36-char string.
2. Device Discovery Notify: Disable or Enable
3. Notification Interval:

Use the **Add LLDP Med Policy** window to configure the following information:

1. LLDP Med Policy List Name
2. LLDP Med Policy List Entry
3. Admin State: Enable or Disable the network policy

4. Type: The media type that defines the primary function of the application for the policy advertised by an endpoint. Valid Types are Voice, Voice Signal, Guest Voice, Guest Voice Signal, Soft Phone, Video Conf, Video Streaming, Video Signal
5. VLAN Id: The VLAN ID of the application for the policy advertised by an endpoint. Range is 0-4095, default is 0.
6. COS: The Class Of Service of the application for the policy advertised by an endpoint. Range is 0-7, default is 0.
7. DSCP: The Differentiated Service Code Point of the application for the policy advertised by an endpoint. Range is 0-63.

GPON ONT Inventory Tool

After GPON ONT Inventory Tool script is installed, it enables a ZMS Tool menu option that launches the GPON ONT Inventory Tool web page. In the GPON ONT Inventory Tool web page, user can select one or multiple MXKs and generate an inventory report of all the GPON CPEs connected with the selected MXK(s). The inventory report can be displayed in Excel or imported into an OSS/BSS application as a CSV file. It consists of CPE system information, service configuration information, and ONT status information for each ONT in the report.

Follow the installation instructions in the **ZMS Installation Guide** to install and launch the GPON inventory tool.

The following section describes how to use the GPON ONT Inventory Tool.

Generating GPON reports with the GPON ONT Inventory Tool

- 1 When launching the GPON Inventory Tool from the ZMS NetHorizon client, the device selection screen will be displayed. This screen will display the list of MXKs that have GPON cards installed.
- 2 Select single device or use shift key or Ctrl key to select multiple devices. And then click blue **Run** button to generate the GPON inventory report for all the CPEs connected with the device(s).
If you click the green **Reset** button, the selected devices will be released.
- 3 A **File Download** window appears. You can decide to save the csv file locally in your PC or open it with Excel.



Note: Note that if you are using Excel 2003 or prior to open the inventory report, the maximum rows can be displayed in the file is 65,000.

Voice configuration

NetHorizon enables users to add, modify, and view voice connections for the desired voice connection type. Voice connections can be added manually or through a configuration wizard using pre-configured voice connection templates.

The following types of voice connections between subscriber and remote end-points are supported:



Note: The voice gateway card requires NetHorizon software version 1.11 or higher on the uplink cards.



Note: The voice connections over ATM are removed for device version 1.14.2 or greater. All voice connection tabs that have AAL2 end point as one of the end points will not appear in ZMS client if the device is running with 1.14.2 or greater.

Subscriber end-points	Gateway end-points	MALC Uplinks
POTS	AAL2	All
	DS1	TDM, OC-12c/STM4, Gigabit Ethernet
	GR303	TDM, OC-12c/STM4, Gigabit Ethernet
	VOIP	All
	V5.2	TDM, OC-12c/STM4, Gigabit Ethernet
ISDN	AAL2	All
	V5.2	TDM, OC-12c/STM4, Gigabit Ethernet
VOIP	GR303	All TDM IP (voice gateway card required)
	V5.2	All TDM IP (voice gateway card required)
AAL2	GR303	All TDM ATM (voice gateway card required)
	V5.2	All TDM ATM (voice gateway card required)
ALL2 ELCP	V5.2	All TDM ATM (voice gateway card required)



Note: These procedures assumes you have configured the required TDM/ATM Uplink physical interfaces as explained in [Card configuration on page 130](#), and the required settings for POTS, AAL2, ISDN, VOIP, V5.2 and GR303 interfaces.

Topics:

[Voice configuration templates](#)

[Manage voice connections](#)

[Manage voice gateway AAL2 subscribers](#)

[Manage VOIP connections](#)

[Configuring voice DSP settings](#)

[Creating an ATM AAL2 VCL](#)

[Configuring ESA voice connections](#)

Voice configuration templates

Topics:

[Creating AAL2 to V5.2 \(PSTN\) voice configuration templates](#)

[Creating AAL2 to V5.2 \(ISDN\) voice configuration templates](#)

[Creating AAL2 to GR-303 voice configuration templates](#)

[Creating AAL2 ELCP to V5.2 \(ISDN\) configuration templates](#)

[Creating AAL2 ELCP to V5.2 \(POTS\) configuration templates](#)

[Creating ISDN to AAL2 configuration templates](#)

[Creating ISDN to V5.2 configuration templates](#)

[Creating POTS to GR-303 configuration templates](#)

[Creating POTs to V5.2 configuration templates](#)

[Creating POTs to AAL2 configuration templates](#)

[Creating POTs to DS1 configuration templates](#)

[Creating EBS to GR-303 configuration templates](#)

Creating AAL2 to V5.2 (PSTN) voice configuration templates

To create a template for AAL2 to V5.2 PSTN voice connections:

- 1 Select **Tools > Configure Templates**.

The **Template Configuration** dialog box appears.

- 2 Expand **Voice Connections Templates**.

- 3 Right click **AAL2 to V52 (PSTN) Voice Connections Templates** and select **Add**.

The **Add Composite Voice Configuration** dialog box appears.

- 4 Enter a name and a description for this template.

The name appears in the selection dialog boxes.

- 5 Configure the voice connection:

From this dialog box you can configure:

- Subscriber information. See [Adding voice gateway AAL2 subscribers on page 347](#) or [Adding POTS to AAL2 voice connections using the wizard \(MALC\) on page 318](#).
- AAL2 VCLs. See [Creating an ATM AAL2 VCL on page 349](#)[Creating an ATM AAL2 VCL](#)
- ATM CIDs. . The template provides appropriate CID values for a PSTN connection. Refer to the online help for details on the CID settings.
- V5.2 user port information:

Admin Status: Set to **In Service**

Port Type: Indicates this is a PSTN interface

Lease Type: Specify the lease type

Block Type: Specify the port blocking

For more information on these settings, see the online help.

- 6 After finishing the configuration, click **Add**, then **Close**.

After adding the template, it will appear in the **Template Configuration** dialog box.

Related topics:

o

[Creating POTs to AAL2 configuration templates on page 314](#)

[Creating POTS to GR-303 configuration templates on page 312](#)

[Creating POTs to V5.2 configuration templates on page 313](#)

[Finding ATM VCLs and cross connects on page 461](#)

Creating AAL2 to V5.2 (ISDN) voice configuration templates

To create a template for AAL2 to V5.2 ISDN voice connections:

- 1 Select **Tools > Configure Templates**.

The **Template Configuration** dialog box appears.

- 2 Expand **Voice Connections Templates**.

- 3 Right click **AAL2 to V52 (ISDN) Voice Connections Templates** and select **Add**.

The **Add AAL2 to V52 (ISDN) Voice Connection Template** dialog box appears.

- 4 Enter a name and a description for this template.

The name appears in the selection dialog boxes.

- 5 Configure the voice connection:

From this dialog box you can configure:

- Subscriber information. See [Adding voice gateway AAL2 subscribers on page 347](#) or [Adding POTS to AAL2 voice connections using the wizard \(MALC\) on page 318](#).
- AAL2 VCLs. See [Creating an ATM AAL2 VCL on page 349](#).
- ATM CIDs. The template provides appropriate CID values for an ISDN connection. Refer to the online help for details on the CID settings.
- V5.2 user port information:

Admin Status: Set to **In Service**

Port Type: Indicates this is an ISDN interface

Lease Type: Specify the lease type

Block Type: Specify the port blocking

For more information on these settings, see the online help.

- 6 After finishing the configuration, click **Add**, then **Close**.

After adding the template, it will appear in the **Template Configuration** dialog box.

Related topics:

[Creating POTs to AAL2 configuration templates on page 314](#)

[Creating POTS to GR-303 configuration templates on page 312](#)

[Creating POTs to V5.2 configuration templates on page 313](#)

[Creating AAL2 to V5.2 \(PSTN\) voice configuration templates on page 306](#)

[Finding ATM VCLs and cross connects on page 461](#)

Creating AAL2 to GR-303 voice configuration templates

To create a template for GR-303 voice connections:

- 1 Select **Tools > Configure Templates**.

The **Template Configuration** dialog box appears.

- 2 Expand **Voice Connections Templates**.

- 3 Right click **Aal2 To Gr303 Voice Connections Templates** and select **Add**.

The **Add AAL2 to GR303 Voice Configuration** dialog box appears.

- 4 Enter a name and a description for this template.

The name appears in the selection dialog boxes.

- 5 Configure the voice connection:

From this dialog box you can configure:

- Subscriber information.
- AAL2 VCLs.
- ATM CIDs.
- GR-303 CRV endpoints.

See the online help for details on these settings.

- 6 After finishing the configuration, click **Add**, then **Close**.

After adding the template, it will appear in the **Template Configuration** dialog box.

Related topics:

[Creating AAL2 to V5.2 \(PSTN\) voice configuration templates on page 306](#)

[Creating AAL2 to V5.2 \(ISDN\) voice configuration templates on page 307](#)

[Creating POTs to AAL2 configuration templates on page 314](#)
[Creating POTs to AAL2 configuration templates](#)

[Creating POTS to GR-303 configuration templates on page 312](#)

[Creating AAL2 to GR-303 voice configuration templates on page 308](#)

Creating AAL2 ELCP to V5.2 (ISDN) configuration templates

To create a template for AAL2 ELCP to V5.2 (ISDN) voice connections:

- 1 Select **Tools > Configure Templates**.

The **Template Configuration** dialog box appears.

- 2 Expand **Voice Connections Templates**.

- 3 Right click **ELCP to V52 ISDN Voice Connections Templates** and select **Add**.

The **Add ELCP to V52 ISDN Voice Connection Template** dialog box appears.

- 4 Enter a name and a description for this template.

The name appears in the selection dialog boxes.

- 5 Configure the voice connection:

From this dialog box you can configure subscriber information.

For details on the subscriber settings, see the online help.

- 6 After finishing the configuration, click **Add**, then **Close**.

After adding the template, it will appear in the **Template Configuration** dialog box.

Related topics:

[Creating AAL2 to V5.2 \(ISDN\) voice configuration templates on page 307](#)

[Creating POTS to GR-303 configuration templates on page 312](#)

[Creating POTs to V5.2 configuration templates on page 313](#)

[Creating POTS to GR-303 configuration templates on page 312](#)

[Creating POTs to V5.2 configuration templates on page 313](#)

[Creating AAL2 ELCP to V5.2 \(POTS\) configuration templates on page 310](#)

Creating AAL2 ELCP to V5.2 (POTS) configuration templates

To create a template for AAL2 ELCP to V5.2 (POTS) voice connections:

- 1 Select **Tools > Configure Templates**.

The **Template Configuration** dialog box appears, listing all the templates.

- 2 Expand **Voice Connections Templates**.

- 3 Right click **ELCP to V52 Pots Voice Connections Templates** and select **Add**.

The **ELCP to V52 POTS Voice Connection Template** dialog box appears.

- 4 Enter a name and a description for this template.

The name appears in the selection dialog boxes.

- 5 Configure the voice connection:

From this dialog box you can configure subscriber information.

For details on the subscriber settings, see the online help.

- 6 After finishing the configuration, click **Add**, then **Close**.

After adding the template, it will appear in the **Template Configuration** dialog box.

Related topics:

[Creating AAL2 to V5.2 \(ISDN\) voice configuration templates on page 307](#)

[Creating POTS to GR-303 configuration templates on page 312](#)

[Creating POTS to GR-303 configuration templates on page 312](#)

[Creating POTS to GR-303 configuration templates on page 312](#)

[Creating POTs to V5.2 configuration templates on page 313](#)

[Creating AAL2 ELCP to V5.2 \(ISDN\) configuration templates on page 309](#)

Creating ISDN to AAL2 configuration templates

To create a template for ISDN to AAL2 voice connections:

- 1 Select **Tools > Configure Templates**.

The **Template Configuration** dialog box appears.

- 2 Expand **Voice Connections Templates**.

- 3 Right click **ISDN to AAL2 Voice Connections Templates** and select **Add**.

The **Add ISDN to AAL2 Voice Connection Template** dialog box appears.

- 4 Enter a name and a description for this template.
The name appears in the selection dialog boxes.
- 5 Configure the voice connection:
From this dialog box you can configure subscriber information.
For details on the subscriber settings, refer to the online help.
- 6 After finishing the configuration, click **Add**, then **Close**.
After adding the template, it will appear in the **Template Configuration** dialog box.

Related topics:

[Creating AAL2 to V5.2 \(ISDN\) voice configuration templates on page 307](#)

[Creating POTs to V5.2 configuration templates on page 313](#)

[Creating POTS to GR-303 configuration templates on page 312](#)

[Creating POTs to V5.2 configuration templates on page 313](#)

[Creating AAL2 ELCP to V5.2 \(POTS\) configuration templates on page 310](#)

[Creating AAL2 ELCP to V5.2 \(ISDN\) configuration templates on page 309](#)

Creating ISDN to V5.2 configuration templates

To create a template for ISDN to V5.2 voice connections:

- 1 Select **Tools > Configure Templates**.
The **Template Configuration** dialog box appears.
- 2 Expand **Voice Connections Templates**.
- 3 Right click **ISDN to V52 Voice Connections Templates** and select **Add**.
The **ISDN to V52 Voice Connection Template** dialog box appears.
- 4 Enter a name and a description for this template.
The name appears in the selection dialog boxes.
- 5 Configure the voice connection:
From this dialog box you can configure subscriber information.
For details on the subscriber settings, see the online help.
- 6 After finishing the configuration, click **Add**, then **Close**.
After adding the template, it will appear in the **Template Configuration** dialog box.

Related topics:

[Creating AAL2 to V5.2 \(ISDN\) voice configuration templates on page 307](#)

[Creating AAL2 to V5.2 \(PSTN\) voice configuration templates on page 306](#)

[Creating POTS to GR-303 configuration templates on page 312](#)

[Creating POTs to V5.2 configuration templates on page 313](#)

[Creating AAL2 ELCP to V5.2 \(POTS\) configuration templates on page 310](#)

[Creating AAL2 ELCP to V5.2 \(ISDN\) configuration templates on page 309](#)

Creating POTS to GR-303 configuration templates

To create a template for POTS to GR-303 voice connections:

- 1 Select **Tools > Configure Templates**.

The **Template Configuration** dialog box appears.

- 2 Expand **Voice Connections Templates**.

- 3 Right click **POTS to Gr303 Voice Connections Templates** and select **Add**.

The **POTS to GR303 Voice Configuration** dialog box appears.

- 4 Enter a name and a description for this template.

The name appears in the selection dialog boxes.

- 5 Configure the voice connection:

From this dialog box you can configure:

- Subscriber information.
- GR-303 settings:

Local Admin State: Set to **In Service**

Signal Type: Specify **Loop Start**, **Ground Start**, **Loop Reverse Battery**, or **Electronic Business Set**, depending on the configuration of the interface.

- Voice FXS Configuration:

Ring Back: Mark the checkbox to request ring back.

Ring Frequency: Choose the ring frequency from options: **20 Hz**, **25 Hz**, **30 Hz**, or **50 Hz**, to be used in the FXS interface. The default value is **20 Hz**.

Signal Type: Specify a signaling type of FXS interface. The default value is **Loop Start**.

For details on the settings, refer to the online help.

- 6 After finishing the configuration, click **Add**, then **Close**.

After adding the template, it will appear in the **Template Configuration** dialog box.

Related topics:

[Creating AAL2 to V5.2 \(PSTN\) voice configuration templates on page 306](#)

[Creating AAL2 to V5.2 \(ISDN\) voice configuration templates on page 307](#)

[Creating POTs to AAL2 configuration templates on page 314](#)

[Creating POTs to V5.2 configuration templates on page 313](#)

[Creating AAL2 to GR-303 voice configuration templates on page 308](#)

Creating POTs to V5.2 configuration templates

To create a template for POTs to V5.2 voice connections:

- 1 Select **Tools > Configure Templates**.

The **Template Configuration** dialog box appears.

- 2 Expand **Voice Connections Templates**.

- 3 Right click **POTs to V5.2 Voice Connections Templates** and select **Add**.

The **POTs to V5.2 Voice Connection Template** dialog box appears.

- 4 Enter a name and a description for this template.

The name appears in the selection dialog boxes.

- 5 Configure the voice connection:

From this dialog box you can configure:

- Subscriber information.
- AAL2 VCL information.
- V5.2 settings:

Admin Status: Set to **In Service**

Port Type: Specify whether the interface is PSTN or ISDN.

Lease Type: Specify the lease type

Block Type: Specify the port blocking

- CID information.

For more information on these settings, see the online help.

- 6 After finishing the configuration, click **Add**, then **Close**.

After adding the template, it will appear in the **Template Configuration** dialog box.

Related topics:

[Creating AAL2 to V5.2 \(PSTN\) voice configuration templates on page 306](#)

[Creating AAL2 to V5.2 \(ISDN\) voice configuration templates on page 307](#)

[Creating POTs to AAL2 configuration templates on page 314](#)

[Creating POTs to GR-303 configuration templates on page 312](#)

[Creating AAL2 to GR-303 voice configuration templates on page 308](#)

Creating POTs to AAL2 configuration templates

To create a template for POTS voice connections:

- 1 Select **Tools > Configure Templates**.

The **Template Configuration** dialog box appears.

- 2 Expand **Voice Connections Templates**.

- 3 Right click **POTS to AAL2 Voice Connections Templates** and select **Add**.

The **Add Composite Voice Configuration** dialog box appears.

- 4 Enter a name and a description for this template.

The name appears in the selection dialog boxes.

- 5 Configure the voice connection:

From this dialog box you can configure:

- Subscriber information. .
- AAL2 VCLs.
- ATM CIDs.

For information on these settings, see the online help.

- 6 After finishing the configuration, click **Add**, then **Close**.

After adding the template, it will appear in the **Template Configuration** dialog box.

Related topics:

[Creating AAL2 to V5.2 \(PSTN\) voice configuration templates on page 306](#)

[Creating AAL2 to V5.2 \(ISDN\) voice configuration templates on page 307](#)

[Creating POTS to GR-303 configuration templates on page 312](#)

[Creating POTs to V5.2 configuration templates on page 313](#)

[Creating AAL2 to GR-303 voice configuration templates on page 308](#)

Creating POTs to DS1 configuration templates

To create a template for POTS voice connections:

- 1 Select **Tools > Configure Templates**.

The **Template Configuration** dialog box appears.

- 2 Expand **Voice Connections Templates**.

- 3 Right click **POTS to DS1 Voice Connections Templates** and select **Add**.

The **Add POTS to DS1 Voice Connection Template** dialog box appears.

- 4 Enter a name and a description for this template.

The name appears in the selection dialog boxes.

5 Configure Subscriber information. .

For information on these settings, see the online help.

6 After finishing the configuration, click **Add**, then **Close**.

After adding the template, it will appear in the **Template Configuration** dialog box.

Creating EBS to GR-303 configuration templates

To create a template for EBS to GR-303 voice connections:

1 Select **Tools > Configure Templates**.

The **Template Configuration** dialog box appears.

2 Expand **Voice Connections Templates**.

3 Right click **EBS to Gr303 Voice Connections Templates** and select **Add**.

The **Add EBS to GR303 Voice Configuration Template** dialog box appears.

4 Enter a name and a description for this template.

The name appears in the selection dialog boxes.

5 Configure the voice connection:

From this dialog box you can configure:

- Subscriber information.
- GR-303 information:

Local Admin State: Set to **In Service**

Signal Type: Specify **Electronic Business Set**.

For details on the settings, refer to the online help.

6 After finishing the configuration, click **Add**, then **Close**.

After adding the template, it will appear in the **Template Configuration** dialog box.

Related topics:

[Creating AAL2 to V5.2 \(PSTN\) voice configuration templates on page 306](#)

[Creating AAL2 to V5.2 \(ISDN\) voice configuration templates on page 307](#)

[Creating POTs to AAL2 configuration templates on page 314](#)

[Creating POTs to V5.2 configuration templates on page 313](#)

[Creating AAL2 to GR-303 voice configuration templates on page 308](#)

Manage voice connections

NetHorizon enables users to add voice connections for the desired voice connection type. Voice connections can be added manually or through a configuration wizard using pre-configured voice connection templates.

Topics:

[POTS to AAL2 voice connections](#)

[POTS to DS1 voice connections](#)

[POTS to V5.2 voice connections](#)

[POTS to VOIP voice connections](#)

[POTS to GR303 voice connections](#)

[POTS \(RT\) to GR-303 \(COT\) voice connections](#)

[POTS to GR303 ESA voice connections](#)

[ISDN to AAL2 voice connections](#)

[ISDN to V5.2 voice connections](#)

[ISDN SIG to VOIP voice connections](#)

[ISDN to VOIP voice connections](#)

[VOIP \(SIP PLAR\) to GR303 voice connections \(Voice Gateway\)](#)

[VOIP \(SIP PLAR\) to V5.2 voice connections \(Voice Gateway\)](#)

[AAL2 to GR303 voice connections \(Voice Gateway\)](#)

[AAL2 to V5.2 voice connections \(Voice Gateway\)](#)

[AAL2 ELCP to V5.2 voice connections \(Voice Gateway\)](#)

[EBS to GR303 voice connections](#)

[EBS to VOIP voice connections](#)

POTS to AAL2 voice connections

This type of voice connection supports POTS subscriber connections to an AAL2 voice network. For POTS-to-AAL2 configurations, either a voice gateway (such as a Sechtor 100) or a TDM/ATM Uplink card can be used to convert AAL2-derived voice into TDM signaling. For AAL2 connections, the ATM traffic descriptor is required before the voice connection can be configured.

To add voice connections

[Adding POTS to AAL2 voice connections](#)

[Adding POTS to AAL2 voice connections using the wizard \(Z-Edge\)](#)

[Adding POTS to AAL2 voice connections using the wizard \(MALC\)](#)

To modify or view a voice connection, select the desired connection and click **Modify** or **View**. The Modify/View Subscriber Voice Connections dialog appears. When viewing voice connections the fields appear as read-only.

To display voice statistics, select the desired connection and click **Statistics**. The Voice Statistics dialog appears with data for the selected connection.

Adding POTS to AAL2 voice connections

This procedure contains steps for manually adding POTS to AAL2 voice connections.

- 1 Right-click the desired MALC device and select **Manage Voice Connections**. The **Subscriber Voice Connections** dialog box appears.
- 2 Click **POTS To AAL2** tab. The POTS to AAL2 voice connection information appears.
- 3 To add a voice connection, click **Add**. The Creating MALC POTs to AAL2 voice connection screen appears.
- 4 Specify the desired voice connections settings and click **Add** to add the connection.
- 5 Click **Close** to exit the dialog without adding a voice connection.
- 6 Click **Help** to display the help topic for this dialog.

Adding POTS to AAL2 voice connections using the wizard (Z-Edge)

To add POTS to AAL2 voice connections to the MALC:

- 1 Add an ATM traffic descriptor to a device that has already been added to ZMS. See [Creating ATM traffic descriptor configuration templates on page 361](#).
- 2 Add an ATM AAL2 VCL to the uplink interface. See [Creating an ATM AAL2 VCL on page 349](#).

Next, assign a user to the port using that VCL.

- 3 In the tree view, navigate to the device to which you want to add subscribers.
- 4 Right-click on the device and select **Manage Voice Connections**. The **Subscribers Voice Connections** dialog box appears. If there are any voice connections configured on the device, they are displayed here.
- 5 Click **Add (Wizard)**. The **Z-Edge AAL2 to POTS** voice connection wizard appears.
- 6 Select a template.
To view the template configuration, click **View**.
- 7 Click the next button.

The **Select POTS Ports** dialog box appears.

- 8 Select the ports to configure.
- 9 Set the **Voice Connection Admin Status** to **Enable**.
- 10 Click the next button. The **Enter VCL Information** dialog box appears.
- 11 Select one of the options:
 - **Auto-create the AAL2 VCL and CIDs.**
 - **Use an existing AAL2 VCL and auto-create the CIDs**
- 12 If you chose **Auto-create the AAL2 VCL and CIDs**:
 - Enter VPI and VCI values
 - Select a Transmit Traffic Descriptor Template by clicking on the Browse button
 - Select a Receive Traffic Descriptor Template by clicking on the Browse button
 - Enter the POTS channel's CID (ATM Forum suggests 16 to 127).
 - Click **Add**.

For details on these settings, see the online help.

- 13 If you chose **Use an existing AAL2 VCL and auto-create the CIDs**:
 - Select an AAL2 VCL by clicking on the Browse button.
 - Enter the POTS channel's CID (ATM Forum suggests 16 to 127).
 - Click **Add** and then **Close**.

For details on these settings, see the online help.

The status of AAL2 to POTS voice connections is displayed.

Adding POTS to AAL2 voice connections using the wizard (MALC)

- 1 Add an ATM traffic descriptor to a device that has already been added to ZMS. See [Creating ATM traffic descriptor configuration templates on page 361](#).
- 2 Add an ATM AAL2 VCL to the uplink interface. See [Creating an ATM AAL2 VCL on page 349](#).

Next, assign a user to the port using that VCL.

- 3 In the tree view, navigate to the device to which you want to add subscribers.
- 4 Right-click on the device and select **Manage Voice Connections**.

The **Subscribers Voice Connections** dialog box appears. If there are any voice connections configured on the device, they are displayed here.

- 5 Click the POTS to AAL2 tab (the default).

6 Click Add (Wizard).

The POTS to AAL2 wizard appears.

7 Select a template.

To view the template configuration, click **View**.

8 Click the next button.

The **Select POTS Ports** dialog box appears.

9 From this dialog box select the POTS ports to configure connections on:

- Enable the voice connection.
- Select the slot and port for the connection. Note that you can select multiple ports to create multiple connections.

10 Click the next button.**11 If there is already a VCL connection configured for this slot, the View VCL Information dialog box appears, displaying the configured VCL.**

If there is not a VCL configured for the slot:

- Click the browse button to specify an Uplink interface.
- Select a VPI/VCI.
- Click the browse button to specify an ATM traffic descriptor.

12 Click Add.

ZMS displays a status screen, which indicates the progress of adding the voice connections.

13 When the connections have been added, click Close.

The connections are displayed in the **Subscriber Voice Connections** dialog box. To modify or delete the connection, highlight the connection and click **Modify** or **Delete**.

Related topics:

[Adding POTS to GR-303 ESA voice connections using the wizard on page 332](#)

[Adding voice gateway AAL2 subscribers on page 347](#)

[Finding ATM VCLs and cross connects on page 461](#)

[Ringing POTS phone on page 319](#)

Ringing POTS phone

NetHorizon allows you to test the connection to the POTS phone by sending a ring command to a selected POTS port.

To ring a POTS port:

1 Select the desired POTS port in the Tree view and either choose View > Test > Ring Phone or right click the desired port and choose Ring Phone.

The Modify POTS Ring Phone dialog appears.

- 2 Specify the desired ring cadence and ring time.
- 3 Click **Apply** to ring the specified port. Otherwise, click **Close**.
- 4 The Ring Status dialog appears.

If the ring ends successfully a confirmation message appears. Otherwise, a message describing the ring failure appears.

POTS to DS1 voice connections

This type of voice connection supports POTS subscriber connections to an DS1 voice signals.

To add voice connections

[Adding POTS to DS1 voice connections on page 320](#)

To modify or view a voice connection, select the desired connection and click **Modify** or **View**. The Modify/View Subscriber Voice Connections dialog appears. When viewing voice connections the fields appear as read-only. .

To display voice statistics, select the desired connection and click **Statistics**. The Voice Statistics dialog appears with data for the selected connection. .

To ring the POTS port, see [Ringing POTS phone on page 319](#)

Adding POTS to DS1 voice connections

This procedure contains steps for manually adding POTS to DS1 voice connections.

- 1 Right-click the desired MALC device and select **Manage Voice Connections**. The **Subscriber Voice Connections** dialog box appears.
- 2 Click **POTS To DS1** tab. The POTS to DS1 voice connection information appears.
- 3 To add a voice connection, click **Add**. The Creating MALC POTS to DS1 voice connection screen appears.
- 4 Specify the desired voice connections settings and click **Add** to add the connection.
- 5 Click **Close** to exit the dialog without adding a voice connection.
- 6 Click **Help** to display the help topic for this dialog.

POTS to V5.2 voice connections

This type of voice connection supports POTS subscriber connections to an V5.2 voice network. For POTS-to-V5.2 configurations, either a voice gateway (such as a Sechtor 100) or a TDM/ATM Uplink card can be used to convert AAL2-derived voice into TDM signaling. For AAL2 connections, the

ATM traffic descriptor is required before the voice connection can be configured.

To add voice connections

[Adding POTS to V5.2 voice connections](#)

[Adding POTS to V5.2 voice connections using the wizard](#)

To modify or view a voice connection, select the desired connection and click **Modify** or **View**. The Modify/View Subscriber Voice Connections dialog appears. When viewing voice connections the fields appear as read-only..

To display voice statistics, select the desired connection and click **Statistics**. The Voice Statistics dialog appears with data for the selected connection..

To ring the POTS port, see [Ringing POTS phone on page 319](#)

Adding POTS to V5.2 voice connections

This procedure contains steps for manually adding POTS to V5.2 voice connections.

- 1** Right-click the desired MALC device and select **Manage Voice Connections**. The **Subscriber Voice Connections** dialog box appears.
- 2** Click **POTS To V5.2** tab. The POTS to V5.2 voice connection information appears.
- 3** To add a voice connection, click **Add**. The **Creating MALC POTS to V5.2 Voice Connection** screen appears.
- 4** Specify the desired voice connections settings and click **Add** to add the connection.
- 5** Click **Close** to exit the dialog without adding a voice connection.
- 6** Click **Help** to display the help topic for this dialog.

Adding POTS to V5.2 voice connections using the wizard

- 1** Right-click the device and select **Manage Voice Connections**. The **Subscriber Voice Connections** dialog box appears.
- 2** Click **Add (Wizard)**. The **POTS to V5.2** voice connection wizard appears.
- 3** Select a template.
To view the template configuration, click **View**.
- 4** Click the next button.
The **Select POTS Ports** dialog box appears.
- 5** Select the ports to configure.
- 6** Set the **Voice Connection Admin Status** to **Enable**.
- 7** Click the next button.

The **V5.2 User Endpoint** dialog box appears.

- 8 Select the interface group and the starting address.

For details on these settings, see the online help.

- 9 Click the next button.

The status of POTS to V5.2 voice connections is displayed.

POTS to VOIP voice connections

This type of voice connection supports POTS subscriber connections to an VOIP voice network. For POTS-to-VOIP configurations, the MALC converts POTS voice signals into VOIP packets for either SIP, MGCP, Megaco VOIP networks. For VOIP connections, ensure the VOIP systems settings are configured for the desired VOIP network. See [Manage VOIP connections on page 350](#).

To add voice connections

[Adding POTS to VOIP voice connections on page 322](#)

To modify or view a voice connection, select the desired connection and click **Modify** or **View**. The Modify/View Subscriber Voice Connections dialog appears. When viewing voice connections the fields appear as read-only..

To display voice statistics, select the desired connection and click **Statistics**. The Voice Statistics dialog appears with data for the selected connection. .

To ring the POTS port, see [Ringing POTS phone on page 319](#).

ISDN to VOIP voice connection is similar to the POTS to VOIP connection.

Adding POTS to VOIP voice connections

This procedure contains steps for manually adding POTS to VOIP voice connections.



Note: VOIP connections to SIP phones is only possible out one MALC interface. Communication with SIP phones which are in the same network as other interfaces on the MALC is not supported.

- 1 Right-click the desired device and select **Manage Voice Connections**. The **Subscriber Voice Connections** dialog box appears.
- 2 Click **POTS To VOIP** tab. The POTS to VOIP voice connection information appears.
- 3 To add a voice connection, click **Add**. The **Creating POTs to VOIP Voice Connection** screen appears.
- 4 Specify the desired voice connections settings and click **Add** to add the connection.

VOIP Endpoint pane provides the following voice features:

1. Directory Number

2. The VOIP endpoint User Name is case sensitive and must match the voice switch requirements, for example AAL/1 for Nortel switch MGCP or TP/0001 for Nortel switch Megaco.
3. The Authorized User Name is used for calculating the credentials, when received 401/407 response. This field is optional, if it is not configured, then its value is same as User Name field.



Note: The * character is supported in the Directory number.

The Registration server option is available only when PLAR is disabled.

4. Password
5. Preferred Codec
6. G711 Fallback
7. Frames Per Packet
8. G726 Byte Order
9. Hotline DN: Specify a hotline directory number.
10. Hotline Initialization Timer
11. PLAR Address Type: Specify it is IPv4 or DNS
12. PLAR Address:
13. UDP Port Number
14. The T.38 fax option enables fax messages to be transported across VoIP networks between G3 fax terminals. When configured for VoIP or SIP PLAR and T.38, MALC provides a T.38 fax relay service between two devices configured for the same VoIP protocol. If one side of the T.38 connection is not configured for T.38 support, the fax call reverts to g.711 pass through when this option is configured. Otherwise, the fax may not go through.

By default, T.38 fax service is T38 NONE, it is disabled. To enable T. 38 fax service using UDP IP packet, select T38 UDPTL.
15. The Registration Server contains numbers between 1 and 255 which identifies the VoIP server that is responsible for this particular end point. If this value is not 0, a voip-server-entry with this address.

Connection Features pane provides the following subscriber voice features:

1. hookflash: Hookflash is either a button on the phone to simulate the quick offhook/onhook/offhook cycle or the actual cycle itself. Hookflash can be used as the trigger event for switching to call waiting or three way call conferencing.
2. On-hook signaling: On-hook signaling indicates the phone can accept any features or signals that only enabled while the phone is on-hook.

3. Call wait: When an incoming call is received the receiver of the call is notified by a tone of an incoming call; the hookflash trigger switches the subscriber between the ongoing call and the incoming call. The original call is placed on hold.

4. Call transfer: When the call transfer feature is added to hookflash, the NetHorizon supports transferring calls. The hookflash trigger during an ongoing call gives the subscriber a secondary dialtone and will accept dialing. The original call is on hold until another hookflash.

5. Conference:

The MXK local call conferencing feature is supported only with SIP.

MGCP and H.248 have the conferencing feature on their switch side.

The MXK call conferencing feature enables three-way conference calls during which three parties can use one calling session to communicate. The voice cards support call conferencing. These cards work with any VOIP-enabled uplink card installed in the MXK.

The MXK call conferencing feature deploys an efficient end-mixing conference call technology, avoiding the overhead of the centralized conference server.

Three-way call conferencing follows the Telcordia (Bellcore) three-way calling standard called Telcordia - TR - TSY - 000577, Three-Way Calling.

6. Reverse Polarity: The reverse-battery feature is supported for SIP, SIP-PLAR, MGCP and H.248 softswitch applications.

For SIP, LSAS is provided when “200 OK” is received on the far end answer. The LSAS tone can be configured in the subscriber side.

For SIP-PLAR, the v5 switch configures the reverse-battery feature automatically, no configuration required at the subscriber side.

For MGCP, and H.248, the softswitch configures the reverse battery feature automatically, no configuration required at the subscriber side.

7. Line Side Supervising Tone: In this case the MXK plays a far end answer supervision tone on the local loop when it receives “200 OK” on far end answer. This feature is for SIP only. This signal support requires the MXK-POTS-72. For SIP, the LSAS tone or reverse battery signal are configured via the **features** parameter in the **subscriber-voice** profile. These options — **lss-tone** and **lss-rb** are mutually exclusive, so cannot be set on the same interface. These **feature** options are also mutually exclusive with **hookflash**.

8. DTMF-RFC 2833 and DTMF-Inband: The behavior changes based on the settings in the POTS and VoIP connection (the **Creating POTS to VOIP Voice Connection** window or the **Modifying POTS to VOIP Voice Connection** window) and VoIP server (the **Add VoIP Server** window or the **Modify VoIP Server** window):

If neither DTMF-RFC 2833 and DTMF-Inband field are set in the POTS and VoIP connection, the behavior will be based on the DTMF mode field of the VoIP server;

If only DTMF-RFC 2833 is set in the POTS and VoIP connection, the subscriber will support RFC 2833 only irrespective of what set in the DTMF mode field in the VoIP server;

If only DTMF-Inband is set in the POTS and VoIP connection, the subscriber will support DTMF inband only irrespective of what set in the DTMF mode field of the VoIP server;

If both DTMF-RFC 2833 and DTMF-Inband field are set in the subscriber level, should be the same behavior as if the DTMF mode field of the VoIP server is set to RFC 2833.

9. Voice Only

10. Hot Line: Enable or disable hot line on a port after creating the POTS and VoIP connection. Note that hot line and warm line features cannot be enabled at the same time.

11. Warm Line: Enable or disable warm line on a port after creating the POTS and VoIP connection. Note that hot line and warm line features cannot be enabled at the same time.

12. Call On Disconnect

13. Data Only

14. Centrex : Enable or disable centrex on the subscriber. The difference between a centrex subscriber and a non-centrex subscriber is when the subscriber goes onhook after initiating a local three way conference. centrex subscriber initiates a call transfer between the remaining subscribers in the conference. That way the other two parties can still be in a conversation. A non-centrex subscriber disconnects the conference completely and all the parties involved in the conference are disconnected.

5 Click **Close** to exit the dialog without adding a voice connection.

6 Click **Help** to display the help topic for this dialog.

POTS to GR303 voice connections

This type of voice connection supports POTS subscriber connections to an GR-303 voice network.

To add voice connections:

[Configuring VOIP settings for POTS to GR303 voice connections on page 326](#)

[Adding POTS to GR303 voice connections on page 326](#)

[Adding POTS to GR-303 voice connections using the wizard on page 327](#)

To modify or view a voice connection, select the desired connection and click **Modify** or **View**. The Modify/View Subscriber Voice Connections dialog appears. When viewing voice connections the fields appear as read-only..

To display voice statistics, select the desired connection and click **Statistics**. The Voice Statistics dialog appears with data for the selected connection..

To ring the POTS port, see [Ringling POTS phone on page 319](#).

Configuring VOIP settings for POTS to GR303 voice connections

This procedure contains steps for configuring VOIP settings for POTS to GR303 voice connections.

- 1 Right-click the desired MALC device and select **Manage VOIP**. The **VOIP Configuration Manager** dialog box appears with VOIP server settings.
- 2 Click **Add** to add a voice server with the following entries:
 - Registration Service set to 255
 - Server Address set to the IP address of the MALC
 - Address Type set to IPv4
 - UDP Port Number set to 5060
 - Server Type set to the type of VOIP server used.
 - Protocol set to SIP.Click **OK** to add the VOIP server with the specified entries.
- 3 To setup the SIP dialplan, click the **SIP DialPlan** tab. The SIP Dialplan settings appear.
- 4 Click **Add** to add a SIP dialplan with the desired settings.

Specify the desired SIP dialplan settings. Ensure that the Registration Server Index value is set to 0.
- 5 Click **Close** to exit the dialog without adding a voice connection.
- 6 Click **Help** to display the help topic for this dialog.

Adding POTS to GR303 voice connections

This procedure contains steps for manually adding POTS to GR303 voice connections.

- 1 Right-click the desired MALC device and select **Manage Voice Connections**. The **Subscriber Voice Connections** dialog box appears.
- 2 Click **POTS To GR303** tab. The POTS to GR303 voice connection information appears.
- 3 To add a voice connection, click **Add**. The **Creating MALC POTs to GR303 voice connection** screen appears.

- 4 Specify desired voice connection settings:
 - a Specify the Voice Connection Admin Status.
 - b Select the POTS ports.
 - c Specify the desired GR303 CRV Endpoint settings:
 - **GR303 Interface Group:** This value is fixed to **164 Gr303Ig**
 - **Starting Crv Index:** Select a available Crvs index or range.
 - **Signal Type:** Specify **Loop Start**, **Loop Reverse Batter**, **Ground Start**, or **Electronic Business Set**, depending on the configuration of the interface.
- 5 Click **Add** to add the connection.
- 6 Click **Close** to exit the dialog without adding a voice connection.
- 7 Click **Help** to display the help topic for this dialog.
- 8 To modify the GR303 CRV configuration settings, right-click on the desired GR303 Interface Group CRV profile that is listed under **GR303 Interface Groups** under device in the tree view, and select **Modify**.
The **Modify GR303 CRV Configuration** dialog appears.
- 9 In the **Modify GR303 CRV Configuration** dialog, specify the desired changes.
For the details on the settings, refer to online help.

Adding POTS to GR-303 voice connections using the wizard

To add POTS to GR-303 voice connections to the MALC:

- 1 Add an ATM traffic descriptor to a device that has already been added to ZMS. See [Creating ATM traffic descriptor configuration templates on page 361](#).
- 2 Add an ATM AAL2 VCL to the uplink interface. See [Creating an ATM AAL2 VCL on page 349](#).

Next, assign a user to the port using that VCL.

- 3 In the tree view, navigate to the device to which you want to add subscribers.
- 4 Right-click on the device and select **Manage Voice Connections**.
The **Subscribers Voice Connections** dialog box appears. If there are any voice connections configured on the device, they are displayed here.
- 5 Click the **POTS to GR-303** tab.
The information for POTS to GR-303 voice connections appears in the Subscribe Voice Connections dialog.
- 6 Click **Add (Wizard)** button.
The POTS to GR-303 wizard appears.

7 Select a template.

To view the template configuration, click **View**.

8 Click the next button.

The **Select POTS Ports** dialog box appears.

9 From this dialog box select the POTS ports to configure connections on:

- Enable the voice connection.
- Select the slot and port for the connection. Note that you can select multiple ports to create multiple connections.

10 Click the next button.

The **GR303 CRV Endpoint** dialog box appears.

11 Enter the CRV starting value. If you have selected multiple connections, ZMS will create the connections starting with this value.

Specify the Local Admin State and Signal Type.

12 Click **Add**.

ZMS displays a screen for the directory number and registration server.

13 When the connections have been added, the confirmation message appears.

Click **OK**.

The connections are displayed in the **Subscriber Voice Connections** dialog box. To modify or delete the connection, highlight the connection and click **Modify** or **Delete**.

Related topics:

[Creating POTS to GR-303 configuration templates on page 312](#)

[Adding POTS to GR303 voice connections on page 326](#)

POTS (RT) to GR-303 (COT) voice connections

POTS (RT) to GR-303 (COT) voice connections cross two MALCs using POTS to VOIP and VOIP to GR-303 connections over an RPR ring. ZMS enables users to provision POTS (RT) to GR-303 (COT) voice connections on both MALCs from a single dialog.

For POTS to VOIP configurations, the MALC converts POTS voice signals into VOIP SIP packets and transports the packets around an RPR ring to the MALC with the voice gateway card.

For VOIP to GR-303 connections on the voice gateway card, VOIP packets destined for the voice gateway card enter through the GigE MALC uplink card interface and are terminated on the voice gateway card. The voice signal is converted to TDM T1/E1 channels and sent to the local switch for TDM voice processing. For traffic coming from the local switch, the TDM voice signals are converted to VOIP packets by the voice gateway card and routed

back out the MALC uplink card, transported around the RPR ring to the configured VOIP destination, and then converted to POTS voice signals.

To modify or view the POTS(RT) to GR-303 (COT) voice connection data:

- For POTS to VOIP connections, see [POTS to VOIP voice connections on page 322](#).
- For VOIP to GR-303 connections using the voice gateway, see [VOIP \(SIP PLAR\) to GR303 voice connections \(Voice Gateway\) on page 337](#)

Adding POTS (RT) to GR-303 (COT) voice connections

This procedure contains steps for adding POTS (RT) to GR-303 (COT) voice connections across two MALCs that are connected over an RPR ring.



Note: All uplink cards, subscriber cards, IP interfaces, GR-303 interface groups and RPR ring settings must be configured before provisioning this type of voice connection.

To configure IP and VOIP settings, see [Manage VOIP connections on page 350](#) [Manage VOIP connections on page 350](#).

- 1 Right-click the MALC with the configured voice gateway card and select **Provision POTS(RT) to GR303(COT) Voice**. The **Creating POTS to VOIP and VOIP to GR303 Voice Connections on Selected MALCs** dialog box appears.

Specify the connection name and select **Enabled** Admin Status to enable the voice connections. For disabled voice connections, the configuration settings are preserved, but the voice connections are not provisioned.

For MALC with the voice gateway card, modify the desired Voice Gateway Endpoint, VOIP Endpoint, Connection Features, and GR303 CRV endpoint data. The VOIP endpoint user name is case sensitive and must match the voice switch requirements, for example AAL/1 for Nortel switch MGCP or TP/0001 for Nortel switch Megaco.

- 2 Click the browse button to select the MALC on the Subscriber End.
The Available POTS Ports information appears.
- 3 Specify the Subscriber End data and select the desired POTS ports. The VOIP endpoint user name is case sensitive and must match the voice switch requirements, for example AAL/1 for Nortel switch MGCP or TP/0001 for Nortel switch Megaco.
- 4 Click **Add** to add voice connection and subscribers across the MALCs to complete the POTS (RT) to GR-303 (COT) voice connection.
The Creating Voice Connections status message appears followed by a confirmation that all voice connections were successfully created.
- 5 Click **OK**.

- 6 Click **Help** to display the help topic for this dialog.

Click **Close** to exit the dialog without adding a voice connection.

To modify or view the voice connection data for POTS subscribers or voice gateway connections, right-click the desired MALC and select **Manage Voice Connections**.

For VOIP to GR-303 connections using the voice gateway, see [VOIP \(SIP PLAR\) to GR303 voice connections \(Voice Gateway\) on page 337](#).

For POTS to VOIP connections, see [POTS to VOIP voice connections on page 322](#).

POTS to GR303 ESA voice connections

This type of voice connection supports POTS subscriber connections to an GR-303 voice network with an Emergency Standalone (ESA) backup connection enabled. For POTS-to-GR303 ESA configurations, the MALC interconnects POTS equipment directly to GR-303 switches. For GR-303 voice connections, the GR-303 interface with IG must already exist.

In addition, VOIP server and SIP dialplan settings are required for the ESA support.

To add voice connections:

[Configuring VOIP settings for POTS to GR303 ESA voice connections on page 330](#)
[Configuring VOIP settings for POTS to GR303 ESA voice connections](#)

[Adding POTS to GR303 ESA voice connections on page 331](#)

[Adding POTS to GR-303 ESA voice connections using the wizard on page 332](#)

To modify or view a voice connection, select the desired connection and click **Modify** or **View**. The Modify/View Subscriber Voice Connections dialog appears. When viewing voice connections the fields appear as read-only..

To display voice statistics, select the desired connection and click **Statistics**. The Voice Statistics dialog appears with data for the selected connection..

To ring the POTS port, see [Ringing POTS phone on page 319](#).

Configuring VOIP settings for POTS to GR303 ESA voice connections

This procedure contains steps for configuring VOIP settings for POTS to GR303 ESA voice connections.

- 1 Right-click the desired MALC device and select **Manage VOIP**. The **VOIP Configuration Manager** dialog box appears with VOIP server settings.
- 2 Click **Add** to add a voice server with the following entries:
 - Registration Service set to 255

- Server Address set to the IP address of the MALC
- Address Type set to IPv4
- UDP Port Number set to 5060
- Server Type set to the type of VOIP server used.
- Protocol set to SIP.

Click **OK** to add the VOIP server with the specified entries.

- 3** To setup the SIP dialplan, click the **SIP DialPlan** tab. The SIP Dialplan settings appear.
- 4** Click **Add** to add a SIP dialplan with the desired settings.
Specify the desired SIP dialplan settings. Ensure that the Registration Server Index value is set to 0.
- 5** Click **Close** to exit the dialog without adding a voice connection.
- 6** Click **Help** to display the help topic for this dialog.

Adding POTS to GR303 ESA voice connections

This procedure contains steps for manually adding POTS to GR303 ESA voice connections.

- 1** Right-click the desired MALC device and select **Manage Voice Connections**. The **Subscriber Voice Connections** dialog box appears.
- 2** Click **POTS To GR303 ESA** tab. The POTS to GR303 ESA voice connection information appears.
- 3** To add a voice connection, click **Add**. The **Creating MALC POTs to GR303 ESA voice connection** screen appears.
- 4** Specify desired voice connection settings:
 - a** Specify the Voice Connection Admin Status.
 - b** Select the POTS ports.
 - c** Specify the desired GR303 CRV Endpoint settings:
 - **GR303 Interface Group:** This value is fixed to **164 Gr303Ig**
 - **Starting Crv Index:** Select a available Crvs index or range.
 - **Signal Type:** Specify **Loop Start**, **Loop Reverse Batter**, **Ground Start**, or **Electronic Business Set**, depending on the configuration of the interface.
 - d** Specify the desired ESA settings. The Directory Number is the phone number associated with the selected port for ESA connections.
- 5** Click **Add** to add the connection.
- 6** Click **Close** to exit the dialog without adding a voice connection.
- 7** Click **Help** to display the help topic for this dialog.

Adding POTS to GR-303 ESA voice connections using the wizard

To add POTS to GR-303 ESA voice connections to the MALC:

- 1** Add an ATM traffic descriptor to a device that has already been added to ZMS. See [Creating ATM traffic descriptor configuration templates on page 361](#).
- 2** Add an ATM AAL2 VCL to the uplink interface. See [Creating an ATM AAL2 VCL on page 349](#).

Next, assign a user to the port using that VCL.

- 3** In the tree view, navigate to the device to which you want to add subscribers.
- 4** Right-click on the device and select **Manage Voice Connections**.

The **Subscribers Voice Connections** dialog box appears. If there are any voice connections configured on the device, they are displayed here.

- 5** Click the **POTS to GR-303 ESA** tab.

The information for ESA connections appears in the Subscribe Voice Connections dialog.

- 6** Click **Add (Wizard)** button.

The POTS to GR-303 ESA wizard appears.

- 7** Select a template.

To view the template configuration, click **View**.

- 8** Click the next button.

The **Select POTS Ports** dialog box appears.

- 9** From this dialog box select the POTS ports to configure connections on:
 - Enable the voice connection.
 - Select the slot and port for the connection. Note that you can select multiple ports to create multiple connections.

- 10** Click the next button.

The **GR303 CRV Endpoint** dialog box appears.

- 11** Enter the CRV starting value. If you have selected multiple connections, ZMS will create the connections starting with this value.

- 12** Click **Add**.

ZMS displays a screen for the directory number and registration server.

- 13** When the connections have been added, the confirmation message appears.

Click **OK**.

The connections are displayed in the **Subscriber Voice Connections** dialog box. To modify or delete the connection, highlight the connection and click **Modify** or **Delete**.

Related topics:

[Creating AAL2 to GR-303 voice configuration templates on page 308](#)

[Adding POTS to GR303 ESA voice connections on page 331](#)

ISDN to AAL2 voice connections

This type of voice connection supports ISDN subscriber connections to an AAL2 voice network. For ISDN-to-AAL2 configurations, either a voice gateway (such as a Sechtor 100) or a TDM/ATM Uplink card can be used to convert AAL2-derived voice into TDM signaling. For AAL2 connections, the ATM traffic descriptor is required before the voice connection can be configured.

To add voice connections

[Adding ISDN to AAL2 voice connections on page 333](#)

To modify or view a voice connection, select the desired connection and click **Modify** or **View**. The Modify/View Subscriber Voice Connections dialog appears. When viewing voice connections the fields appear as read-only. .

To display voice statistics, select the desired connection and click **Statistics**. The Voice Statistics dialog appears with data for the selected connection. .

Adding ISDN to AAL2 voice connections

To add ISDN to AAL2 voice connections to the MALC:

- 1 Add an ATM traffic descriptor to a device that has already been added to ZMS. See [Creating ATM traffic descriptor configuration templates on page 361](#).
- 2 Add an ATM AAL2 VCL to the uplink interface. See [Creating an ATM AAL2 VCL on page 349](#).

Next, assign a user to the port using that VCL.

- 3 In the tree view, navigate to the device to which you want to add subscribers.
- 4 Right-click on the device and select **Manage Voice Connections**.

The **Subscribers Voice Connections** dialog box appears. If there are any voice connections configured on the device, they are displayed here.

- 5 Click the **ISDN to AAL2** tab.
- 6 Click **Add**.

The **MALC ISDN to AAL2 Voice Connection** wizard appears.

- 7 Select a template.

To view the template configuration, click **View**.

- 8 Click the next button.

The **Select ISDN Ports** dialog box appears.

- 9 From this dialog box select the ISDN ports on which to configure connections by selecting the ISDN port.
- 10 Click the next button. The **VCL Info for D Channels** dialog box appears.
- 11 Select one of the options:

- **Auto-create the AAL2 VCL and CIDs.**
- **Use an existing AAL2 VCL and auto-create the CIDs**

- 12 If you chose **Auto-create the AAL2 VCL and CIDs**:

- Select an Uplink/AAL2 physical interface by clicking on the Browse button.
- Enter VPI and VCI values
- Enter the D channel's CID (ATM Forum suggests 128 to 159).
- Click **Add**.

For details on these settings, see the online help.

- 13 If you chose **Use an existing AAL2 VCL and auto-create the CIDs**:

- Select an AAL2 VCL by clicking on the Browse button.
- Enter the D channel's CID (ATM Forum suggests 128 to 159).
- Click **Add**.

For details on these settings, see the online help.

The status of ISDN to AAL2 voice connections is displayed.

- 14 When the connections have been added, click **Close**.

Related topics:

[Adding POTS to GR-303 ESA voice connections using the wizard on page 332](#)

[Adding voice gateway AAL2 subscribers on page 347](#)

[Finding ATM VCLs and cross connects on page 461](#)

ISDN to V5.2 voice connections

This type of voice connection supports ISDN subscriber connections to an V5.2 voice network. For ISDN-to-V5.2 configurations, either a voice gateway (such as a Sechtor 100) or a TDM/ATM Uplink card can be used to convert AAL2-derived voice into TDM signaling.

To add voice connections:

[Adding ISDN to V5.2 voice connections](#)

To modify or view a voice connection, select the desired connection and click **Modify** or **View**. The Modify/View Subscriber Voice Connections dialog appears. When viewing voice connections the fields appear as read-only..

To display voice statistics, select the desired connection and click **Statistics**. The Voice Statistics dialog appears with data for the selected connection..

Adding ISDN to V5.2 voice connections

- 1 Right-click the device and select **Manage Voice Connections**. The **Subscriber Voice Connections** dialog box appears.
- 2 Click **Add**. The **Creating MALC ISDN to V5.2 Voice Connection** dialog appears.
- 3 Select a template.
To view the template configuration, click **View**.
- 4 Click the next button.
The **Select ISDN Ports** dialog box appears.
- 5 Select the ports to configure.
- 6 Set the **Voice Connection Admin Status** to **Enable**.
- 7 Click the next button.
The **V5.2 User Endpoint** dialog box appears.
- 8 Select the interface group and the starting address.
For details on these settings, see the online help.
- 9 Click the **Add** button.

The status of ISDN to V5.2 voice connections is displayed.

ISDN SIG to VOIP voice connections

This type of voice connection supports ISDN subscriber connections to an VOIP voice network. For ISDN-to-VOIP configurations, the MALC converts ISDN voice signals into VOIP packets. For VOIP connections, ensure the VOIP systems settings are configured for the desired VOIP network. See [Manage VOIP connections on page 350](#).

To add voice connections

[Adding ISDN SIG to VOIP voice connections](#)

To modify or view a voice connection, select the desired connection and click **Modify** or **View**. The Modify/View Subscriber Voice Connections dialog appears. When viewing voice connections the fields appear as read-only..

To display voice statistics, select the desired connection and click **Statistics**. The Voice Statistics dialog appears with data for the selected connection..

Adding ISDN SIG to VOIP voice connections

This procedure contains steps for manually adding ISDN to VOIP voice connections.

- 1 Right-click the desired MALC device and select **Manage Voice Connections**. The **Subscriber Voice Connections** dialog box appears.
- 2 Click **ISDN SIG To VOIP** tab. The ISDN to VOIP voice connection information appears.
- 3 To add a voice connection, click **Add**. The **Creating ISDN Signalling to VOIP Voice Connection** screen appears.
- 4 Specify the desired voice connections settings and click **Add** to add the connection. For details on Signaling Index, refers to [Configuring ISDN signaling profiles on page 357](#).
- 5 Click **Close** to exit the dialog without adding a voice connection.
- 6 Click **Help** to display the help topic for this dialog.

ISDN to VOIP voice connections

There are two types of Isdn To Voip connection can be created:

- PLAR enabled
- PLAR disabled

(ISDN to VOIP voice connection is similar to the POTS to Voip connection)

.See [Manage VOIP connections on page 350](#).

To add voice connections

[Adding ISDN to VOIP voice connections on page 336](#)

To modify or view a voice connection, select the desired connection and click **Modify** or **View**. The Modify/View Subscriber Voice Connections dialog appears. When viewing voice connections the fields appear as read-only..

To display voice statistics, select the desired connection and click **Statistics**. The Voice Statistics dialog appears with data for the selected connection. .

Adding ISDN to VOIP voice connections

This procedure contains steps for manually adding ISDN to VOIP voice connections.

- 1 If Plar is disabled. There must be an existing IUA server entry before the ISDN to VOIP connection creation.

To create an iua-server-entry for an application, it is mandatory that configure at least one voip-server entry with megaco protocol for the application.

- a Right-click the desired MALC device and select **Manage VoIP**. The **VoIP Configuration Manager** dialog box appears.

- b** Click **IUA Server** tab. The existing IUA servers information appear.
- c** To add an IUA server entry, click **Add**. The **Add IUA Server** screen appears.
- d** Specify the following settings to your desired values, and click **Add** to add the IUA server information:

Registration Server (0...255): VoIP registration server address. A number between 1 and 255 which identifies the VoIP server that is responsible for this particular end point.

Server Index (0..255) : A unique identifier of a server address. When multiple addresses are configured and if one address isn't reachable, then another can be tried.

Server Address: The address of IUA server.

UDP Port Number: The port number for IUA server. It is an integer and in the range of 1 to 65535.

2 To create ISDN to VOIP voice connection.

- a** Right-click the desired MALC device and select **Manage Voice Connections**. The **Subscriber Voice Connections** dialog box appears.
- b** Click **ISDN To VOIP** tab. The existing ISDN to VOIP voice connections information appears.
- c** To add a voice connection, click **Add**. The **Creating ISDN to VOIP Voice Connections** screen appears.
- d** Specify the desired settings and click **Add** to add the IUA server information.

If PLAR is disabled, an IUA server entry must be created in the Step 1.

If PLAR is enabled, there is no need for IUA server entry instead VOIP entry with SIP protocol should be configured.

VOIP (SIP PLAR) to GR303 voice connections (Voice Gateway)

For VOIP to GR303 connections on the voice gateway card, VOIP packets destined for the voice gateway card enter through one of the MALC uplink card interfaces (GigE, SONET, IP) and are terminated on the voice gateway card. The voice signal is converted to TDM T1/E1 channels and sent to the local switch for TDM voice processing. For traffic coming from the local switch, the TDM voice signals are converted to VOIP packets by the voice gateway card and routed back out the MALC uplink card to the configured VOIP destination.

All the ATM/IP uplink cards including Uplink-GIGE/OC-12-HP and Uplink-RprGigE cards can be used for connecting VOIP traffic to the voice gateway card.

Configuring a VOIP to TDM voice gateway connection involves configuring the voice gateway for a VOIP host and adding a VOIP to TDM voice connection. Before configuring a VOIP to TDM connection, create a new ip-interface-record and unnumbered interface.

To configure IP and VOIP settings, see [Manage VOIP connections on page 350](#).

To add voice connections see [Adding VOIP to GR303 voice connections on page 338](#).

To modify or view a voice connection, select the desired connection and click **Modify** or **View**. The Modify/View Subscriber Voice Connections dialog appears. When viewing voice connections the fields appear as read-only. .

To display voice statistics, select the desired connection and click **Statistics**. The Voice Statistics dialog appears with data for the selected connection. .

Adding VOIP to GR303 voice connections

This procedure contains steps for manually adding VOIP to GR303 voice connections.

- 1 Right-click the desired MALC device and select **Manage Voice Connections**. The **Subscriber Voice Connections** dialog box appears.
- 2 Click **VOIP To GR303** tab. The VOIP to GR303 voice connection information appears.
- 3 To add a voice connection, click **Add**. The **Creating MALC VOIP to GR303 Voice Connections** screen appears.
- 4 Specify desired voice connection settings:
 - a Select the IP Interface.
 - b Specify the PLAR status.
 - c Specify the Voice Connection Admin Status.
 - d Specify the desired GR303 CRV Endpoint settings:
 - **GR303 Interface Group**: This value is fixed to **164 Gr303Ig**
 - **Starting Crv Index**: Select a available Crvs index or range.
 - **Signal Type**: Specify **Loop Start**, **Loop Reverse Batter**, **Ground Start**, or **Electronic Business Set**, depending on the configuration of the interface.
 - e Specify the desired Connection Features settings.
 - f Specify the desired VOIP Endpoint settings.
- 5 Click **Add** to add the connection.
- 6 Click **Close** to exit the dialog without adding a voice connection.
- 7 Click **Help** to display the help topic for this dialog.

VOIP (SIP PLAR) to V5.2 voice connections (Voice Gateway)

For VOIP to V5.2 connections on the voice gateway card, VOIP packets destined for the voice gateway card enter through one of the NetHorizon uplink card interfaces (GigE, SONET, IP) and are terminated on the voice gateway card. The voice signal is converted to TDM T1/E1 channels and sent to the local switch for TDM voice processing. For traffic coming from the local switch, the TDM voice signals are converted to VOIP packets by the voice gateway card and routed back out the NetHorizon uplink card to the configured VOIP destination.

All the ATM/IP uplink cards including Uplink-GIGE/OC-12-HP and Uplink-RprGigE cards can be used for connecting VOIP traffic to the voice gateway card.

Configuring a VOIP to TDM voice gateway connection involves configuring the voice gateway for a VOIP host and adding a VOIP to TDM voice connection. Before configuring a VOIP to TDM connection, create a new ip-interface-record and unnumbered interface.

To configure IP and VOIP settings, see [Manage VOIP connections on page 350](#).

To add voice connections see [Adding VOIP to V5.2 voice connections on page 339](#).

To modify or view a voice connection, select the desired connection and click **Modify** or **View**. The Modify/View Subscriber Voice Connections dialog appears. When viewing voice connections the fields appear as read-only..

To display voice statistics, select the desired connection and click **Statistics**. The Voice Statistics dialog appears with data for the selected connection..

Adding VOIP to V5.2 voice connections

This procedure contains steps for manually adding VOIP to V5.2 voice connections.

- 1** Right-click the desired MALC device and select **Manage Voice Connections**. The **Subscriber Voice Connections** dialog box appears.
- 2** Click **VOIP To V5.2** tab. The VOIP to V5.2 voice connection information appears.
- 3** To add a voice connection, click **Add**. The Creating MALC VOIP to V5.2 voice connection screen appears.
- 4** Specify the desired voice connections settings and click **Add** to add the connection.
- 5** Click **Close** to exit the dialog without adding a voice connection.
- 6** Click **Help** to display the help topic for this dialog.

AAL2 to GR303 voice connections (Voice Gateway)

For VoATM traffic, ATM traffic destined for the voice gateway card enters through one of the MALC uplink card's ATM interfaces and is terminated on the voice gateway card. The ATM voice signals are converted to TDM T1/E1 channels and sent to the local TDM switch for processing. For traffic coming from the local switch, the TDM voice signals are converted to VoATM signals by the voice gateway card and sent back out the MALC uplink card to configured ATM destination. See [Manage voice gateway AAL2 subscribers on page 346](#) for more details on voice gateway VPI/VCI configuration.

All uplink cards can be used for connecting VoATM traffic to the voice gateway card.

To add voice connections see [Adding AAL2 to GR303 voice connections on page 340](#).

To modify or view a voice connection, select the desired subscriber in the Manage Subscribers dialog and click **Voice Connection**. The Subscriber Voice Connections dialog appears. When viewing voice connections the fields appear as read-only..

To display voice statistics, select the desired connection and click **Statistics**. The Voice Statistics dialog appears with data for the selected connection..

Adding AAL2 to GR303 voice connections

This procedure contains steps for manually adding AAL2 to GR303 voice connections.

- 1 Right-click the desired MALC device and select **Manage VG Subscribers**. The **Manager Subscriber** dialog box appears.

For configured subscribers:

- Click **Modify** to modify or view the selected subscriber.
- Click **Delete** to remove the selected subscriber.
- Click **Voice Connections** to modify or view the voice connections for the selected subscriber.

- 2 Click **Add** to add voice subscribers. The Template Selection dialog appears.
- 3 Select **BulkAAL2ToGR303** for the desired type of voice connection and click **OK**. The Creating MALC VOIP to GR303 voice connection screen appears.
- 4 Specify the desired voice connections settings. Click **Add** to add the subscriber and voice connection. The subscriber appears in the Manage Subscriber dialog.

Click **Details** to access the Voice Connections Template for the current voice connection.

Click **Close** to exit the dialog without adding a voice connection.

Click **Help** to display the help topic for this dialog.

- 5 To modify or view the voice connections for the current subscriber, in the Manage Subscriber dialog, select the desired subscriber and click **Voice Connections**.

AAL2 to V5.2 voice connections (Voice Gateway)

For VoATM traffic, ATM traffic destined for the voice gateway card enters through one of the MALC uplink card's ATM interfaces and is terminated on the voice gateway card. The ATM voice signals are converted to TDM T1/E1 channels and sent to the local TDM switch for processing. For traffic coming from the local switch, the TDM voice signals are converted to VoATM signals by the voice gateway card and sent back out the MALC uplink card to configured ATM destination. See [Manage voice gateway AAL2 subscribers on page 346](#) for more details on voice gateway VPI/VCI configuration.

All uplink cards can be used for connecting VoATM traffic to the voice gateway card.

To add voice connections see [Adding AAL2 to GR303 voice connections on page 340](#).

To modify or view a voice connection, select the desired connection and click **Modify** or **View**. The Modify/View Subscriber Voice Connections dialog appears. When viewing voice connections the fields appear as read-only..

To display voice statistics, select the desired connection and click **Statistics**. The Voice Statistics dialog appears with data for the selected connection..

Adding AAL2 to V5.2 voice connections

This procedure contains steps for manually adding AAL2 to V5.2 voice connections.

- 1 Right-click the desired MALC device and select **Manage VG Subscribers**. The **Manager Subscriber** dialog box appears.

For configured subscribers:

- Click **Modify** to modify or view the selected subscriber.
- Click **Delete** to remove the selected subscriber.
- Click **Voice Connections** to modify or view the voice connections for the selected subscriber.

- 2 Click **Add** to add voice subscribers. The Template Selection dialog appears.
- 3 Select **BulkAAL2ToV52 (ISDN)** or **BulkAAL2ToV52 (PSTN)** for the desired type of voice connection and click **OK**. The Add a V5.2 Voice Subscriber and Connections screen appears.

- 4 Specify the desired voice connections settings.click **Add** to add the voice connection. The subscriber appears in the Manage Subscriber dialog.
Click **Details** to access the Voice Connections Template for the current voice connection.
Click **Close** to exit the dialog without adding a voice connection.
Click **Help** to display the help topic for this dialog.
- 5 To add, modify or view the voice connections for the current subscriber, in the **Manage Subscriber** dialog, select the desired subscriber and click **Voice Connections**.
The **Subscriber Voice Connections** dialog appears. Click **AAL2 To V5.2** tab.
- 6 To add a voice connections for the current subscriber, click **Add**. The **Creating AAL2 to V5.2 Voice Connections** screen appears.
- 7 Specify the desired voice connection settings and click **Add** to add the connection.
- 8 Click **Close** to exit the dialog without adding a voice connection.
- 9 Click **Help** to display the help topic for this dialog.

AAL2 ELCP to V5.2 voice connections (Voice Gateway)

For VoATM traffic, ATM traffic destined for the voice gateway card enters through one of the MALC uplink card's ATM interfaces and is terminated on the voice gateway card. The ATM voice signals are converted to TDM T1/E1 channels and sent to the local TDM switch for processing. For traffic coming from the local switch, the TDM voice signals are converted to VoATM signals by the voice gateway card and sent back out the MALC uplink card to configured ATM destination. See [Manage voice gateway AAL2 subscribers on page 346](#) for more details on voice gateway VPI/VCI configuration.

All uplink cards can be used for connecting VoATM traffic to the voice gateway card.

To add voice connections see [Adding AAL2 ELCP to V5.2 voice connections on page 342](#).

To modify or view a voice connection, select the desired connection and click **Modify** or **View**. The Modify/View Subscriber Voice Connections dialog appears. When viewing voice connections the fields appear as read-only..

To display voice statistics, select the desired connection and click **Statistics**. The Voice Statistics dialog appears with data for the selected connection..

Adding AAL2 ELCP to V5.2 voice connections

This procedure contains steps for manually adding AAL2 ELCP to V5.2 voice connections.

- 1 Right-click the desired MALC device and select **Manage VG Subscribers**. The **Manager Subscriber** dialog box appears.

For configured subscribers:

- Click **Modify** to modify or view the selected subscriber.
- Click **Delete** to remove the selected subscriber.
- Click **Voice Connections** to modify or view the voice connections for the selected subscriber.

- 2 Click **Add** to add voice subscribers. The Template Selection dialog appears.
- 3 Select **BulkELCPAAL2ToV52 (ISDN)** or **BulkELCPAAL2ToV52 (PSTN)** for the desired type of voice connection and click **OK**. The Adding a V5.2 Voice Subscriber and Connections screen appears.
- 4 Specify the desired voice connections settings. Click **Add** to add the voice connection. The subscriber appears in the Manage Subscriber dialog.

Click **Details** to access the Voice Connections Template for the current voice connection.

Click **Close** to exit the dialog without adding a voice connection.

Click **Help** to display the help topic for this dialog.

- 5 To add, modify or view the voice connections for the current subscriber, in the **Manage Subscriber** dialog, select the desired subscriber and click **Voice Connections**.

The **Subscriber Voice Connections** dialog appears. Click **AAL2 Elcp To V5.2** tab.

- 6 To add a voice connections for the current subscriber, click **Add**. The **Creating AAL2 ELCP to V52 Voice Connections** screen appears.
- 7 Specify the desired voice connection settings and click **Add** to add the connection.
- 8 Click **Close** to exit the dialog without adding a voice connection.
- 9 Click **Help** to display the help topic for this dialog.

EBS to GR303 voice connections

This type of voice connection supports Electronic Business Set (EBS) subscriber connections to a GR-303 voice network.

Prior to configure the EBS to GR303 voice connection, make sure the P-phone card is inserted into the MALC chassis.

To add voice connections:

[Adding EBS to GR303 voice connections on page 344](#)

[Adding EBS to GR-303 voice connections using the wizard on page 344](#)

To modify or view a voice connection, select the desired connection and click **Modify** or **View**. The Modify/View Subscriber Voice Connections dialog appears. When viewing voice connections the fields appear as read-only..

To delete a voice connection, at first change its admin status to **Disabled** in the **Modify Subscriber Voice Connections** dialog box, then highlight the voice connection and click **Delete**.

To display voice statistics, select the desired connection and click **Statistics**. The Voice Statistics dialog appears with data for the selected connection..

Adding EBS to GR303 voice connections

This procedure contains steps for manually adding EBS to GR303 voice connections.

- 1 Right-click the desired MALC device and select **Manage Voice Connections**. The **Subscriber Voice Connections** dialog box appears.
- 2 Click **EBS To GR303** tab. The EBS to GR303 voice connection information appears.
- 3 To add a voice connection, click **Add**. The **Creating MALC EBS to GR303 Voice Connection** screen appears.
- 4 Specify the desired voice connections settings and click **Add** to add the connection.
- 5 Click **Close** to exit the dialog.
- 6 Click **Help** to display the help topic for this dialog.

Adding EBS to GR-303 voice connections using the wizard

To add EBS to GR-303 voice connections to the MALC:

- 7 In the tree view, navigate to the device to which you want to add subscribers.
- 8 Right-click on the device and select **Manage Voice Connections**.
The **Subscribers Voice Connections** dialog box appears. If there are any voice connections configured on the device, they are displayed here.
- 9 Click the **EBS to GR-303** tab.
The information for EBS to GR-303 connections appears in the **Subscribe Voice Connections** dialog.
- 10 Click **Add (Wizard)** button.
The EBS to GR-303 wizard appears.
- 11 Select a template.
To view the template configuration, click **View**.
- 12 Click the next button.
The **Select EBS Ports** dialog box appears.

- 13** From this dialog box select the EBS ports to configure connections on:
 - Enable the voice connection.
 - Select the slot and port for the connection. Note that you can select multiple ports to create multiple connections.
- 14** Click the next button.
The **GR303 CRV Endpoint** dialog box appears.
- 15** Enter the starting CRV index. If you have selected multiple connections, ZMS will create the connections starting with this value.
- 16** Click **Add**.
- 17** When the connections have been added, the confirmation message appears.
Click **OK**.
- 18** The new connections are displayed in the **Subscriber Voice Connections** dialog box.

EBS to VOIP voice connections

This type of voice connection supports EBS subscriber connections to an VOIP voice network. For EBS-to-VOIP configurations, the MALC converts P-phone voice signals into VOIP packets. For VOIP connections, ensure the VOIP systems settings are configured for the desired VOIP network. See [Manage VOIP connections on page 350](#).

To add voice connections

[Adding EBS to VOIP voice connections on page 345](#)

To modify or view a voice connection, select the desired connection and click **Modify** or **View**. The Modify/View Subscriber Voice Connections dialog appears. When viewing voice connections the fields appear as read-only..

To display voice statistics, select the desired connection and click **Statistics**. The Voice Statistics dialog appears with data for the selected connection. .

Adding EBS to VOIP voice connections

This procedure contains steps for manually adding EBS to VOIP voice connections.

- 1** Right-click the desired MALC device and select **Manage Voice Connections**. The **Subscriber Voice Connections** dialog box appears.
- 2** Click **EBS To VOIP** tab. The EBS to VOIP voice connection information appears.
- 3** To add a voice connection, click **Add**. The **Creating MALC EBS to VOIP Voice Connection** screen appears.

- 4 Specify the desired voice connections settings and click **Add** to add the connection. The VOIP endpoint user name is case sensitive and must match the voice switch requirements, for example AAL/1 for Nortel switch MGCP or TP/0001 for Nortel switch Megaco.



Note: The * character is supported in the Directory number.

The Registration server option is available only when PLAR is disabled.

The T.38 fax option enables fax messages to be transported across IP networks between existing G3 fax terminals. The MALC supports T.38 fax service between two MALC devices configured for SIP VoIP and MGCP VoIP. If one side of the T.38 connection is not configured for T.38 support, the fax call reverts to g.711 pass through when this option is configured. Otherwise, the fax may not go through. By default, T.38 fax service is disabled.

- 5 Click **Close** to exit the dialog.
- 6 Click **Help** to display the help topic for this dialog.

Manage voice gateway AAL2 subscribers

The MALC voice gateway card (VG-T1/E1-32-2S) enables voice connections from an ATM and IP voice network to a TDM local exchange switch using GR-303 or V5.2 protocols. The following AAL2 voice connection types are supported using the voice gateway card.

Voice over ATM:

- BLES to GR-303 or V5.2
- ELCP to V5.2

The MALC voice gateway card enables a combination of VP and VC switching for flexible VoATM voice gateway configurations and maximum subscriber support.

- VC-switched

In VC-switching, VCs are switched independently of each other based on VPI and VCI value. The VP range of 0-7 is reserved for VC-switching on the voice gateway card. The VCs in each VC-switched VP must start with 32 and can contain any number up to the maximum number of 448 VCs. The maximum number of VCs that can be allocated to an individual VC-switched VPI is determined by the `zhoneAtmVpiMaxVci` parameter in the `atm-vpi` profile.

- VP-switched

In VP-switching, VCs are switched collectively in groups or Virtual Paths (VPs) based on VPI value. The VP range of 16 to 63 is reserved for VP-switching on the voice gateway card. The VP range of 16 to 63 is reserved for VP-switching on the voice gateway card. Up to 48 VPs can be switched from the NetHorizon uplink card to a voice gateway card. The VCs in each VP-switched VP must start with 32 and can contain any number up to the maximum number of 7,680 VCs. The maximum VCI value that can be allocated to an individual VP-switched VP is determined by the `zhoneAtmMaxVciPerVp` parameter in the atm-vpi profile. For example, if this parameter is set to 1023 for VPI 16, a VC with vpi/vci 16/1024 will not be allowed even if it is the only VC configured on the voice gateway card. The sum of this parameter in all VP-switched atm-vpi profiles on the voice gateway card cannot exceed 7680.

To add subscribers for AAL2 voice connections, see [Adding voice gateway AAL2 subscribers on page 347](#). Voice connections can be after creating subscribers by clicking the Voice Connections button.

After subscribers for AAL2 voice connections have been added, voice connections can also be created from the Subscriber Voice Connections dialog. Right-click the desired MALC device and select **Manage Voice Connections**. The **Subscriber Voice Connections** dialog box appears.

[Adding AAL2 to GR303 voice connections on page 340](#)

[Adding AAL2 to V5.2 voice connections on page 341](#)

[Adding AAL2 ELCP to V5.2 voice connections on page 342](#)

Adding voice gateway AAL2 subscribers

Voice gateway AAL2 subscriber provisioning is a process of creating ATM logical connections, determining voice or data communication physical requirements, and then assigning subscribers to those pre-defined voice or data connections.

To assign subscribers to voice ports:

- 1 Add an ATM traffic descriptor to a device that has already been added to ZMS. See [Creating ATM traffic descriptor configuration templates on page 361](#).
- 2 Add an ATM AAL2 VCL. See [Creating an ATM AAL2 VCL on page 349](#).
- 3 Next, assign a subscriber to the port using that VCL.
 - a In the tree view, navigate to the device to which you want to add subscribers.
 - b Right-click on the device and select **Manage VG Subscribers**. The **Manage Subscribers** dialog appears.
 - c Click **Add** to add a port.
The **Selection** dialog box appears.

- d** Select a template and click **Add**.

These templates are either standard templates or user-defined templates. See [Voice configuration templates](#).

Depending on the type of AAL2 voice connection template selected, the **Add a V52 Voice Subscriber and Connections** dialog box or the **Add a GR-303 Voice Subscriber and Connections** appears.

To view the settings for the template, click the **Details** button.

- 4** In the **Subscriber Information** area, select the AAL2 interface for the subscriber by clicking the browse button, navigating to an interface on the device and clicking **OK**.

- 5** Enter the subscriber contact information.

If you are just creating the subscriber Select **Create the Subscriber Only** and proceed to [Step 7](#).

- 6** Configure the endpoint connections:

To configure a V52 voice connection:

- a** In the **Voice Connection Information** area, specify whether you want to enter:

CID range and starting user port address

User port address range and starting CID index

- b** In the **AAL2 Endpoint** area, specify:

- VPI/VCI
- Starting CID or the CID range
- Browse for an ATM traffic descriptor.

If an appropriate traffic descriptor does not exist, highlight Traffic Descriptor Templates in the selection dialog box and click **Add**.

- c** In the **V52 User Endpoint** area, specify:

- V52 interface group name
- Starting address or the address range

To configure a GR-303 voice connection:

- a** In the **Voice Connection Information** area, specify whether you want to enter:

CID range and starting user port address

User port address range and starting CID index

- b** In the **AAL2 Endpoint** area, specify:

- VPI/VCI

- Starting CID or the CID range
- Browse for an ATM traffic descriptor.

If an appropriate traffic descriptor does not exist, highlight Traffic Descriptor Templates in the selection dialog box and click **Add**.

c In the **V52 User Endpoint** area, specify:

- V52 interface group name
- Starting address or the address range

7 When finished, click **Add**, then **Close**.

8 Activate the voice connection by setting the admin status to **Enable**.

Related topics:

[Adding POTS to AAL2 voice connections using the wizard \(MALC\) on page 318](#)

Creating an ATM AAL2 VCL

1 Navigate to the port you want to create an ATM VCL on.

2 Right-click **ATM VCL Endpoints** and select **Add**.

If there is more than one type of VCL endpoint supported on the port, the Selection dialog box appears.

3 Select the type of endpoint and click **OK**.

Depending on the type of the template selected, a dialog box for configuring AAL2 endpoints appears.

4 In the **Add ATM AAL2 VCL Endpoint Configuration** dialog box, specify:

VPI/VCI: The VPI/VCI for the interface.

Application ID: Select POTS or ISDN, as appropriate.

Transmit Traffic Descriptor and **Receive Traffic Descriptor:** Select a traffic descriptor. The transmit and receive traffic descriptors must be the same.

Refer to the online help for details on the configuration settings.

5 Click **Add**, then **Close**.

[Adding ATM cross connect on MALC, and Raptor using the wizard](#)

[Adding ATM cross connect on MALC, and Raptor \(advanced mode\)](#)

[Adding an ATM cross connect \(VP switched connection\)](#)

[Changing VCL rates](#)

[Creating ATM cross connect configuration templates](#)

[Creating ATM traffic descriptor configuration templates](#)

[Creating an ATM VCL for data](#)

- [Creating an ATM VPL](#)
- [Creating an ATM VPI profile](#)
- [Finding ATM VCLs and cross connects](#)
- [Pinging ATM VCL endpoints](#)

Manage VOIP connections

POTS to VOIP connections convert POTS subscriber voice signals into IP packets and use IP servers to transport the packets through the VOIP system.

The VOIP system protocol setting can be configured as either Media Gateway Control Protocol (MGCP) or Session Initiation Protocol (SIP) signaling. MGCP signaling establishes call control elements or call agents to handle call control. MGCP devices execute the commands sent by the call agents. SIP signaling identifies callers and callees by SIP addresses and allows signals to be redirected to proxy servers. By default, the NetHorizon uses SIP signaling.

- [Configuring VOIP system parameters](#)
- [Configuring VOIP server parameters](#)
- [Configuring malicious caller lists](#)
- [Configuring hunt groups](#)
- [Configuring SIP dial plans](#)
- [Configuring voicegateway](#)
- [Configuring ISDN signaling profiles](#)
- [Configuring ESA voice connections](#)

Configuring VOIP system parameters

- 1 Right-click a device and select **Manage VoIP**.
The **VoIP Configuration Manager** dialog box appears.
- 2 Click **Voice System** tab.
- 3 Specify the desired VoIP system parameters:
VoIP System Configuration
 - Hookflash Minimum Timer
 - Hookflash Maximum Timer
 - Pulse Interdigit Timeout
 - Minimum Make Pulse Width
 - Minimum Break Pulse Width
 - Maximum Break Pulse Width

- 4 Click **Refresh** to update the displayed settings.

Click **Modify** to apply setting changes.

Click **Close** to exit the dialog.

Click **Help** to access the related help topic.

For details on the settings in this dialog box, refer to the online help.

Configuring VOIP server parameters

- 1 Click the **VoIP Server** tab to display the VOIP server settings.

- 2 Click **Add** to add new VOIP server. The **Add VoIP Server** dialog box appears.

Specify the following VOIP server settings:

- Registration Server Name
- Server Index
- Server Address
- Address Type
- UDP Port Number
2944 for Megaco. 2472 for MGCP. 5060 for SIP.
- Server Type
- Protocol
- Send Call Processing Tone
- RTCP Enabled
- RTCP Packet Interval
- Interdigit Timeout
- IP Type of Service
- Domain Name
- Signaling DSCP
Add DSCP marking for SIP packets.
- RTP DSCP
Add DSCP marking for RTP packets.

- 3 Click **Session & Expires Configuration** to change the current VoIP server SIP timer settings. The Add VoIP Server dialog box appears with SIP timer settings.

Specify the following SIP timer configuration settings:

- Invite
- Register

- Header Invite
- Header Register
- Session Timer
- Session Expiration
- Session Min Session Expiration
- Caller Request Timer
- Callee Request Timer
- Caller Specify Refresher
- Callee Specify Refresher

4 Click **Reset Defaults** to return the displayed settings to default values.

Click **Add** to add VoIP server with the current settings. Up to two MGCP servers can be added for redundant support.

Click **Close** to exit the dialog.

Click **Help** to access the related help topic.

5 Click **Modify** to change the current VoIP server configuration or SIP timer settings. The Modify VoIP Server dialog box appears.

Specify the following VOIP server configuration settings:

- Registration Server Name
- Server Index
- Server Address
- Address Type
- UDP Port Number
2944 for Megaco. 2472 for MGCP. 5060 for SIP.
- Server Type
- Protocol
- Send Call Processing Tone
- RTCP Enabled
- RTCP Packet Interval
- Interdigit Timeout
- IP Type of Service
- Domain Name

6 Click **Session & Expires Configuration** to change the current VoIP server SIP timer settings. The Modify VoIP Server dialog box appears with SIP timer settings.

Specify the following SIP timer configuration settings:

- Invite
- Register
- Header Invite
- Header Register
- Session Timer
- Session Expiration
- Session Min Session Expiration
- Caller Request Timer
- Callee Request Timer
- Caller Specify Refresher
- Callee Specify Refresher

7 Click **Reset Defaults** to return the displayed settings to default values.

Click **Modify** to apply the VoIP server setting changes.

Click **Close** to exit the dialog.

Click **Help** to access the related help topic.

For details on the settings in this dialog box, refer to the online help.

Related topics:

[Adding IP interfaces on page 391](#)

Configuring malicious caller lists

1 Click the **Malicious Caller List** tab to display the Malicious Caller List settings.

2 Click **Add** to add new malicious caller list. The Add Malicious Caller List dialog box appears.

Specify the following VOIP server settings:

- URI
- Status

3 Click **Reset Defaults** to return the displayed settings to default values.

Click **Add** to add a malicious caller list with the current settings.

Click **Close** to exit the dialog.

Click **Help** to access the related help topic.

- 4 Click **Modify** to change the current malicious caller settings. The Modify Modify Malicious Caller dialog box appears.



Note: To view malicious caller settings, click the **View** button. the malicious caller settings appear as read-only values.

Specify the following malicious caller list settings:

- URI
- Status

- 5 Click **Reset Defaults** to return the displayed settings to default values.
Click **Modify** to apply the caller setting changes.
Click **Close** to exit the dialog.
Click **Help** to access the related help topic.

For details on the settings in this dialog box, refer to the online help.

Related topics:

[Adding IP interfaces on page 391](#)

Configuring hunt groups

- 1 Click the **Hunt Groups** tab to display the Hunt Group settings.
- 2 Click **Add** to add a new hunt group. The Creating Hunt Group dialog box appears.

Specify the following hunt group settings:

- IP Interface
- User Id
- Directory Number
- Preferred Codec
- G711 Fallback
- Frames Per Packet
- G726 Byte Order
- Password
- Subscriber PLAR
- Address Type

- Address
 - UDP Port Number
2944 for Megaco. 2472 for MGCP. 5060 for SIP.
 - Admin Status
 - Registration Server
- 3** Click **Add** to add a malicious caller list with the current settings.
Click **Close** to exit the dialog.
Click **Help** to access the related help topic.
 - 4** Click **Modify** to change the current hunt group settings. The Modify Hunt Group dialog box appears.



Note: To view hunt group settings, click the **View** button. the same settings appear as read-only values.

Modify the desired settings:

- 5** Click **Reset Defaults** to return the displayed settings to default values.
Click **Modify** to apply the caller setting changes.
Click **Close** to exit the dialog.
Click **Help** to access the related help topic.

For details on the settings in this dialog box, refer to the online help.

Related topics:

[Adding IP interfaces on page 391](#)

Configuring SIP dial plans

- 1** In the VOIP Configuration Manager screen, click the **SIP Dial Plan** tab to display the SIP dial plan settings.
- 2** Click **Add** to add a SIP dial plan. The Add SIP Dial Plan dialog box appears.

Specify the following SIP dial plan settings:

- Match String
- SIP IP Address
- Destination Name
- Number of Digits
- Prefix Strip
- Prefix Add

- Dial Plan Type (Normal, Call Park, ESA)

For ESA cluster support, create an ESA dialplan for each of the MALC devices participating in the ESA cluster. For each dialplan, enter the IP addresses of the desired MALC in the **sip-ip-address** field and change the **dialplan-type** to **esa**.

- Inter-digit Timeout
- Registration Server Index
- Dial Plan Class (Emergency)

Use this field to enable or disable the Enhanced SIP911 service.

When the Enhanced SIP 911 service has been enabled, there will be indication on the MXK that if there is a emergency call (e.g. 911) in progress, the system will not allow itself to be upgraded/rebooted.

- Dial Plan Description

Brief description about the sip-dialplan.

- 3 Click **Reset Defaults** to restore the default settings.

Click **Add** to add a SIP dial plan with the current settings.

Click **Close** to exit the dialog.

Click **Help** to access the related help topic.

- 4 Click **Modify** to change the current SIP dial plan settings. The Modify SIP Dial Plan dialog box appears.



Note: To view dial plan settings, click the **View** button. the dial plan settings appear as read-only values.

Modify the desired settings:

- 5 Click **Reset Defaults** to return the displayed settings to default values.

Click **Modify** to apply the caller setting changes.

Click **Close** to exit the dialog.

Click **Help** to access the related help topic.

For details on the settings in this dialog box, refer to the online help.

Related topics:

[Adding IP interfaces on page 391](#)

Configuring voicegateway

For VOIP to TDM connections on the voice gateway card, VOIP packets destined for the voice gateway card enter through one of the NetHorizon

uplink card interfaces (GigE, SONET, IP) and are terminated on the voice gateway card. The voice signal is converted to TDM T1/E1 channels and sent to the local switch for TDM voice processing. For traffic coming from the local switch, the TDM voice signals are converted to VOIP packets by the voice gateway card and routed back out the NetHorizon uplink card to the configured VOIP destination.



Note: Only one IP interface can be configured on the voice gateway card.

All the ATM/IP uplink cards including Uplink-GIGE/OC-12-HP and Uplink-RprGigE cards can be used for connecting VOIP traffic to the voice gateway card.

- 1 Click the **Voice Gateway** tab to display the voice gateway settings.
- 2 Click **Add** to add a voice gateway as an IP host. The Add SIP Dial Plan dialog box appears.

Specify the following voice gateway settings:

- Address

The IP address of the voice gateway.

- Traffic Descriptor

The traffic descriptor associated with the VOIP traffic using this voice gateway. The connection uses traffic descriptor 1 and an AAL5 physical interface of aal5proxy. Click the browse button, to use a template to create the traffic descriptor.

- 3 Click **Reset Defaults** to restore the default settings.

Click **Add** to add the voice gateway with the current settings.

Click **Close** to exit the dialog.

Click **Help** to access the related help topic.

For details on the settings in this dialog box, refer to the online help.

Related topics:

[Adding IP interfaces on page 391](#)

Configuring ISDN signaling profiles

An ISDN signaling profile is used to specify the type of ISDN signaling used between the MALC and a PBX switch. Each ISDN signaling profile record contains the setting for the switch type. A unique ISDN signaling profile should be configured for each voicegateway card in the MALC.

The ISDN signaling profile is specified in **Creating ISDN Signaling to VOIP Voice Connection** dialog map the PRI's on the PBX to a the

voicegateway card. The **ds1-group-number** field in the **ds1-profile** record corresponds to the ISDN signaling profile record.

- 1** Click the **Isdn Signaling Profile** tab to display the ISDN signaling profile records.
- 2** Click **Add** to add a ISDN signaling profile record. The Add ISDN Signaling dialog box appears.

Select a switch type from the Protocol drop-down menu:

- SwissNet-3
- SwissNet-2
- Q.SIG
- TS014
- TS013
- CORNET
- 1TR6 (BRI, PRI)
- NTT INS1500
- NTT INS64
- KDD
- VN6
- VN4
- VN3
- VN2
- Next One
- ISDN 2 (BRI, PRI)
- ISDN 1 (BRI)
- NT DMS250
- NT DMS100
- AT&T 5ESS
- AT&T 4ESS
- DASS2
- ETSI
- DSS1

- 3** Click **Reset Defaults** to restore the default settings.
Click **Add** to add the ISDN signaling profile record.

Click **Close** to exit the dialog.

Click **Help** to access the related help topic.

For details on the settings in this dialog box, refer to the online help.

Related topics:

[ISDN SIG to VOIP voice connections on page 335](#)

Configuring ESA voice connections

For VOIP SIP or SIP PLAR and POTS to GR303 or V5.2 voice connections, the MALC provides emergency calling services during network or equipment failures that cause a loss of connection to the configured SIP server.

The ESA feature enables numbers configured within the same dialplan using the same shelf to communicate with any residences or businesses sharing that dialplan. Incoming calls from outside the ESA group and outgoing calls to numbers outside the SIP dialplan receive a fast-busy signal.

When ESA is activated, call features, such as call waiting, are not supported.



Note: After a loss of connection to the SIP server, there may be a delay up to 5 minutes before ESA notification is received and ESA features are accessible.

There maybe a similar delay before resuming normal calling after the outage is restored.

To configure ESA for VOIP connections within the same MALC, configure a VOIP server, create an ESA dialplan with the MALC IP address as the SIP IP address. Also, change the dialplan type to esa.

To configure ESA for VOIP connections for 911 calls, create an ESA dialplan with a match-string of 911 and the IP address of the MALC shelf in the SIP IP address. Also, change the number of digits and prefix-strip to 3. The prefix-strip setting deletes the dialed 911 numbers. Enter the desired phone number to be called in the prefix-add field. This number must be a valid voicefxs line in the same MALC shelf. Change the dial plan type to esa.

For POTS to GR303 voice connections, the MALC enables a VOIP endpoint for emergency calling services during network or equipment failures that cause a loss of connection to a configured SIP server.

The ESA feature enables numbers configured within the same ESA dialplan using the same MALC shelf to communicate with any residences or businesses sharing that dialplan. Incoming calls from outside the ESA group and outgoing calls to numbers outside the SIP dialplan receive a fast-busy signal.

- 1 Right-click the MALC and select **Voice Connections** to display the Subscriber Voice Connections dialog.
- 2 Click **POTS to GR303 ESA** tab and click the **Add** button to add an ESA voice connection.

The **Creating MALC POTS to GR303 with ESA Voice Connections** dialog box appears.

Specify the following ESA voice connection settings:

- Voice Connection Admin Status
- POTS port
- GR-303 interface group
- Starting CRV index number
- Signal Type
- Local Admin State
- Starting Directory Number
- Registration server

3 Click **Add** to add the voice gateway with the current settings.

Click **Close** to exit the dialog.

Click **Help** to access the related help topic.

4 To view ESA connection data, in the Subscriber Voice Connections dialog, select the desired ESA connection and click **Modify** button.

The **Modifying Subscriber Voice Connections** dialog box appears.

5 Click the ESA tab to display the ESA options. These options are read-only.

6 To modify the ESA settings, delete the ESA connection and re-add it.

7 Click **Close** to exit the dialog.

Click **Help** to access the related help topic.

To verify whether ESA support is in-use, enter the **voice status** command. This command lists the voice port, destination, call state, and ESA state along with other status information.

For details on the settings in this dialog box, refer to the online help.

Related topics:

[Adding POTS to GR-303 ESA voice connections using the wizard on page 332](#)

Data configuration

Topics:

[Data templates](#)

[Adding an ATM cross connect](#)

[Adding ATM cross connect on MALC, and Raptor using the wizard](#)

[Adding ATM cross connect on MALC, and Raptor \(advanced mode\)](#)
[Adding an ATM cross connect \(VP switched connection\)](#)
[Creating an ATM VCL for data](#)
[Creating an ATM VPL](#)
[Adding an ATM cross connect \(CES\)](#)
[Adding an ATM Circuit Emulation Service \(CES\) cross connect using the wizard](#)
[Modifying CES](#)
[Optical cross connection \(GigaMux only\)](#)

Data templates

Topics:

[Creating ATM traffic descriptor configuration templates](#)
[Creating ATM cross connect configuration templates](#)

Creating ATM traffic descriptor configuration templates

To create a template for ATM traffic descriptors:

- 1 Select **Tools > Configure Templates**.
The **Template Configuration** dialog box appears.
- 2 Right click **Traffic Descriptor Templates** and select **Add**.
The **Add ATM Traffic Descriptor Configuration** dialog box appears.
- 3 Enter a name and a description for this template.
The name appears in the selection dialog boxes.
- 4 Enter the parameters for the traffic descriptor. Depending on the **Service Category** and **Traffic Type**, different settings are allowed. Keep in mind that templates may only apply to specific device types, depending in the setting selected.
For details on the settings, see the online help.
- 5 After finishing the configuration, click **Add**.
After adding the template, it will appear in the **Template Configuration** dialog box.
- 6 You can continue to add traffic descriptor templates by modifying the settings, then clicking **Add**.
- 7 When finished, click **Close**.

Related topics:

[Adding ATM cross connect on MALC, and Raptor using the wizard on page 364](#)

[Adding ATM cross connect on MALC, and Raptor \(advanced mode\) on page 366](#)

[Adding an ATM cross connect \(VP switched connection\) on page 369](#)

[Changing VCL rates on page 141](#)

[Creating ATM cross connect configuration templates on page 362](#)

[Creating ATM traffic descriptor configuration templates on page 361](#)

[Creating an ATM VCL for data on page 372](#)

[Creating an ATM VPL on page 373](#)

[Creating an ATM VPI profile on page 143](#)

[Finding ATM VCLs and cross connects on page 461](#)

Creating ATM cross connect configuration templates

To create a template for ATM cross connects:

- 1 Select **Tools > Configure Templates**.

The **Template Configuration** dialog box appears.

- 2 Right click **Cross Connect Templates** and select **Add**.

The **Streamline Add ATM Cross Connects** dialog box appears.

- 3 Enter a name and a description for this template.

The name appears in the selection dialog boxes.

- 4 Enable the cross connect.

- 5 Specify whether you want to:

- Automatically create the VCL endpoints.

If you automatically create the endpoints, you can configure all the settings for the cross connect templates in this dialog box.

- Use existing ATM endpoints.

If you use existing endpoints, the endpoints must already exist.

- 6 For the upstream VCL specify:

- Select **Auto Increment VPI If Necessary** if you want NetHorizon to continue to provision cross connects using a particular VPI until all the VCIs are provisioned. NetHorizon will then start creating cross connects on the next available VPI.
- Select **Auto Select Available VCI** for NetHorizon to automatically use the next available VCI values for the cross connect.
- Select **Manually Select Starting VCI** to indicate the VCI you want NetHorizon to use in the cross connect. As you add cross connects, NetHorizon increments the VCI value.

- Specify the traffic descriptor to use.
- 7** For the downstream VCL specify the VPI/VCI.
- 8** After finishing the configuration, click **Add**.
After adding the template, it will appear in the **Template Configuration** dialog box.
- 9** You can continue to add cross connect templates by modifying the settings, then clicking **Add**.
- 10** When finished, click **Close**.

Related topics:

[Adding ATM cross connect on MALC, and Raptor using the wizard on page 364](#)

[Adding ATM cross connect on MALC, and Raptor \(advanced mode\) on page 366](#)

[Adding an ATM cross connect \(VP switched connection\) on page 369](#)

[Changing VCL rates on page 141](#)

[Creating ATM cross connect configuration templates on page 362](#)

[Creating ATM traffic descriptor configuration templates on page 361](#)

[Creating an ATM VCL for data on page 372](#)

[Creating an ATM VPL on page 373](#)

[Creating an ATM VPI profile on page 143](#)

[Finding ATM VCLs and cross connects on page 461](#)

Adding an ATM cross connect

This section describes the basics of how to use NetHorizon to configure ATM cross connects on your device.

Topics:

[Adding ATM cross connect on MALC, and Raptor using the wizard](#)

[Adding ATM cross connect on MALC, and Raptor \(advanced mode\)](#)

[Adding an ATM cross connect \(VP switched connection\)](#)

[Modifying an ATM cross connection traffic descriptor](#)

[Deleting an ATM cross connect](#)

[Adding an ATM cross connect \(CES\)](#)

[Adding an ATM Circuit Emulation Service \(CES\) cross connect using the wizard](#)

Adding ATM cross connect on MALC, and Raptor using the wizard

When you add an ATM cross connect (VC switched), you can either:

- Specify existing upstream and downstream VCLs in the ATM VCL cross connection. This option requires that the **Admin Status** of the existing upstream and downstream VCLs be set to **Up** before you add the ATM VCL cross connection.
- Request that ZMS automatically create the upstream and downstream VCLs in the ATM VCL cross connection. With this option, ZMS automatically sets the **Admin Status** of the upstream and downstream VCLs to **Up**.

To add a VC switched data connection:

- 1 Right-click a device and select **Manage ATM Connections**.

The **Configure ATM Cross Connects** dialog box appears. If there are any cross connects configured on the system, they are displayed.

- 2 Select the **VC Cross Connects** tab (selected by default).
- 3 Click **Add (Wizard)** to add the cross connect using the wizard.

The wizard dialog box appears.

- 4 Select a template.

To view the template configuration, click **View**.

- 5 Click the next button.

The **Administrative Options** dialog box appears.

- 6 From this dialog box you can specify basic ATM parameters:

- (Optional). Enter a name for the cross connect.
- Verify that the cross connect is enabled (this is the default).
- Decide whether you want to automatically create the VCL endpoints or use existing VCLs.

Select **Auto Create the Upstream/Downstream VCLs** if you want NetHorizon to automatically create the endpoints.

Select **Use Existing Upstream/Downstream VCLs** if you want NetHorizon to use existing endpoints. If you choose this option, the endpoints must already exist.

- 7 Click the next button.

The **Trunk Side Configuration** dialog box appears.

- 8 From this dialog box you configure the ATM trunk side interface.

For automatically created VCLs:

- Click the Browse button and select the trunk physical interface for the cross connect.

- Select the VPI.
- Select **Auto Increment VPI If Necessary** if you want NetHorizon to continue to provision cross connects using a particular VPI until all the VCIs are provisioned. NetHorizon will then start creating cross connects on the next available VPI.
- Select **Auto Select Available VCI** for NetHorizon to automatically use the next available VCI values for the cross connect.
- Select **Manually Select Starting VCI** to indicate the starting VCI you want to use in the cross connect. ZMS will automatically select the next available trunk side VCI to use if you are creating more than one cross connect.
- Click the Browse button and select the traffic descriptor template to use.

For existing VCLs:

Click the Browse button and select the trunk VCL for the cross connect.

- 9 When finished with the trunk side configuration, click the next button.

The **Traffic Descriptor Configuration** dialog box appears. From this dialog box you specify the ATM traffic descriptors to use for the cross connect. (This option is not available if the auto-create option on the **Admin** screen was selected.)

- 10 Specify whether you want to use traffic descriptor templates or existing traffic descriptors, then click the browse button to select the traffic descriptor.
- 11 Click the next button.

The **Line Side Configuration** dialog box appears.

- 12 From this dialog box you configure the ATM line side interface.

For automatically created VCLs:

- Specify the VPI/VCI to be used for all line side VCLs. The ATM VCL profiles and existing VCLs will determine which ports are available. For specific VPI/VCI combinations, the ports will automatically be enabled or disabled when the **Check Availability** button is clicked.

Click the **Check Availability** button every time you change the VPI or VCI in order to ensure that the selected ports are still available.

- Select the slot and port for the cross connect. Note that you can select multiple ports to create multiple cross connects.

For existing VCLs:

Click the Browse button and select the line side interface VCL for the cross connect.

- 13 Click the next button.

14 Click Add.

NetHorizon begins creating the cross connect and displays a status window describing the progress.

After the connection has been successfully added, NetHorizon displays a confirmation dialog box.

15 Click OK to close the confirmation dialog box.

16 Click Close.

NetHorizon displays the new cross connect in the **Configure ATM Cross Connects** dialog box. If you need to modify, view or delete the connection, you can do it from this dialog box.

Related topics:

[Adding an ATM cross connect \(VP switched connection\) on page 369](#)

[Changing VCL rates on page 141](#)

[Creating ATM cross connect configuration templates on page 362](#)

[Adding ATM cross connect on MALC, and Raptor \(advanced mode\) on page 366](#)

[Creating ATM traffic descriptor configuration templates on page 361](#)

[Creating an ATM VCL for data on page 372](#)

[Creating an ATM VPL on page 373](#)

[Creating an ATM VPI profile on page 143](#)

[Deleting an ATM cross connect on page 371](#)

[Finding ATM VCLs and cross connects on page 461](#)

[Modifying a card's ATM bandwidth settings on page 144](#)

Adding ATM cross connect on MALC, and Raptor (advanced mode)

When you add an ATM cross connect (VC-switched), you can either:

- Specify existing upstream and downstream VCLs in the ATM VCL cross connection. This option requires that the **Admin Status** of the existing upstream and downstream VCLs be set to **Up** before you add the ATM VCL cross connection.
- Request that ZMS automatically create the upstream and downstream VCLs in the ATM VCL cross connection. With this option, ZMS automatically sets the **Admin Status** of the upstream and downstream VCLs to **Up**.
- Add DS3 fanout cross connections.

To add a VC switched data connection:

- 1** Right-click a device and select **Manage ATM Connections**.

The **Configure ATM Cross Connects** dialog box appears. If there are any cross connects configured on the system, they are displayed.

- 2 Select the **VC Cross Connects** tab (selected by default).

For DS3 Fanout cross connections, click the DS3 Fanout tab.

- 3 Click **Add** (to add the cross connect using advanced mode)

The **Creating Cross Connects** dialog box appears.

For DS3 Fanouts, the Creating DS3 Fanout Cross Connections dialog box appears.

- 4 Select a template for this cross connect.

- 5 In the **Administrative Information** area, specify:

- (Optional). Enter a name for the cross connect.
- Verify that the cross connect is enabled (this is the default).

Decide whether you want to automatically create the VCL endpoints or use existing VCLs.

- Select **Auto Create the Upstream/Downstream VCLs** if you want NetHorizon to automatically create the endpoints.
- Select **Use Existing Upstream/Downstream VCLs** if you want NetHorizon to use existing endpoints. If you choose this option, the endpoints must already exist.

- 6 Configure or select the upstream interface or trunk side for DS3 fanouts:

For auto-created VCLs, in the **Select Physical for Upstream VCL** area:

- Click the Browse button and select the trunk physical interface for the cross connect.
- Select the VPI.
- Select **Auto Increment VPI If Necessary** if you want NetHorizon to continue to provision cross connects using a particular VPI until all the VCIs are provisioned. NetHorizon will then start creating cross connects on the next available VPI.
- Select **Auto Select Available VCI** for NetHorizon to automatically use the next available VCI values for the cross connect.
- Select **Manually Select Starting VCI** to indicate the starting VCI you want to use in the cross connect. ZMS will automatically select the next available trunk side VCI to use if you are creating more than one cross connect.

For existing VCLs, in the **Select Upstream VCL** area:

Click the Browse button and select the existing upstream VCL to use.

- 7 (For auto-created VCLs only) In the **Transmit and Receive Traffic Descriptor** area, specify whether you want to use traffic descriptor templates or existing traffic descriptors, then click the browse button to select the traffic descriptor.
- 8 Configure or select the downstream interface or line side for DS3 fanouts:
For automatically created VCLs, in the **Select Physical for Downstream VCL** area:
 - Specify the VPI/VCI to be used for all line side VCLs. The ATM VCL profiles and existing VCLs will determine which ports are available. For specific VPI/VCI combinations, the ports will automatically be enabled or disabled when the **Check Availability** button is clicked.
Click the **Check Availability** button every time you change the VPI or VCI in order to ensure that the selected ports are still available.
 - Select the slot and port for the cross connect. Note that you can select multiple ports to create multiple cross connects.For existing VCLs, in the **Select Downstream VCL** area:
Click the Browse button and select the existing downstream VCL to use.
- 9 Click **Add**.
After the connection has been successfully added, NetHorizon display a confirmation dialog box.
- 10 Click **OK** to close the confirmation dialog box.
- 11 Click **Close**.
NetHorizon displays the new cross connect in the **Configure ATM Cross Connects** dialog box. If you need to modify, view or delete the connection, you can do it from this dialog box.

Related topics:

[Adding an ATM cross connect \(VP switched connection\) on page 369](#)

[Changing VCL rates on page 141](#)

[Creating ATM cross connect configuration templates on page 362](#)

[Adding ATM cross connect on MALC, and Raptor using the wizard on page 364](#)

[Creating ATM traffic descriptor configuration templates on page 361](#)

[Creating an ATM VCL for data on page 372](#)

[Creating an ATM VPI profile on page 143](#)

[Creating an ATM VPL on page 373](#)

[Deleting an ATM cross connect on page 371](#)

[Finding ATM VCLs and cross connects on page 461](#)

[Modifying a card's ATM bandwidth settings on page 144](#)

Adding an ATM cross connect (VP switched connection)

In VP switching, cells are switched based on the VPI only. The VCI remains the same on both the incoming and outgoing interfaces.

Configuring VP switched connections is similar to VC switched connections, except:

- An **ATM VPI Profile** must be created for each switched VP. This profile specifies whether the interface is VP or VC switched and the number of VCs on the VP. For more information, see [Creating an ATM VPI profile on page 143](#).
- **ATM VPL Endpoints** specify the characteristics of each end of the connection. Each interface is assigned an ATM VPL, and cross connects join the two ATM VPLS.

To add a VP switched data connection:

- 1 Right-click a device and select **Manage ATM Connections**.

The **Configure ATM Cross Connects** dialog box appears. If there are any cross connects configured on the system, they are displayed.

- 2 Select the **VP Cross Connects** tab.

- 3 Click **Add**.

The **Quick Add ATM VP Cross Connects** dialog box appears.

- 4 From this dialog box you create the VP switched cross connect:

- (Optional). Enter a name for the cross connect.
- Decide whether you want to automatically create the VPL endpoints or use existing VPLs.

Select **Auto Create the Upstream/Downstream VPLs** if you want NetHorizon to automatically create the endpoints. Continue to [Step 5](#).

Select **Use Existing Upstream/Downstream VPLs** if you want NetHorizon to use existing endpoints. If you choose this option, the endpoints must already exist. Continue to [Step 6](#).

- 5 For automatically created VPLs:
 - Click the Browse button and select an existing traffic descriptor to use.
 - Click the Browse button and select the upstream physical interface for the cross connect.
 - Specify the upstream VPI.
 - Click the Browse button and select the downstream physical interface for the cross connect.

- Specify the downstream VPI
- 6 For existing VPLs:
 - Click the Browse button and select the upstream VPL for the cross connect.
 - Click the Browse button and select the downstream VPL for the cross connect.
 - 7 When finished with the ATM configuration, click **Add**.

NetHorizon begins creating the cross connect and displays a status window describing the progress.

After the connection has been successfully added, NetHorizon display a confirmation dialog box.
 - 8 Click **OK** to close the confirmation dialog box.
 - 9 Click **Close**.

NetHorizon displays the new cross connect in the **Configure ATM Cross Connects** dialog box. If you need to modify, view or delete the connection, you can do it from this dialog box.

Related topics:

[Adding ATM cross connect on MALC, and Raptor using the wizard on page 364](#)

[Adding ATM cross connect on MALC, and Raptor \(advanced mode\) on page 366](#)

[Changing VCL rates on page 141](#)

[Creating ATM cross connect configuration templates on page 362](#)

[Creating ATM traffic descriptor configuration templates on page 361](#)

[Creating an ATM VCL for data on page 372](#)

[Creating an ATM VPL on page 373](#)

[Creating an ATM VPI profile on page 143](#)

[Deleting an ATM cross connect on page 371](#)

[Finding ATM VCLs and cross connects on page 461](#)

[Modifying a card's ATM bandwidth settings on page 144](#)

Modifying an ATM cross connection traffic descriptor

Use these procedures to modify a traffic descriptor in an existing cross connection.



Note: Modifying a traffic descriptor in an existing VCL interrupts traffic on that VCL. Perform this procedure during a maintenance window.

To modify a traffic descriptor in an existing cross connection:

- 1** Right-click a device and select **Manage ATM Connections**.
The **Configure ATM Cross Connects** dialog box appears.
- 2** Highlight a cross connect and click **Modify VCL TD**.
The **Modify Cross Connection Traffic Descriptors** dialog box appears.
- 3** Select the transmit traffic descriptor to modify by clicking on the browse button.
- 4** Select the receive traffic descriptor to modify by clicking on the browse button.
- 5** Click **Modify**. A prompt appears: “Traffic at the selected Cross Connections will be interrupted. Do you want to continue?”
- 6** Click **Yes**.

Related topics:

[Adding an ATM cross connect \(VP switched connection\) on page 369](#)

[Changing VCL rates on page 141](#)

[Creating ATM cross connect configuration templates on page 362](#)

[Adding ATM cross connect on MALC, and Raptor using the wizard on page 364](#)

[Creating ATM traffic descriptor configuration templates on page 361](#)

[Creating an ATM VCL for data on page 372](#)

[Creating an ATM VPI profile on page 143](#)

[Creating an ATM VPL on page 373](#)

[Finding ATM VCLs and cross connects on page 461](#)

[Modifying a card's ATM bandwidth settings on page 144](#)

Deleting an ATM cross connect

To delete a cross connect:

- 1** Right-click a device and select **Manage ATM Connections**.
The **Configure ATM Cross Connects** dialog box appears.
- 2** Highlight a cross connect and click **Delete**.

Related topics:

[Adding an ATM cross connect \(VP switched connection\) on page 369](#)

[Changing VCL rates on page 141](#)

[Creating ATM cross connect configuration templates on page 362](#)

[Adding ATM cross connect on MALC, and Raptor using the wizard on page 364](#)

[Creating ATM traffic descriptor configuration templates on page 361](#)

[Creating an ATM VCL for data on page 372](#)

[Creating an ATM VPI profile on page 143](#)

[Creating an ATM VPL on page 373](#)

[Finding ATM VCLs and cross connects on page 461](#)

[Modifying a card's ATM bandwidth settings on page 144](#)

Creating an ATM VCL for data

Use this procedure to create an ATM VCL for ATM terminated connections (AAL5 VCL endpoints) or VCLs used in cross connects (ATM Other endpoints)

- 1 Navigate to the port you want to create an ATM VCL on.
- 2 Expand the tree view to display the **ATM Logical** label.
- 3 Right-click the **ATM VCL Endpoints** label and select **Add**.

The selection dialog box appears:

For ATM termination endpoints, select **Aal5 Vcl End Point Default** (or a user-defined template).

For VCLs used in cross connects, select **Atm Other Vcl End Point Default** (or a user-defined template).

- 4 Click **OK**.
- 5 The **Add ATM Other VCL Endpoint Configuration** dialog box or the **Add ATM AAL5 VCL Endpoint Configuration** appears, depending on the type of endpoint you are configuring.
- 6 Specify the following:
Admin Status. Set to **Up**.
(Optional). Specify a name.
Specify the VPI/VCI for the VCL.
Click the browse button to select an existing traffic descriptor to use.

- 7 Click **Add**.
NetHorizon creates the VCL.

- 8 Click **Close**.
The VCL can now be used for data connections.

Related topics:

[Adding ATM cross connect on MALC, and Raptor using the wizard on page 364](#)

[Adding ATM cross connect on MALC, and Raptor \(advanced mode\) on page 366](#)

[Adding an ATM cross connect \(VP switched connection\) on page 369](#)

[Changing VCL rates on page 141](#)

[Creating ATM cross connect configuration templates on page 362](#)

[Creating ATM traffic descriptor configuration templates on page 361](#)

[Creating an ATM AAL2 VCL on page 349](#)

[Creating an ATM VPL on page 373](#)

[Creating an ATM VPI profile on page 143](#)

[Finding ATM VCLs and cross connects on page 461](#)

Creating an ATM VPL

To create an ATM VPL:

- 1 Navigate to the port you want to create an ATM VPL on.
- 2 Expand the tree view to display the **ATM Logical** label.
- 3 Right-click the **ATM VPL Endpoints** label and select **Add**.
The selection dialog box appears.
- 4 Select the VPL template to use.
- 5 Click **OK**.
- 6 The **Add ATM VPL Endpoint Configuration** dialog box appears.
- 7 Specify the following:
Admin Status. Set to **Up**.
(Optional). Specify a name.
Specify the VPI for the VPL.



Note: An existing ATM VPI profile with **Switch Type** set to **Vp Switched** must already exist for the selected VPI. See [Creating an ATM VPI profile on page 143](#).

Click the browse button to select an existing traffic descriptor to use.

- 8 Click **Add**.
NetHorizon creates the VPL.
- 9 Click **Close**.
The VPL can now be used for data connections.

Related topics:

[Adding ATM cross connect on MALC, and Raptor using the wizard on page 364](#)

[Adding ATM cross connect on MALC, and Raptor \(advanced mode\) on page 366](#)

[Adding an ATM cross connect \(VP switched connection\) on page 369](#)

[Changing VCL rates on page 141](#)

[Creating ATM cross connect configuration templates on page 362](#)

[Creating ATM traffic descriptor configuration templates on page 361](#)

[Creating an ATM VCL for data on page 372](#)

[Creating an ATM VPI profile on page 143](#)

[Finding ATM VCLs and cross connects on page 461](#)

Adding an ATM cross connect (CES)

There two types of CES cross connected circuits: structured and unstructured. In unstructured emulation (also known as clear channel emulation) the entire services bandwidth is emulated and reproduced at the target port. Structured emulation service (also called channelized emulation) emulates a point-to-point fractional T1/E1 (less than a full T1/E1 line) connections.

The frame structure is maintained. Individual streams are visible and are byte aligned. This allows the T1/E1 trunks to break into multiple DS-0 channels towards different destinations.

Configuring CES cross connections is similar to other types of cross connections:

- VCLs can be autocreated or existing.
- Traffic descriptors can be autocreated or existing.
- ATM endpoints VPI/VC are specified for uplink and downstream sides of the cross connect.

To add a CES cross connection:

- 1** Right-click a device and select **Manage ATM Connections**.

The **Configure ATM Cross Connects** dialog box appears. If there are any cross connects configured on the system, they are displayed.

- 2** Select the **CES Cross Connects** tab.

- 3** Click **Add**.

The **Creating CES Cross Connects on device [device name]** dialog box appears.

- 4** From this dialog box you create the desired CES cross connect:
 - Select a configuration template.
 - Enter a name for the cross connect.
 - Select the desired Admin Status.

- Decide whether you want to automatically create the traffic descriptors or use existing traffic descriptors.
- Select the desired upstream physical port and VPI

Decide whether you want to automatically select the VCI or use an existing VCI.

- Select the desired downstream physical port, VPI and VCI.

Use the Check Availability button to verify access.

- Specify the desired upstream (Trunk) and downstream (Line) DS0 bundles.

T1 circuits contain DS0's 1 to 24. E1 circuits contain DS0's 0 to 31. For CES port to port cross connections, the upstream and downstream DS0 bundles must contain the same number of DS0's.

5 When finished with the cross connect configuration, click **Add**.

NetHorizon begins creating the cross connect and displays a status window describing the progress.

After the connection has been successfully added, NetHorizon displays a confirmation dialog box.

6 Click **OK** to close the confirmation dialog box.

7 Click **Close**.

NetHorizon displays the new cross connect in the **Configure ATM Cross Connects** dialog box. If you need to modify, view or delete the connection, you can do it from this dialog box.

Related topics:

[Adding ATM cross connect on MALC, and Raptor using the wizard on page 364](#)

[Adding ATM cross connect on MALC, and Raptor \(advanced mode\) on page 366](#)

[Changing VCL rates on page 141](#)

[Creating ATM cross connect configuration templates on page 362](#)

[Creating ATM traffic descriptor configuration templates on page 361](#)

[Creating an ATM VCL for data on page 372](#)

[Creating an ATM VPL on page 373](#)

[Creating an ATM VPI profile on page 143](#)

[Deleting an ATM cross connect on page 371](#)

[Finding ATM VCLs and cross connects on page 461](#)

[Modifying a card's ATM bandwidth settings on page 144](#)

Adding an ATM Circuit Emulation Service (CES) cross connect using the wizard

When you add an CES cross connect, you can:

- Specify existing upstream and downstream VCLs in the ATM VCL cross connection. This option requires that the **Admin Status** of the existing upstream and downstream VCLs be set to **Up** before you add the ATM VCL cross connection.
- Request that ZMS automatically create the upstream and downstream VCLs in the ATM VCL cross connection. With this option, ZMS automatically sets the **Admin Status** of the upstream and downstream VCLs to **Up**.
- Specify existing Traffic Descriptors or use Traffic Descriptor templates.

To add a VC switched data connection:

- 1 Right-click a device and select **Manage ATM Connections**.

The **Configure ATM Cross Connects** dialog box appears. If there are any cross connects configured on the system, they are displayed.

- 2 Select the **CES Cross Connects** tab.

- 3 Click **Add (Wizard)** to add the cross connect using the wizard.

The wizard dialog box appears.

- 4 Select a template.

To view the template configuration, click **View**.

- 5 Click the next button.

The **Administrative Options** dialog box appears.

- 6 From this dialog box you can specify basic ATM parameters:

- (Optional). Enter a name for the cross connect.
- Verify that the cross connect is enabled (this is the default).
- Decide whether you want to automatically create the VCL endpoints or use existing VCLs.

Select **Auto Create the Upstream/Downstream VCLs** if you want NetHorizon to automatically create the endpoints.

Select **Use Existing Upstream/Downstream VCLs** if you want NetHorizon to use existing endpoints. If you choose this option, the endpoints must already exist.

- 7 Click the next button.

The **Trunk Side Configuration** dialog box appears.

- 8 From this dialog box you configure the ATM trunk side interface.

For automatically created VCLs:

- Click the Browse button and select the trunk physical interface for the cross connect.
- Select the VPI.
- Select **Auto Increment VPI If Necessary** if you want NetHorizon to continue to provision cross connects using a particular VPI until all the VCIs are provisioned. NetHorizon will then start creating cross connects on the next available VPI.
- Select **Auto Select Available VCI** for NetHorizon to automatically use the next available VCI values for the cross connect.
- Select **Manually Select Starting VCI** to indicate the starting VCI you want to use in the cross connect. ZMS will automatically select the next available trunk side VCI to use if you are creating more than one cross connect.
- Click the Browse button and select the traffic descriptor template to use.

For existing VCLs:

Click the Browse button and select the trunk VCL for the cross connect.

- 9 When finished with the trunk side configuration, click the next button.

The **Traffic Descriptor Configuration** dialog box appears. From this dialog box you specify the ATM traffic descriptors to use for the cross connect. (This option is not available if the auto-create option on the **Admin** screen was selected.)

- 10 Specify whether you want to use traffic descriptor templates or existing traffic descriptors, then click the browse button to select the traffic descriptor.
- 11 Click the next button.

The **Line Side Configuration** dialog box appears.

- 12 From this dialog box you configure the ATM line side interface.

For automatically created VCLs:

- Specify the VPI/VCI to be used for all line side VCLs. The ATM VCL profiles and existing VCLs will determine which ports are available. For specific VPI/VCI combinations, the ports will automatically be enabled or disabled when the **Check Availability** button is clicked.

Click the **Check Availability** button every time you change the VPI or VCI in order to ensure that the selected ports are still available.

- Select the slot and port for the cross connect. Note that you can select multiple ports to create multiple cross connects.

For existing VCLs:

Click the Browse button and select the line side interface VCL for the cross connect.

13 Click the next button.

The **Circuit Emulation Service** dialog box appears.

Specify the desired Trunk (upstream) and Line (downstream) DS0 bundles. For port to port cross connections, the DS0 bundle size must match.

14 Click **Add**.

NetHorizon begins creating the cross connect and displays a status window describing the progress.

After the connection has been successfully added, NetHorizon displays a confirmation dialog box.

15 Click **OK** to close the confirmation dialog box.

16 Click **Close**.

NetHorizon displays the new cross connect in the **Configure ATM Cross Connects** dialog box. If you need to modify, view or delete the connection, you can do it from this dialog box.

Related topics:

[Adding an ATM cross connect \(VP switched connection\) on page 369](#)

[Changing VCL rates on page 141](#)

[Creating ATM cross connect configuration templates on page 362](#)

[Adding ATM cross connect on MALC, and Raptor \(advanced mode\) on page 366](#)

[Creating ATM traffic descriptor configuration templates on page 361](#)

[Creating an ATM VCL for data on page 372](#)

[Creating an ATM VPL on page 373](#)

[Creating an ATM VPI profile on page 143](#)

[Deleting an ATM cross connect on page 371](#)

[Finding ATM VCLs and cross connects on page 461](#)

[Modifying a card's ATM bandwidth settings on page 144](#)

Modifying CES

CES circuits can be modified to change the following service parameters

- Name
- CAS
- Partial Fill
- Buffer Max Size

- Cell Loss Integration Period
- DS0 Bundle

To modify a CES circuit:

- 1 Select the CES circuit(s) in the ATM VPL Endpoints folder under the configured slot, port, and interface in the NetHorizon tree.
- 2 From the right-click menu, select **Circuit Emulation Service...**

If a single CES circuit is selected, the **Modify Circuit Emulation Service Configuration** dialog box appears with the CES circuit information.

If a multiple CES circuits are selected, the **Modify Circuit Emulation Service Configuration** dialog box appears with information for the selected CES circuits.

- 3 Click **Reset** to return displayed settings to default values.
- 4 Click **Modify** to apply to setting changes.
- 5 Click **Close** to exit the dialog.

Related topics:

[Adding ATM cross connect on MALC, and Raptor using the wizard on page 364](#)

[Adding ATM cross connect on MALC, and Raptor \(advanced mode\) on page 366](#)

[Adding an ATM cross connect \(VP switched connection\) on page 369](#)

[Finding ATM VCLs and cross connects on page 461](#)

Optical cross connection (GigaMux only)

The optical cross connection feature allows users to associate and track virtual circuits within the system. In the device specific configuration, the cross connection allows the operator to configure database only values including circuit IDs, contact numbers, and any notes associated with the circuits or connections.



Note: Optical cross connection is applicable only on GigaMux devices.

Topics:

- [Adding an optical cross connect](#)
- [Modifying an optical cross connection](#)
- [Deleting an optical cross connect](#)

Adding an optical cross connect

When you add an optical cross connect to a GigaMux device, you can either:

- Select the desired device in the tree view, and from Tools menu select **Manage Optical CrossConnections**.
- Or right-click the desired device in the tree view, and select **Manage Optical CrossConnections**.

To add an optical data cross connection:

- 1** Right-click a device and select **Manage Optical CrossConnections**.

The **Configure Optical Cross Connects** dialog box appears.

If there are any optical cross connects configured on the system, they are displayed.

The speed of the link between the two cross connected devices are also displayed in the **Data Rate** field.

- 2** Click **Add**.

The **Creating Optical Cross Connects** dialog box appears.

- 3** Click the Browse button on the **Select Template** field to select a template for this cross connect.

- 4** In the **Select ports for Cross Connection** area, specify:

- **CircuitID:** Enter an index number for the cross connect.
- **Device A:** Click the Browse button and select the port as one end of the cross connect.
- **Device B:** Click the Browse button and select the port as another end of the cross connect.
- **Parameter A:** User only configurable database field. (Optional)
- **Parameter B:** User only configurable database field. (Optional)
- **Description:** Enter the brief description for the cross connect. (Optional)

Note that Circuit ID, Device A, and Device B fields are mandatory fields, adding with empty fields will pop up an error message.

Port availability for cross connection will also be checked. An error message will pop up if the selected port is not free for cross connection.

- 5** Click **Add**.

The status and information of the cross connection are displayed. After the connection has been successfully added, NetHorizon display a confirmation dialog box.

- 6** Click **OK** to close the confirmation dialog box.

- 7** Click **Close** to close the **Creating Optical Cross Connects** dialog box.

NetHorizon displays the new optical cross connect in the **Configure Optical Cross Connects** dialog box. If you need to modify, view or delete the connection, you can do it from this dialog box.

Modifying an optical cross connection

Use these procedures to modify an existing optical cross connection.

To modify an existing cross connection:

- 1 Right-click the desired GigaMux device and select **Manage Optical CrossConnections**.

The **Configure Optical Cross Connects** dialog box appears.

- 2 Highlight an optical cross connection and click **Modify**.

The **Modify Optical Cross Connects** dialog box appears.

- 3 Make the changes in the Description field.

- 4 Click **Modify**.

NetHorizon displays the new description in the **Configure Optical Cross Connects** dialog box.

Deleting an optical cross connect

To delete an optical cross connect:

- 1 Right-click the desired GigaMux device and select **Manage Optical CrossConnections**.

The **Configure Optical Cross Connects** dialog box appears.

- 2 Highlight an optical cross connection and click **Delete**.

The **Delete Confirmation** dialog box appears.

- 3 Click **OK** to close the confirmation dialog box.

- 4 The status and information of the deletion are displayed in the **Status of Delete** dialog box.

- 5 Click **Close** to complete the deletion procedure.

NetHorizon removed the optical cross connect from the **Configure Optical Cross Connects** dialog box.

IP configuration

Topics:

[DHCP](#)

[Adding network-based routes](#)

[Adding host-based routes](#)

[Adding IP interfaces](#)

[Modifying the IP routing domain and adding static routes](#)

[Adding IP interfaces \(Z-Edge only\)](#)

[Configuring NAT \(Z-edge only\)](#)

[Configuring PAT bindings](#)

[Configuring IPSLA](#)

[Configuring IP on a bridge](#)

[Remote IP address options on IADs](#)

DHCP

Topics:

[DHCP relay](#)

[Specifying DHCP server in DHCP relay mode](#)

[Setting up a DHCP server](#)

[Modifying DHCP defaults](#)

DHCP relay

The MALC/MXK/XP support DHCP relay.

In DHCP relay scenarios, the MALC/MXK/XP serve as a DHCP relay agent that forwards broadcast DHCP discover and DHCP request packets to external DHCP server(s). It then forwards the unicast DHCP offer and DHCP ack/nak replies to the requesting DHCP host.

By default, DHCP broadcast messages cross the router interfaces. To solve the problem of DHCP broadcast messages on multiple subnets, the MALC/MXK/XP can be configured as a DHCP relay agent that communicates with DHCP server(s) and acts as a proxy for DHCP broadcast messages that need to be routed to remote downstream segments.

Note the following requirements for DHCP relay:

- The external DHCP server must be configured to assign addresses on the same subnet as the floating IP address used by the remote device.
- The external DHCP server must be configured with a static route for the remote device's subnet back to the MALC/MXK on which the relay agent is running. (The DHCP server will send DHCP unicast packets to the relay agent's address.)
- A separate DHCP server can be specified per subnet.

Specifying DHCP server in DHCP relay mode

In DHCP relay mode, you can add, delete, modify the primary DHCP server or an alternate DHCP server. The alternate DHCP server can be added only the primary DHCP server contains IP address. The alternate DHCP server will be forwarded DHCP requests and DHCP discoveries as well as the primary DHCP server.



Note: When using the alternate DHCP server option, you should configure your DHCP servers in a mirrored configuration so they are communicating with each other and that both are not giving out the same address to different clients.

To specify the alternate DHCP server (i.e. alternate external server) through the **Manage Bridge Logicals** dialog:

- 1 Right-click a device and select **Manage Bridging**.

The **Manage Bridge Logicals** dialog box appears.

- 2 In the **Manage Bridge Logicals** dialog box, click the **Bridge Filtering** tab.

The **Manage Bridge Logicals** dialog box appears with the bridge filtering options.

- 3 To add a packet rule group, click **Add** in the **Packet Rule Group** portion of the dialog box. The **Add Packet Rule Group Configuration** dialog box for adding a bridge filter appears.

Specify the packet rule group and member settings. The specified group will be created along with the specified member.

Group Name — Specify the bridge filter group name in the **Group Name** field.

Type — Select the DHCP Relay filter type.

Subnet Group Index — Click browse button to select the subnet group index.

Add DHCP Server Configuration dialog — Click **Add** button that appears to the right of the **Subnet Group Index** field to open the **Add DHCP Server Configuration** dialog. Specify the DHCP server information then click **Add** button.

- 4 Click **Add** in the **Add Packet Rule Group Configuration** dialog.
The packet rule group and member are added. The packet rule group index must be assigned to the bridge interface during bridge configuration.
- 5 Click **Help** to access the online help.
- 6 Click **Close** to exit the dialog.

Setting up a DHCP server

The Dynamic Host Control Protocol (DHCP) provides a mechanism through which client computers using TCP/IP can obtain configuration parameters (such as the default router and the DNS server, subnet mask, gateway address, and lease time) from a DHCP server. The most important configuration parameter carried by DHCP is the IP address.

As a DHCP server, the device can assign temporary (leased) IP addresses to clients. Each DHCP client sends a DHCP request to the device for an IP address lease. The device then assigns an IP address and lease time to the client. The device keeps track of a range of assignable IP addresses from a subnetwork.

- 1 Right-click a device icon and select **Manage IP**.
The **IP Configuration Manager** dialog box appears.
- 2 Select the **DHCP** tab.
- 3 Click **Add**. The **Add DHCP Server Configuration** dialog box appears.
- 4 In the **Add DHCP Server Configuration** dialog box specify:

Name—the name of the DHCP server.

Subnet Network—the network address associated with this DHCP subnet.

Subnet Netmask—the network mask associated with this DHCP subnet.

Default Router—the IP address of the client's default gateway.

External Server—the IP address of the primary DHCP server to be used for this subnet.

Alternate External Server—the IP address of the alternate DHCP server to be used for this subnet. You can only add an alternate DHCP server if the primary DHCP server (i.e. external server) contains an address.



Note: When using the alternate DHCP server option, you should configure your DHCP servers in a mirrored configuration so they are communicating with each other and that both are not giving out the same address to different clients.

Subnet Group—specifies a range (or pool) of assignable addresses.

Sticky Address—if enabled, the DHCP server attempts to hand out the same IP address to the same host, when possible, based on hardware address.

See the online help for details on these settings.

- 5 Select **DHCP Subnet Range** from the tree.

The **DHCP Subnet Range** dialog box appears.

- 6 Enter DHCP server ranges. Four address ranges are allowed.

- 7 If you want to configure DNS or modify DHCP lease times, select **DHCP Subnet Options** from the tree.

The **DHCP Subnet Options** dialog box appears.

- 8 In the **DHCP Subnet Options** dialog box specify:

Domain Name—The default domain name for the client to use when resolving host names using DNS.

Primary DNS Server—The IP address of the primary domain name server for the client to use for DNS resolution.

Secondary DNS Server—The IP address of the secondary domain name server for the client to use for DNS resolution.

Boot Server—The IP address of the server from which the initial boot file is to be loaded.

Boot File—The filename of the initial boot file to be loaded by the client. The filename should be recognizable to the file transfer protocol that the client uses to load the file.

Default Lease Time—The default time, in seconds, assigned to a lease if the client requesting the lease does not specify an expiration time.

Min Lease Time(seconds)—The minimum expiration time, in seconds, assigned to a lease regardless of the value specified by a client.

Max Lease Time(seconds)—The maximum expiration time, in seconds, assigned to a lease regardless of the value specified by a client.

The value-1 indicates that this parameter should be ignored.

For details on these settings, see the online help.

- 9 Click **Add**.

The newly added subnet appears in the **IP Configuration Manager** dialog box.

Modifying DHCP defaults

- 1 Right-click a device icon and select **Manage IP**.
The **IP Configuration Manager** dialog box appears.
- 2 Select the **DHCP** tab.
- 3 Select **Subnet**, **Host**, or **Subscriber** to modify.
- 4 Click **Modify** in the Server Defaults pane, the **Modify DHCP Server Configuration** dialog box appears.
- 5 In the **Modify DHCP Server Configuration** dialog box you can specify:
 - Lease Time (seconds)**—Time, in seconds, assigned to a lease if the client requesting the lease does not specify an expiration time.
 - Min Lease Time (seconds)**—The minimum expiration time, in seconds, assigned to a lease regardless of the value specified by a client.
 - Max Lease Time (seconds)**—The maximum expiration time, in seconds, assigned to a lease regardless of the value specified by a client.
 - Num. of IP Add Reserved at Start of Subnet**
 - Num. of IP Addr Reserved at End of Subnet**
 See the online help for details on these settings.

Adding network-based routes

Network-based routing is ideal for adding large numbers of IP addresses. Unlike host-based routing, network based-routing requires numbered IP interfaces on the device. In a network-based routing with DSL bridges application, each bridge is in the same network as one of the device's numbered interfaces.

Network-based routing with DSL routers allows multiple statically assigned addresses per customer. In this application, each remote router is on a subnet with a numbered interface on the device.

Similar to host-based routing, network-based routing interoperates with DSL bridges and routers. The type of AAL5 encapsulation determines interoperability with DSL routers or DSL bridges. LLC encapsulation is used with DSL routers; RFC 1483 encapsulation is used with DSL bridges.

- 1 Right-click a device and select **Manage IP**.
The **IP Configuration Manager** dialog box appears. If there are any IP connections configured on the device, they are displayed here.
- 2 Click the **Subscriber Host** tab. The Local Host Addresses and Remote Host Address are listed.
- 3 Click **Add**. The **Add IP Interfaces** dialog box appears.
- 4 Select a physical
- 5 If you chose **Auto create the VCL for IP traffic**:

- Enter **VPI** and **VCI** values
- Select a **Transmit Traffic Descriptor** by clicking on the Browse button
- Select a **Receive Traffic Descriptor** by clicking on the Browse button
- Select **Encapsulation Type: Routed 1483** is used DSL routers; **Bridged 1483** (RFC 1483) is used with DSL bridges.
- Enter the **IP Address** for the new interface
- Enter the **Netmask** for the new interface.
- Enter the **Broadcast Address** for the new interface.
- Enter the VLAN and VLAN COS settings.
- Enter the SLAN and SLAN COS settings.
- Click **Add**.

For details on these settings, see the online help.

6 If you chose **Use an existing VCL for IP traffic**:

- Select an AAL5 VCL by clicking on the Browse button.
- Enter the **IP Address** for the new interface
- Enter the **Netmask** for the new interface.
- Enter the **Broadcast Address** for the new interface.
- Click **Add**.

For details on these settings, see the online help.

Adding host-based routes

Host-based routing takes advantage of ATM VCLs, IP unnumbered interfaces, and shared DHCP pools to conserve IP addresses. In the host-based routing with DSL bridges application, subscribers connected to the device are on the same subnet as the unnumbered interface.

In the host-based routing with DSL routers application, remote IADs (or routers) are on the same subnet as the unnumbered interface. The IADs connect private networks to the device.

The type of AAL5 encapsulation determines interoperability with DSL routers or DSL bridges. LLC encapsulation is used with DSL routers; RFC 1483 encapsulation is used with DSL bridges. CES over IP connections are also available.

To add host-based routes:

1 Right-click a device and select **Manage IP**.

The **IP Configuration Manager** dialog box appears. If there are any host connections configured on the device, they are displayed here.

- 2 Select the **Floating IP** tab and click **Add**.

The **Add IP Logical Configuration** dialog box appears.

- 3 In the **Add IP Logical Configuration** dialog box specify:

IP Address—The floating IP address that will be shared by all devices in the host-based routing subnet.

NetMask— The subnet mask associated with the floating IP address. The value of the mask is an IP address with all network bits set to 1 and all hosts bits set to 0.

Broadcast Address—The IP broadcast address used for sending datagrams on the (logical) interface associated with the floating IP address.

DHCP Server—if true, the host will act as a DHCP server to assign IP addresses to the DHCP clients.

VLAN and VLAN COS Settings—Specify the desired VLAN and VLAN COS settings.

SLAN and SLAN COS Settings—Specify the desired SLAN and SLAN COS settings for ‘double tagged’ Ethernet frames.

See the online help for details on these settings.

- 4 If the device will be a DHCP server, set **DHCP Server** to **True**. Otherwise, leave the default setting of **False**.

- 5 Click **Add**.

The newly added IP logical connection appears in the **IP Configuration Manager** dialog box.

- 6 Select the DHCP tab and click **Add**.

The **Add DHCP Server Configuration** dialog box appears.

- 7 In the **Add DHCP Server Configuration** dialog box specify:

Name—the name of the DHCP server.

Subnet Network—the network address associated with this DHCP subnet.

Subnet Netmask—the network mask associated with this DHCP subnet.

Default Router—the IP address of the client’s default gateway.

External Server—the IP address of the external DHCP server to be used for this subnet.

Subnet Group—specifies a range (or pool) of assignable addresses.

Sticky Address—if enabled, the DHCP server attempts to hand out the same IP address to the same host, when possible, based on hardware address.

See the online help for details on these settings.

- 8 Select **DHCP Subnet Range** from the tree.

The **DHCP Subnet Range** dialog box appears.

- 9 Enter DHCP server ranges. Four address ranges are allowed.

- 10 If you want to configure DNS or modify DHCP lease times, select **DHCP Subnet Options** from the tree.

The **DHCP Subnet Options** dialog box appears.

- 11 Complete the parameters in the **DHCP Subnet Options** dialog box:

Domain Name—The default domain name for the client to use when resolving host names by way of DNS.

Primary DNS Server—The IP address of the primary domain name server for the client to use for DNS resolution.

Secondary DNS Server—The IP address of the secondary domain name server for the client to use for DNS resolution.

Default Lease Time—The default time, in seconds, assigned to a lease if the client requesting the lease does not specify an expiration time

For details on these settings, see the online help.

- 12 Click **Add**.

The newly added subnet appears in the **IP Configuration Manager** dialog box.

- 13 Click on the **Subscriber Hosts** tab.

The **Subscriber Hosts** window of the **IP Configuration Manager** dialog box appears. This dialog box configures both the local and remote sides of the connection.

- 14 Click **Add**. The **IP Subscriber Hosts on Device** dialog box appears.

- 15 Specify the desired IP subscriber host options:

- Enter **VPI** and **VCI** values. Click Check Availability button to verify valid values.
- Click the check boxes for the desired physical ports. If multiple ports are selected, the specified configuration settings apply to all selected ports.
- Select the desired **GPON GEM port ID**. This option only applies to GPON ONT/ONU port.
- Select the desired **GPON traffic profile index**. This option only applies to GPON ONT/ONU port.
- Select a **Transmit Traffic Descriptor** by clicking on the Browse button
- Select a **Receive Traffic Descriptor** by clicking on the Browse button

- Select **Encapsulation Type**: **Routed 1483** is used DSL routers; **Bridged 1483** (RFC 1483) is used with DSL bridges.
- Enter the **Multicast Control List** for the new interface.
- Enter the **Max Number of Multicast Streams** for the new interface.
- Select **Dynamic** or **Static** IP Address for the new interface.
- For **Dynamic** host routes enter the **Subnet Group** that will be used and the **Number IP**, which indicates the number of hosts that will be assigned.
- For **Static** host routes, enter the **IP Address** of the destination.
- Enter VLAN ID.
- Enter S-tag ID.
- Click **Add.I**

For details on these settings, see the online help.

16 If you chose **Use an existing VCL for IP traffic**:

- Select an AAL5 VCL by clicking on the Browse button.
- Enter the **Multicast Control List** for the new interface.
- Enter the **Max Video Streams** for the new interface.
- For **Dynamic** host routes enter the **Subnet Group** that will be used and the **Number IP**, which indicates the number of hosts that will be assigned.
- For **Static** host routes enter the **IP Address** of the destination.
- Click **Add**.

For details on these settings, see the online help.

17 To add a CES over IP connection:

Right-click a device and select **Manage IP**.

The **IP Configuration Manager** dialog box appears. If there are any host connections configured on the device, they are displayed here.

Click the **CES Hosts** tab.

The following data is displayed for any configured CES hosts.

- Shelf-Slot-Port
- VPI
- VCI
- Source IP
- Source Port
- Destination IP

- Destination Port
- DS0 Bundle

18 Click **Add** to add an CES Host.

The **IP Subscriber Hosts on Device** dialog box appears for CES configuration.

19 Specify the VCL and VC data and enter the desired CES data:

Source IP —The source IP address for the CES circuit. A floating IP address must be configured on the uplink.

Source Port— The source port used for the CES circuit.

Destination IP—The destination IP address for the CES circuit.

Destination Port—The destination port used for the CES circuit.

Structured/Unstructured—Select the option for structured or unstructured CES circuit. If Structured is selected, specify the DS0 bundle size.

See the online help for details on these settings.

Related topics:

[Adding an ATM cross connect \(VP switched connection\) on page 369](#)

[Creating an ATM VCL for data on page 372](#)

Adding IP interfaces

1 Right-click a device and select **Manage IP**.

The **IP Configuration Manager** dialog box appears. If there are any IP connections configured on the device, they are displayed here.

2 Click **Add**.

The **Add IP Interfaces** dialog box appears.

3 Select one of the options:

- **Select the physical to create the IP interface**
- **Select the VCL to create the IP interface**

4 If you chose **Select the physical to create the IP interface**:

- Select a **Physical** interface by clicking on the Browse button
- Enter **VPI** and **VCI** values
- Select a **Transmit Traffic Descriptor** by clicking on the Browse button
- Select a **Receive Traffic Descriptor** by clicking on the Browse button
- Select **Encapsulation Type: Routed 1483** is used DSL routers; **Bridged 1483** (RFC 1483) is used with DSL bridges.
- Enter the **IP Address** for the new interface

- Enter the **Netmask** for the new interface.
- Enter the **Broadcast Address** for the new interface.
- Enter the **Address Mode** for the new interface (static or DHCP client).
- Specify if the **DHCP Server** is used for the new interface.
- Enter the **Max Number of Multicast Streams** for the new interface.
- Enter the **Ingress Filter ID** for the new interface.
- Enter the **Egress Filter ID** for the new interface.
- Enter the **VLAN Class-of-Service** for the new interface.
- Enter the **COS Option** for the new interface.
- Enter the **COS Value** for the new interface.
- Click **Add**.

For details on these settings, see the online help.

5 If you chose **Select the VCL to create the IP interface:**

- Select an AAL5 **VCL** by clicking on the Browse button.
- Select a **Transmit Traffic Descriptor** by clicking on the Browse button
- Select a **Receive Traffic Descriptor** by clicking on the Browse button
- Enter the **IP Address** for the new interface
- Enter the **Netmask** for the new interface.
- Enter the **Broadcast Address** for the new interface.
- Click **Add**.

For details on these settings, see the online help.

For interface changes, see [Modifying the IP routing domain and adding static routes](#)

Modifying the IP routing domain and adding static routes

1 Right-click a routing domain and select Modify.

The **Modify IP Routing Domain Configuration** dialog box appears. If there are any routing domains configured on the device, they are displayed here.

2 Modify the desired fields.

To modify the identity.

- a** Change the displayed identity name.

- b** Click **Modify** to apply the change.
- c** Click **Reset** to undo the changes or click **Close** to exit the dialog.

To modify the DNS resolver.

- a** Click **DNS Resolver** in the tree and modify the desired fields:

- Query order
- Domain name
- First name server
- Second name server
- Third name server

- b** Click **Modify** to apply the change.
- c** Click **Reset** to undo the changes or click **Close** to exit the dialog.

To modify the static routes.

- a** Click **Static Routes** in the tree and modify the desired fields:

The MALC supports IP redundancy or fallback IP routes. A fallback route is a second static route with the same destination and netmask of an existing route but with a different nexthop destination. The redundant or fallback route is used when the original nexthop destination is unavailable. The fallback route continues to be used until it is unavailable. At that time, traffic switches back to the primary route.

A ping interval and ping retry count are used to determine route availability. The MALC pings the active nexthop router once during each ping interval. The ping-interval is specified in milliseconds and has a minimum value of 500 milliseconds or 1/2 second. If the number of ping failures to the current nexthop destination exceeds the ping-fail-max setting, the current nexthop destination is replaced in the routing table with the fallback nexthop destination. The system begins pinging the new nexthop router and monitoring the number of ping failures.

- Address
- Net mask
- Next hop router
- Routing method
- Interface
- Backup metric
- Ping interval
- Ping fail max

- b** Click **Modify** to apply the change.

c Click **Reset** to undo the changes or click **Close** to exit the dialog.

d To add a static route, click **Add**.

The **Add IP Static Route Configuration** dialog box appears.

e Enter the name of the static route.

f Click **Static Route Configuration**.

The static route settings appear.

Settings for destination based routes.

Settings for source address based routes

Select the desired Static Route Configuration fields:

- Select the desired routing method: destination or static routing.
- Specify the IP address
- Specify the net mask.
- For destination based routes, specify the next hop router. For source address based routes, specify the source interface.
- Specify the desired metric for the route.

g Click **Add** to add the specified route.

h Click **Reset Defaults** to restore the default settings. Click **Close** to exit the dialog.

For details on these settings, see the online help.

Adding IP interfaces (Z-Edge only)

1 Right-click a Z-Edge 64 device and select **Manage IP**.

The **IP Configuration Manager** dialog box appears. If there are any IP connections configured on the device, they are displayed here.

2 Click **Add**.

The **Add IP Interfaces** dialog box appears.

3 Select one of the options:

- **Select the physical to create the IP interface**
- **Select the VCL to create the IP interface**

4 If you chose **Select the physical to create the IP interface**:

- Enter **VPI** and **VCI** values
- Select a **Transmit Traffic Descriptor** by clicking on the Browse button

- Select a **Receive Traffic Descriptor** by clicking on the Browse button
- Select **Encapsulation Type: Routed 1483** is used DSL routers; **Bridged 1483** (RFC 1483) is used with DSL bridges.
- Enter the **IP Address** for the new interface
- Enter the **Netmask** for the new interface.
- Enter the **Broadcast Address** for the new interface.
- Enter the VLAN and VLAN COS settings.
- Enter the SLAN and SLAN COS settings for ‘double tagged’ Ethernet frames.
- Click **Add**.

For details on these settings, see the online help.

5 If you chose **Select the VCL to create the IP interface:**

- Select an AAL5 VCL by clicking on the Browse button.
- Select a **Transmit Traffic Descriptor** by clicking on the Browse button
- Select a **Receive Traffic Descriptor** by clicking on the Browse button
- Enter the **IP Address** for the new interface
- Enter the **Netmask** for the new interface.
- Enter the **Broadcast Address** for the new interface.
- Click **Add**.

For details on these settings, see the online help.

Configuring NAT (Z-edge only)

Network Address Translation (NAT) is an Internet standard that enables a local area network (LAN) to use one set of IP addresses for internal traffic and a second set of addresses for external traffic. Hosts in a private network can transparently access an external network and enable access to selective local hosts from the outside.

- 1** Right-click a device and select **Modify**.
- 2** From the **Modify Device** dialog box, click **NAT Configuration**.
The **NAT Configuration** dialog box appears.
- 3** Modify NAT settings:
 - **TCP Timeout**
 - **UDP Timeout**

For details on these settings, see the online help.

You also have the option to clear NAT Bindings from the NAT Configuration dialog box.

- 4 Click **Modify** and then **Close**.

Related topics:

[Configuring PAT bindings on page 396](#)

Configuring PAT bindings

One limitation of NAT is that local hosts cannot be contacted from the Internet, unless the local host has already established communications with the Internet-accessible device. Port address translation (PAT) is a form of NAT which overcomes this limitation. PAT bindings map public IP addresses with either UDP or TCP ports to make local hosts accessible from the Internet.



Note: You must have NAT enabled on the IP interface of the WAN port before enabling PAT. See [. Configuring NAT \(Z-edge only\) on page 395](#).

- 1 Right-click a device and select **Modify**.
- 2 From the **Modify Device** dialog box, click **PAT Bindings**.
The **PAT Bindings** dialog box appears.
- 3 Click **Add**.
The **Add PAT Bindings** dialog box appears.
- 4 Enter a **Name** to identify the PAT connection.
- 5 Enter the **Public Address**. This is the IP address that will be used on the Internet.
- 6 Enter the **Public Port**. This is the port on the Internet side of the connection.
- 7 Enter the **Local Address**. This is the private address that is the real destination.
- 8 Enter the **Local Port**. This the port number on the local host where packets will be forwarded.
- 9 Enter the **Port Type**: CPE Manager, UDP, or TCP
For details on these settings, see the online help.
- 10 Click **Add** and then **Close**. The PAT binding appears in the **PAT Bindings** window of the **Modify Device** dialog box.

Related topics:

[Configuring NAT \(Z-edge only\) on page 395](#)

Configuring IPSLA

Topics:

- [Configuring IPSLA statistics path](#)
- [Configuring CoS action](#)
- [Configuring CoS map](#)
- [Viewing the Real time IPSLA statistics](#)
- [Viewing the historical IPSLA statistics](#)

The IP Service Level Agreement (IPSLA) feature assists service providers and network operators with enforcing and monitoring access network connections and performance. IPSLA uses ICMP Ping messages over configured IPSLA paths to track Round Trip Times (RTTs) and EHCOREQs/RSPs between initiator and responder devices to determine network performance and delays. Typically, one initiator device is used to monitor other responder devices in the network. A maximum of 32 IPSLA paths can be configured per MALC/MXK/XP and 4 IPSLA paths per IP device.



Note: Networks must support CoS queues and DSCP to provide valid per CoS statistics. Otherwise, all statistics are sent to the default CoS queue.

Initiator devices must be running IPSLA to request data for a responder device. Responder devices must be accessible through the ping command in the IP network, but do not need to run IPSLA. Responder devices not running IPSLA display limited statistical data and functionality.

Default CoS-actions are assigned to each CoS queue so threshold crossing alarms can be configured to generate system alarms when thresholds are crossed for uptime, latency, jitter, and packet size.

Data based on received/sent packets and train rates is collected and displayed as real-time statistics for the current 15 minute interval as well as over 96 15-minute intervals for 24 hour historical statistics.

By default, IPSLA is disabled on all EtherXtend, MALC/MXK/XP card ports and other SLMS devices.

Configuring IPSLA statistics path

To add, modify, delete, and view the IP SLA statistics path:

- 1 To display the global IPSLA settings, right-click a device and select **Manage IP SLA**.

The **Modify IP SLA Configuration** dialog box appears. If there are any IP SLA connections configured on the device, they are displayed here.

By default, the **Global Configuration** window appears in the **Modify IP SLA Configuration** dialog box.

- 2 To enable global IPSLA and set the polling interval (in seconds):
 - Click the check box of the **Enabled status**.
 - Enter the **Poll Interface** value (60 to 3600 seconds) for real-time and historical statistics.
 - Click **Modify**.
- 3 To create a ICMP path between the initiator devices and the responder device. The device on which this configuration is configured becomes the initiator device, while the device for which an IP address is configured becomes the responder device. Typically, one initiator device can be used to monitor other responder devices in the network over a maximum of 32 MALC/MXK/XP and 4 EtherXten IPSLA paths per device.

Select **Static Path** from the tree menu. The **Static Path** window appears.
- 4 Click **Add**, the **Add Static Path** dialog box appears.
- 5 In the **Add Static Path** dialog box enter the desired value. Typically, one initiator device can be used to monitor other responder devices in the network over a maximum of 32 MALC and 4 EtherXtend IPSLA paths per device.
 - Enter **Action Index**
 - Enter the **Route Domain Index** for the target IP address.
 - Enter **Target IP** for the responder device which is at the other end of the path.
 - Select **Enabled** or **Disabled** in the **Source Forwarding**.
 - Select **Enabled** or **Disabled** in the **Admin State**. It specifies if the IPSLA feature actions will be exerted on the current member of the static entry list.
 - Click **Add** and then **Close**. The ICMP path appears in the **Static Path** window of the **Modify IP SLA Configuration** dialog box.
- 6 To modify an existing static path, in the **Static Path** window of the **Modify IP SLA Configuration** dialog box, select the desired static path and click **Modify**. The **Modify Static Path** dialog appears.
- 7 Enter the new static path settings.
- 8 Click **Modify** and **Close**, the static path with new settings appears in the **Static Path** window of the **Modify IP SLA Configuration** dialog box.
- 9 To delete a static path. Select the desired static path in the **Static Path** window of the **Modify IP SLA Configuration** dialog box, click **Delete**. The **Confirmation** dialog box appears.



Note: Disabling or deleting the path or globally disabling the IPSLA feature will reset historical data.

- 10** In the Confirmation dialog box, click **OK** to delete this static path, otherwise click **Cancel**.
- 11** To view the detail information of a static path. Select the desired static path in the **Static Path** window of the **Modify IP SLA Configuration** dialog box, click **View**. The **View Static Path** dialog box appears.

Configuring CoS action

Modify the default CoS actions to specify the response and threshold behavior for each CoS Action Index (1-8). These CoS actions map respectively to the CoS queues (0-7).

To configure CoS action:

- 1** Select **CoS Action** from the tree menu. The **CoS Action** window appears.
- 2** Select the desired CoS action and click **Modify**. The **Modify IP SLA COS Action** dialog appears.
- 3** In the **Modify IP SLA COS Action** dialog enter the desired CoS action settings:
 - Name
Name of the IPSLA CoS action, up to 9 characters in length.
 - Trap On Error
Select **Enabled** or **Disabled** to specify a trap is issued or not when any SLA performance error threshold within this CoS is crossed.
 - Timeout Error Threshold
The number of consecutive missed IP SLA responses within this CoS before a zhoneIpSLATimeoutTrap is issued.
 - Timeout Clear Threshold
The number of consecutive missed IP SLA responses within this CoS which must be received before the timeout error condition is cleared.
 - Latency Error Threshold
The 15 sample average round trip latency value which must be exceeded within this CoS before a zhoneIpSLALatencyTrap is issued.
 - Latency Clear Threshold
The number of consecutive IP SLA latency samples for which the 15 sample average round trip latency must be below the configured SLA latency error threshold within this CoS before the latency error condition is cleared.
 - Jitter Error Threshold

The 15 sample round trip jitter value which must be exceeded within this CoS before a zhonelpSLAJitterTrap is issued.

- Jitter Clear Threshold

The number of consecutive IP SLA RTT samples for which the 15 sample round trip jitter must be below the configured SLA jitter error threshold within this CoS before the jitter error condition is cleared.

- Metrics

Select **Enabled** or **Disabled** to specify if latency and availability measurements should be carried out for this CoS.

- Packet Size

The minimum IP SLA Ping packet size in bytes. The range is 64 to 2048 if the target IP device is running IPSLA, 64 to 512 otherwise.

- 4 Click **Modify** and then **Close**. The modified CoS action appears in the **CoS Action** window of the **Modify IP SLA Configuration** dialog box.
- 5 To view the settings for an individual CoS action. Select the desired CoS action and click **View**. The **View IP SLA COS Action** dialog appears.

Configuring CoS map

Configure the desired CoS maps to modify the default DSCP to CoS Action Index mappings. By default, DSCP are mapped to CoS Action Index entries based on RFC2599.

To configure CoS map:

- 1 Select **CoS Map** from the tree menu. The **CoS Map** window appears.
- 2 Select the desired DSCP and CoS Action mapping and click **Modify**. The **Modify IP SLA COS Map** dialog appears.
- 3 In the **Modify IP SLA COS Map** dialog select the desired **Action Index** for the DSCP Index.
- 4 Click **Modify** and then **Close**. The modified CoS map appears in the **CoS Map** window of the **Modify IP SLA Configuration** dialog box.
- 5 To view the settings for an individual CoS map. Select the desired CoS map and click **View**. The **View IP SLA COS Map** dialog appears.

Viewing the Real time IPSLA statistics

Real-time statistics represent minimum, maximum, average, and current values over the current 15 minute polling period based on data collected for each polling intervals. For example, if the polling interval is configured for 60

seconds, the real-time statistics display the data compiled from the latest 15 60-second polling intervals contained in the current polling period.

These statistics can be displayed individually or collectively for a specific IP address or for all configured paths.

To view the real time IPSLA statistics:

- 1 To view the real-time statistics for path or CoS queue, first, enable bulk statistics for the device in the **Modify Device Configuration** dialog box.
- 2 Next, right-click a device and select **Manage Bulk Statistics**.
The **Configure Bulk Statistics** dialog box appears.
- 3 Select an uplink card (Slot 1 or Slot 2) in the **Select card** box.
- 4 Click the **IP SLAs** tab.
- 5 In the IP SLAs dialog box, select the ip address, CoS index action, and index value you want to gather statistics on. You can select multiple paths by clicking and dragging.
- 6 Select the type of statistics to gather in the right side pane.
- 7 Click **Apply**.
- 8 To export the statistics, right-click in the **Bulk Stats** window and select **Export Data**.

For details on these settings, see the online help.

Viewing the historical IPSLA statistics

View the historical statistics individually or collectively based on IP address, CoS action index, and index value of a 15 minute interval. Historical statistics are displayed for the latest 24 hour period or a specified 15 minute interval within the latest 24 hour period.

To view the historical IPSLA statistics:

- 1 To view the historical statistics for IPSLA, first, enable bulk statistics for the device in the **Modify Device Configuration** dialog box.
- 2 Next, right-click a device and select **Manage Bulk Statistics**.
The **Configure Bulk Statistics** dialog box appears.
- 3 Select an uplink card (Slot 1 or Slot 2) in the **Select card** box.
- 4 Click the **IP SLAs** tab.
- 5 In the IP SLAs dialog box, select the ip address, CoS index action, and index value you want to gather statistics on. You can select multiple paths by clicking and dragging.
- 6 Select the type of statistics to gather in the right side pane.
- 7 Click **Apply**.

- 8 Right-click a device, select **View Historical Statistics**, the **Historical Statistics on the Device** window appears.
- 9 Select an entry combined with the desired IP address, CoS action index, and index value in the **Node** box. Enter the from time and to time. Click **Apply**. The defined historical statistics appears in the window.

Configuring IP on a bridge

IP on a bridge allows users to put an IP address on a bridged VLAN for managing the device. This VLAN can be used to manage multiple MALC/MXK/XPs or other SLMS devices. MXK supports six IP on a bridge can be created on per device.

When configuring Voice or PWE on an EAPS, must use the IP address that enter for the IP on a bridge interface. The ipobridge must be a TLS bridge for PWE and Voice configuration. The creation of the ipobridge interface with TLS bridge type on the VLAN automatically creates a TLS bridge interface on the VLAN. Asymmetric bridge interfaces (uplink, downlink, intralink, rlink) may not be used on the same VLAN as TLS interfaces.

Create an IP on a bridge interface, use the following procedure.



Note: The logical port interface for IP on a bridge *must* be IpOnBridge Proxy: 1-1-6-0 (on MALC or XP), or IpOnBridge Proxy: 1-a-6-0 (on MXK) for correct transmission of IP packets.

- 1 Right-click a device and select **Manage IP**.
The **IP Configuration Manager** dialog box appears. If there are any IP connections configured on the device, they are displayed here.
- 2 Click **Add**. The **Add IP Interfaces** dialog box appears.
- 3 Select a **IpOnBridgeProxy Port** interface by clicking on the Browse button. The **Select Physical** dialog box appears.
- 4 In the **Select Physical** dialog box, expand the device to the physicals level, and select **IpOnBridge Proxy: 1-1-6-0** on MALC or XP, or **IpOnBridge Proxy: 1-a-6-0** on MXK. Click **OK**.
- 5 In the **Add IP Interface** dialog box:
 - The **IpOnBridgeProxy Port** appears in the **Physical**.
 - Select the **Bridge Type** for the new interface (TLS or Downlink)
 - Enter the **VLAN ID** for the new interface
 - Enter the **IP Address** for the new interface
 - Enter the **Netmask** for the new interface.
 - Enter the **Broadcast Address** for the new interface.
 - Enter the **Address Mode** for the new interface (static or DHCP client).

- Specify if the **DHCP Server** is used for the new interface.
 - Select the **Multicast Control List** for the new interface.
 - Enter the **Max Number of Multicast Streams** for the new interface.
 - Select the **Tag Protocol Id** for the new interface.
 - Select the **Stag Id** for the new interface.
 - Enter the **TOS option** for the new interface.
 - Enter the **TOS Value** for the new interface.
 - Enter the **VLAN Class-of-Service** for the new interface.
 - Enter the **Stag COS** for the new interface.
 - Enter the **Ingress Filter ID** for the new interface.
 - Enter the **Egress Filter ID** for the new interface.
 - Click **Add**.
 - Click **Close**.
- 6 The newly added iponbridge port appears in the **IP Configuration Manager** dialog box.
 - 7 The newly added iponbridge port also appears in the **Manage Bridge Logical** dialog box.

Bridge configuration

Bridging involves configuring the NetHorizon to direct traffic based on Ethernet MAC addresses.

Topics:

[Overview](#)

[Configuring bridging](#)

[Modifying bridging logicals](#)

[Configuring bridge paths](#)

[Bridge filter groups and members](#)

[Viewing Bridge IGMP tables](#)

[Bridge template](#)

[External DHCP subnet template](#)

[Packet rule member template](#)

[Packet rule group template](#)

[IGMP Snooping with Proxy Reporting](#)

[IGMP DSCP](#)

[ADSL fall-back Mode for VDSL 2 card](#)

[Secure DHCP, Secure IP without DHCP](#)

[Multiple Spanning Tree Protocol \(MSTP\)](#)

[IPv6 bridges](#)

Overview

Asymmetrical and symmetrical bridges

The NetHorizon supports a variety of asymmetrical and symmetrical bridge interface types which enable different methods to learn, forward, and manipulate traffic.

The system automatically creates a bridge path with default values when creating a uplink, intralink, and TLS bridges.

- Asymmetrical bridges use three different bridge interface types:

- Uplinks

Uplinks are normally used for upstream traffic toward the Internet core.

Uplink bridge interfaces only work in conjunction with asymmetric bridge interface.

RSTP(802.1W) option on the uplink bridge, which is an evolution of the Spanning Tree Protocol (STP802.1D). STP links network segments and eliminates one of the difficulties of configuring bridge topologies — bridge loops. There still can only be one active path. Once RSTP is configured for a bridged network the Spanning Tree Algorithm (STA) analyzes the network and determines which links should be active or not. The STA defines the links by configuring the ports.

- Downlinks

Downlinks are normally used for downstream traffic toward the subscribers.

Downlink bridge interfaces only work in conjunction with asymmetric bridge interfaces.

- Intralinks

Intralinks are normally used for subtending other SLMS devices.

Intralink bridge interfaces only work in conjunction with asymmetric bridge interfaces.

- RLink

This is the enhance version of RSTP bridge (i.e Uplink bridge interface with RSTP option). With the RSTP rlink, instead of having a second redundant cloud link at each SLMS device in RSTP, it allows traffic to proceed through the other SLMS device, which has its own uplink bridge. In that case, those two devices are redundant to each other, if an active uplink fails on one device, the another device will provide backup uplink.

- MVR

Multicast VLAN Registration (MVR) allows video subscribers to share one multicast VLAN in the network while remaining in their own unique VLAN. MVR can send packets received from the multicast headend device on one MVR VLAN to one or more than one subscriber VLAN IDs.

In cases where the CPE devices have preconfigured VLANs or SLANs, the MXK supports VLAN translation, that is, the ability to translate preconfigured VLANs on the subscriber side to VLANs currently assigned on the network side.

In cases where devices upstream from the MXK expect SLAN IDs, SLAN IDs can be promoted from *tagged* downstream bridges to *staged* upstream bridges.

The range for translated VLAN IDs is 1-4090 (some VLANs are reserved).

MVR option in the bridge logical type means an MVR uplink. This bridge type is similar to an uplink but does not expect or handle unicast traffic. It mainly accepts multicast IP (video) traffic, and IGMP proxying is enabled by default.

- Symmetrical bridges use Transparent LAN service (TLS) and wire bridge interfaces.

- TLS

TLS bridge interfaces have the same behavior regardless of which ports are being bridged.

A TLS bridge interfaces only work in conjunction with other TLS bridge interfaces.

- Wire bridge interfaces

Wire bridge interfaces are a reserved TLS bridge, which have the same behavior regardless of the ports being bridged. When configuring wire bridges, the VLAN ID used on the two wire bridge interfaces is reserved for the entire device and cannot be used again. Wire bridges are confined to two bridge interfaces on a VLAN ID. Additional bridge interfaces on the VLAN ID cannot be added.

A wire bridge is only connected to another wire bridge in a two bridge interface configuration and reserves a VLAN ID for two ports for the entire system.

Untagged, tagged, and double tagged bridges

Bridges also utilize VLAN tagging for tagged and untagged traffic segregation. Packets which have a VLAN ID are tagged packets. Packets which have both a VLAN ID and a second tag, an SLAN ID are double-tagged (or also called s-tagged or Q in Q). If the packet does not have a VLAN ID or SLAN ID then the packet is untagged.

Based on the tagging there are three distinct cases:

- **Untagged bridging**
Untagged bridges forward traffic based on MAC addresses but do not further segregation traffic. Traffic is broadcast over the Ethernet port and is either accepted or rejected based on the destination MAC address. In other words, there is no VLAN tagging; all ports are learning and forwarding without restriction without broadcast suppression. Forwarding to a default port is not allowed.
- **Tagged bridging**
Tagged bridges forward traffic based on the logical VLAN ID number. This tagging allows the segregation of a single Ethernet network into multiple virtual network segments.
- **Double tagged bridging**
Double tagging expands the VLAN space in the Ethernet frame, so that you may further segregate traffic. The packet is differentiated by VLAN ID and SLAN ID. This second tag gives a whole other layer, so you can have VLAN 100 which may be a department in a global organization, and VLAN 100, SLAN 100 be one group within that department.

The packets which come into the SLMS device are untagged, tagged and double tagged. The tagged values will be from 1 to 4094.

VLAN packets are tagged, however that is half of the solution, the bridges to the destination, or more precisely, the bridge interfaces must be configured to accept packets.

Bridge filtering

The NetHorizon also supports bridge filtering (also known as packet rule records) so an open-ended number of filter settings can be configured for a bridge interface. The same filter settings can also be easily applied to multiple bridge interfaces.



Note: Bridge configuration record settings supersede the global filter settings set using the bridge-path add filter command.

VLAN/SLAN Translation

VLAN/SLAN Translation:

In situations when devices in the core network expect unique identifiers for each subscriber, and because subscriber configurations on the MXK can include large numbers of CPE devices with pre-configured VLAN IDs or VLAN/SLAN IDs, the MXK supports VLAN and SLAN translation from the subscriber to the MXK for VLAN/SLANs sent to the core network.

When creating a downlink bridge, after selecting **Double Tagged (ST)** as bridge type, and selecting **Translate** mode, you can specify the original VLAN/SLAN ID on the subscriber side to pass down to the CPE, and specify the translated VLAN/SLAN ID on network side to pass to the core network.

The range for translated VLAN IDs is 1-4090 (some VLANs are reserved).

The following **Bridge Logical on Device** dialog shows a downlink bridge configuration with VLAN translation and SLAN translation. This example creates a downlink bridge on a port on an Active Ethernet card. The original VLAN ID is 100, it will be translated to VLAN ID 1001; the original SLAN ID is 500, it will be translated to the SLAN ID 501.

SLAN Promotion:

When creating a Single Tagged (TG) type of Downlink bridge with VLAN translation, in cases where devices upstream from the MXK expect SLAN IDs, SLAN IDs can be promoted from *tagged* downstream bridges to *tagged* upstream bridges by selecting both **Translation** mode and **QinQ** mode.

The following **Bridge Logical on Device** dialog shows a downlink bridge configuration with VLAN translation and SLAN promotion. This example creates a downlink bridge on a port on an Active Ethernet card. The original VLAN ID is 100, it will be translated to VLAN ID 1001; the SLAN ID for network promotion is 500. **Note that the SLAN ID field can be displayed in Single Tagged (TG) bridge type only if you selected QinQ mode.**

Multicast VLAN Registration (MVR) for video configuration

Multicast VLAN Registration (MVR) allows video subscribers to share one multicast VLAN in the network while remaining in their own unique VLAN. MVR can send packets received from the multicast headend device on one MVR VLAN to one or more than one subscriber VLAN IDs.

In cases where the CPE devices have pre-configured VLANs or SLANs, the MXK supports VLAN translation, that is, the ability to translate pre-configured VLANs on the subscriber side to VLANs currently assigned on the network side.

In cases where devices upstream from the MXK expect SLAN IDs, SLAN IDs can be promoted from *tagged* downstream bridges to *tagged* upstream bridges.

MVR in the bridge logical type means an MVR uplink. This bridge type is similar to an uplink but only accept multicast IP (video) traffic, and IGMP proxying is enabled by default.

The following **Bridge Logical on Device** dialog shows an MVR uplink bridge configuration. This example creates a *tagged* MVR bridge with VLAN ID 2220 on an uplink Ethernet port 1-a-8-0 for all downstream multicast traffic.

The following **Bridge Logical on Device** dialog shows a downlink bridges configuration on the subscriber facing Ethernet ports for both MVR and video. This example creates a downlink bridge on 1-6-1-0 on an Active Ethernet Card, the VLAN ID is 2800, the MVR VLAN ID is 2220, the max number of multicast streams is 3.

Configuring bridging

1 Right-click a device and select **Manage Bridging**.

The **Manage Bridge Logicals** dialog box appears.

2 Click **Add** in the **Bridge Logical** portion of the dialog box. The Bridge Logical dialog box for adding a bridge appears.

3 To add a bridge logical:

- Enter **VPI** and **VCI** values.
- Click the check boxes of the desired physical ports. If multiple ports are selected, the specified configuration settings apply to all selected ports.
- When an ONT/ONU port is selected, **GPON Port ID** and **GPON traffic profile index** fields will be enabled.
- Select a **Transmit Traffic Descriptor** by clicking on the Browse button
- Select a **Receive Traffic Descriptor** by clicking on the Browse button
- Select **Encapsulation Type: Routed 1483** is used DSL routers; **Bridged 1483** (RFC 1483) is used with DSL bridges.
- Enter **Multicast Control List** for bridge video subscribers. An empty list allows bridge video uses to watch all channels.
- Enter **Max Number of Multicast Streams**. A number greater than zero enables the video bridge. For a video bridge, ensure the global bridge path settings on the uplink bridge for multicast aging and IGMP query interval are set properly. See [Configuring bridge paths](#).
- Set **IsPPPoA** to True to enable a PPPoA to PPPoE bridge.

The MALC/MxK supports PPPoA to PPPoE internetworking for connections to a Broadband Remote Access Server (BRAS) using a PPP tunnel. Upon detecting PPPoA traffic, device initiates a PPPoE session the Broadband Remote Access Server (BRAS). PPP traffic

between the CPE and the BRAS is tunneled over this PPPoE session. Device autosenses the type of PPPoA encapsulation as either VCMUX or LLC. Ensure the CPE is configured for PPPoA connections.

An inactivity timeout occurs when a lack of activity is detected on the PPPoA connection for 30-80 seconds, while upstream PPPoE packets are received. When this occurs, the PPPoE session is terminated.

- Select the desired template by selecting **Use Templates**, and clicking on the Browse button.
- Select the **Bridge Logical Type** and click **QinQ** for SLAN ID support. Q-inQ supports SLAN tags or ‘double-tagged’ Ethernet frames on a downlink bridge. When using SLAN tags, S-tag related options can be configured.
- Select the **Translate** for VLAN and SLAN ID translation.
- Select the **Translate** and click **QinQ** for SLAN promotion.
- Select the **Type: Single Tagged, Double Tagged, or Untagged**
- Enter a **VLAN_ID** (if necessary).
- Disable or enable **Increment VlanId** option.

This value is used when a bridge is being created on multiple ports at the same time. Without Increment VlanId checked, all bridges will be created with the same VLAN. With Increment VlanId checked, the VLAN will be incremented for every port.

- To configure secure DHCP, select **secure** option.
- Disable or enable **STP** option. Rapid Spanning Tree Protocol (RSTP, IEEE 802.1W) and MSTP are supported on the upstream interface on the MXK/MALC uplink cards. (Except for 1-a-1-0/eth on MXK or 1-1-1-0/eth on MALC. These ports are for inband management only.)
- **VLAN Class-Of-Service** indicates the value loaded into the COS field of the VLAN header when an untagged packet received on this interface is tagged (VLAN ID inserted) for bridging. Value range is 0 to 7. Default is 0.
- **Outgoing COS option** indicates whether to insert the VLAN COS bits on packets bridged through this interface. Disable means leaving any existing COS values unchanged. This is the default value. All means replacing the current COS values in all VLAN headers in tagged and untagged packets originating and transported through this device.
- For outgoing tagged packets, specifies the **Outgoing COS value** used to overwrite any existing COS value in the VLAN header. Value range is 0 to 7. Default is 0.
- Stag Protocol Id

- SLAN/S-tag Id means tagged with a known SLAN ID but unknown VLAN ID. SLAN IDs can be promoted from downstream bridges to upstream bridges or translated from the original SLAN if the subscriber traffic is already double-tagged.
- S-tag COS
- S-tag Outgoing COS option
- S-tag Outgoing COS Value
- **MVR Vlan ID** is used when creating a downlink bridge on a subscriber facing ethernet port to pass multicast video traffic, and this MVR ID must match that of the MVR uplink where the video traffic comes from.
- **Original VLAN ID (1..4090)** is used in VLAN translation. It passes all downstream traffic that is not multicast video. This is created on the downlink bridges on the subscriber facing ethernet ports.
- **Original SLAN ID** is used in SLAN translation when the subscriber traffic is double-tagged.
- Select to **Use Existing Packet Rules** or **Use Packet Rule Template** for ingress or egress interfaces.
- If using existing packet rules, the **Ingress Packet Rule Group Index** and **Egress Packet Rule Group Index** appear. Click on the Browse button to select one.
- If using packet rule template, the **Ingress Packet Rule Group Template** and **Egress Packet Rule Group Template** appear. Click on the Browse button to select one
- Specify the bridge **Name**.
- Click **Add**.

For details on the settings in this dialog box, refer to the online help.

Related topics:

[Adding an ATM cross connect on page 363](#)

[Adding IP interfaces on page 391](#)

Modifying bridging logicals

- 1** In the **Manage Bridge Logicals** dialog box, select the desired bridge and click **Modify**. The **Modify Logical Bridge Configuration** dialog appears with status options.
- 2** Modify the bridge admin status and name as desired.
- 3** Click **Identity** to display the bridge identification settings.
- 4** If this bridge is up and under control of RSTP or MSTP, the STP Bind tab will be displayed in the tree view. Click **STP Bind**s to display the STP bind profiles.

- a** Click **STP Binds** to display the STP bind profiles.
- b** To modify the STP port priority, highlight the STP bind and click **Modify**.
 - The **Modify STP Bind Configuration** dialog appears.
 - Bind Instance Id
The Bind Instance Id of 0 specifies RSTP. A Bind Instance Id > 0 indicates STP.
 - Port Priority
The Port Priority is used to specify the STP priority of this port. If all other STP packets parameters are the same, then the port priority value will be compared between STP ports. The port with the lowest port priority wins.
- c** Specify the desired port priority value and click **Modify**.
- d** Click **Close** to close the **Modify RTP Bind Configuration** dialog.
The new port priority value appears in the **Modify Logical Bridge Configuration** dialog.
- 5** Click **Bridge Logical Configurations** to display the bridge configuration settings.
- 6** The default settings for bridge interfaces are set based on the bridge type. They are greyed out in the Modify Logical Bridge Configuration window. You can only set those advanced bridge configuration settings when creating a bridge. Examples of advanced bridge configuration include:
 - In most configurations, **VLAN IDs** should be stripped for traffic destined to downlink interfaces and inserted for traffic destined for upstream interfaces. Downlink interfaces typically do not need to know the VLAN ID since they are on a single Ethernet. You can, however, specify that a downlink interface be tagged, or an uplink interface be untagged. You might want this if you are subrending SLMS devices and aggregating Ethernet traffic.
 - The **Strip & Insert** settings defines how VLAN tags are stripped and inserted as they traverse the ingress and egress of the MALC/MXK/XP. The untagged bridge set the strip & insert parameter to TRUE, the tagged bridge set the strip & insert parameter to FALSE. When the strip & insert parameter is set to true, the VLAN ID is stripped and inserted, when the strip & insert parameter is set to FALSE, the VLAN ID remains and is passed on untouched.
 - The **Send ARP Requests** enables ARP broadcast support. When a MALC/MXK/XP receives a broadcast frame it checks to see if it is an ARP protocol packet by looking up an IP address in a database which maintains learned IP addresses. If the packet is an ARP packet, the MALC/MXK/XP compares and filters the requested IP address with

the current forwarding table. When a match is found, the ARP broadcast is forwarded out the interface with the appropriate host. The host then replies to the ARP with a standard response. If a match is not found, the ARP is filtered and is dropped.

- The **Discard Non-ARP Broadcast Packets** enables the filtering that will not propagate broadcasts send from the upstream down to the MALC/MXK/XP. Ports configured as uplinks will send broadcasts upstream.
- The **IP Address Learning** enables/disables IP address learning on device.
- The **Custom DHCP** setting enables bridge interfaces to pass DHCP information independent of the **Discard Non-ARP Broadcast Packets** setting. Setting **Custom DHCP** to TRUE will cause that bridge interface to pass broadcast DHCP OFFER and ACK packets even though the **Discard Non-ARP Broadcast Packets** is set to TRUE.
- Select to **Use Existing Packet Rules** or **Use Packet Rule Template** for ingress or egress interfaces. It allows to enable/disable specific bridge filter groups for ingress or egress interface.
- If using existing packet rules, the **Ingress Packet Rule Group Index** and **Egress Packet Rule Group Index** appear. Click on the Browse button to select one.

If using packet rule template, the **Ingress Packet Rule Group Template** and **Egress Packet Rule Group Template** appear. Click on the Browse button to select one

- **VLAN Class-Of-Service** specifies the value loaded into the CoS field of the VLAN header when an untagged packet receiver on this interface is tagged(VLAN ID inserted) for bridging. Value range is 0 to 7, with the lowest priority being 0 and the highest priority 7. Default is 0.

On MALC, it supports four queues per physical interface, so frames with a 0 or 1 CoS value are put into queue number 1; 2 or 3 are mapped to queue number 2, 4 or 5 are mapped to queue number 3, 6 or 7 are mapped to queue number 4.

On MXK, it supports eight queues, so it is one-to-one mapping. For example, frames with a 0 CoS value are put into queue number 1, 1 are mapped to 2, 7 are mapped to 8.

- **Outgoing CoS option** specifies whether to insert the VLAN COS bits on packets bridge through this interface. Disable means leave any existing COS values unchanged. This is default value. ALL means replace the current COS values in all VLAN headers in tagged and untagged packets originating and transported through this device.

- **Outgoing CoS value** is for outgoing tagged packets. It specifies the value used to overwrite any existing COS value in the VLAN header. Value range is 0 to 7. Default value is 0.

- For SLAN tagging, the following fields are available:

Stag Protocol Id identifies the type of VLAN used. Typically set to 8100.

SLAN/S-tag Id specifies the SLAN ID to insert into the Ethernet frames.

S-Tag Strip&Insert specifies whether to strip and insert s-tag values in Ethernet frames received and transmitted on the bridge interface. When using SLAN tagging, this should be set to true.

S-Tag Outgoing COS Option enables/disables COS values for the SLAN tags.

S-Tag Outgoing COS Value sets the COS value associated with the SLAN tags.

- Configure the **bridge group index** to assign all instances of a given bridge filter to a specified interface.
- **Multicast control list** specifies which control lists to associate with this bridge. An empty list allows bridge video uses to watch all channels.
- **Max Number of Multicast Streams** enables video connections on the bridge. For a video bridge, ensure the global bridge path settings on the uplink bridge for multicast aging and IGMP query interval are set properly. See [Configuring bridge paths on page 415](#).
- **Is PPPoA** specifies the interface is PPPoA or not.
- **Flood Unknown** provides the ability to toggle the flooding of unknown unicast destination frames. When the parameter is set to True, the SLMS device always forwards frames with an unknown unicast MAC if the bridge is set for forward to unicast. when this parameter is set to False, the SLMS device always discards frames with an unknown unicast MAC if the bridge is set for forward to unicast. Any frame that does not find a match in the forwarding table will be discarded.

For uplink bridges, the default settings for this parameter is false.

- **Flood Multicast** allows the SLMS device to flood all multicast traffic received on a bridge out to all other ports in the VLAN. By default, this parameter is set to false for all bridge types except TLS and wire bridges.
- **Dynamic MAC filtering** enables/disables a dynamic MAC address filter on downlink bridges on the SLMS device, or on uplink bridges on the MXK. This filter blocks users with invalid MAC address.

- **Dynamic IP filtering** enables/disables a dynamic IP filter on downlink bridges to prevent users with a statically configured IP address from bypassing DHCP security enforcement. This filter blocks users from accessing the network using anything other than valid DHCP offered IP address.
- **DHCP MAC Learning** enables/disables MAC address learning on DHCP server.
- **DHCP IP Learning** enables/disables IP address learning on DHCP server.
- **MVR VLAN ID** is used when creating a downlink bridge on a subscriber facing ethernet port to pass multicast video traffic, and this MVR ID must match that of the MVR uplink where the video traffic comes from.
- **Original VLAN ID** passes all downstream traffic that is not multicast video. This is created on the downlink bridges on the subscriber facing ethernet ports.
- **Original SLAN ID** is used when the subscriber traffic is double-tagged.
- **Incoming COS Option** is used to enable or disable the COS replacement for single tagged. COS or SCOS replacement is the ability to overwrite COS or SCOS bits in Ethernet frames for traffic entering Active Ethernet cards and sending the configured COS value to the uplink. This feature is only supported on single slot Active Ethernet cards.
- **S-tag Incoming COS Option** is used to enable or disable the SCOS replacement for double tagged. COS or SCOS replacement is the ability to overwrite COS or SCOS bits in Ethernet frames for traffic entering Active Ethernet cards and sending the configured COS value to the uplink. This feature is only supported on single slot Active Ethernet cards.

7 Click one of the buttons.

- **Refresh** to update the data displayed.
- **Reset** to return to the originally displayed settings.
- **Modify** to apply the changes.
- **Close** to exit the dialog box.
- **Help** to display context-sensitive help.
- Enter a **Bridge Group Index** (if filtering has been configured and is required).
- Click **Add**.

For details on the settings in this dialog box, refer to the online help.

Related topics:

[Adding an ATM cross connect on page 363](#)

[Adding IP interfaces on page 391](#)

Configuring bridge paths

Bridge paths are required to connect downstream and upstream VLANs bridges.

The system automatically creates a bridge path with default values when creating a uplink, intralink, and TLS bridges.

The configurable parameters for the bridge-path that are relevant to TLS bridges are the Unicast Aging with a default of 3600, and the Flap Control with a default of *Allow learned MAC to move without a hold time*. Those parameters can be configured from the ZMS with the **Modify bridge path** dialog or **Add Bridge Path** dialog.

The default of *fast* indicates that as a MAC address comes into the system from one source and then is seen from another source, the MAC address table is purged from the first source and replaced with the second source without delay or restriction. If this behavior is not desired, the Flap Control mode can be configured to *Dis-allow learned MAC to move* or *Default*.

The default age of 3600 is how long a MAC address is held in the MAC table before it is purged. This time is configurable on TLS bridges.

The MCAST and IGMP Query Interval are not relevant to TLS bridges.

To configure bridge paths:

- 1 Right-click a device and select **Manage Bridging**.

The **Manage Bridge Logicals** dialog box appears.

- 2 Click **Add** in the Bridge Path portion of the **Manage Bridge Logical** dialog box. The Add Bridge Path dialog box for adding a bridge path appears.

- 3 Specify the desired bridge path settings:

- Select the path **Type**.
- Specify the desired **VLAN ID**.
- Specify the desired **S-tag ID**.
- Enter an **IP address** (if necessary).
- Enter a **Multicast Aging** time (if filtering has been configured and is required). Multicast Aging period in tenths of seconds for the specified VLAN. After the specified aging period is met, the VLAN address is deleted from the routing table. A value of 0 indicates that aging is turned off. Maximum value is 2147483647 tenths of seconds, which equates to approximately 2485.51 days. Usually, this value is more than twice of the IGMP query interval. For subscriber settings, see [Modifying bridging logicals on page 410](#).
- Select the desired **Flap Control** option.

Options are Default, Dis-allow learned MAC to move, Allow learned MAC to move after 60 second hold time, and Allow learned MAC to move without a hold time.

- Select the desired **Loop Prevention** option.

Options are None, Block Asymmetrical, Block Asymmetrical-Auto, Block All, Block All-Auto.

Bridge loop prevention can be configured on both asymmetrical and TLS bridges to resolve certain incorrect MAC address behaviors.

- a. When bridge loop behavior occurs and **Block Asymmetrical** is configured on the uplink bridge interface with VLAN ID, the system will block the downlink after detecting this incorrect MAC address behavior.

After the blocked bridge receives an offending MAC address, the system sends a MAJOR alarm that indicates a bridge was blocked to prevent a loop. This alarm displays the bridge interface and the offending MAC address.

In this case, the blocked bridge interface must be unblocked manually.

- b. When bridge loop behavior occurs and **Block Asymmetrical-Auto** is configured on the uplink bridge interface with VLAN ID, the system initiates a series of three cyclic monitoring checks to see if the bridge loop condition is resolved. If the bridge loop condition is resolved, the bridge interface is automatically unblocked and a bridge loop clear alarm is sent.

If the condition is not resolved, the MAJOR alarm is cleared and a CRITICAL alarm is sent. In this case, the blocked bridge interface must be unblocked manually.

- c. When bridge loop behavior occurs and **Block All** is configured on the VLAN ID of the TLS bridges, the system blocks the second TLS bridge and then sends a MAJOR alarm describing the second TLS bridge that saw the MAC address. The bridge is then blocked to prevent a loop.

In this case, the blocked bridge interface must be unblocked manually.

- d. When bridge loop behavior occurs and **Block Block-Auto** is configured on the uplink bridge interface with VLAN ID, the system initiates a series of three cyclic monitoring checks to see if the bridge loop condition is resolved. If the bridge loop condition is resolved, the bridge interface is automatically unblocked and a bridge loop clear alarm is sent.

If this condition is not resolved, the MAJOR alarm is cleared and a CRITICAL alarm is sent. In this case, the blocked bridge interface must be unblocked manually.

- e. **None** means loop prevention is disabled.

Note that blocked bridge interfaces must be unblocked by clicking **UnBlock** button in the **Modify Logical Bridge Configuration** dialog > **Status** window.

- Enter a **Unicast Aging** time for data bridges (if filtering has been configured and is required).
- Enter an **IGMP Query Interval (seconds)**. This number indicates both the query interval (how often (in seconds) IGMP query values are injected in the video stream. Usually, this value is less than one half the multicast aging period. For example, if the Multicast Aging is 150 seconds, the IGMP Query Interval could be 60. For subscriber settings, see [Modifying bridging logicals on page 410](#).
- Enable or disable **IGMP Join And Leave**. Enable or disable MALC/MXK/XP to send Join and Leave requests to the Multicast router.
- Enable or disable **IGMP Respond to Query**. Allow or not allow MALC/MXK/XP to send query reports to the Multicast router.
- Enter **IGMP Custom IP**. Enable the MALC/MXK/XP to send the custom IP address used for IP on a bridge instead of 0.0.0.0.
- Select **IGMP DSCP**. Specify the source IP and DSCP bits to use when sending IGMP packets to the network.
- Click **Add**.

A confirmation box appears verifying that the bridge path was successfully added.

For details on the settings in this dialog box, refer to the online help.

Related topics:

- 4 To modify a bridge path, select the desired path and click **Modify**.

The Modify Bridge Path Configuration dialog box appears.

- 5 Specify the desired bridge path settings:

- Enter a **Multicast Aging** time (if filtering has been configured and is required). Multicast Aging period in tenths of seconds for the specified VLAN. After the specified aging period is met, the VLAN address is deleted from the routing table. A value of 0 indicates that aging is turned off. Maximum value is 2147483647 tenths of seconds, which equates to approximately 2485.51 days. Usually, this value is twice of the IGMP query interval. For subscriber settings, see [Modifying bridging logicals on page 410](#).
- Select the desired **Flap Control** option.

Options are Default, Dis-allow learned MAC to move, Allow learned MAC to move after 60 second hold time, or Allow learned MAC to move without a hold time.

- Enter a **Unicast Aging** time for data bridges (if filtering has been configured and is required).
- Enter an **IGMP Query Interval**. This number indicates how often (in seconds) IGMP query values are injected in the video stream. Usually, this value is one half the multicast aging period. For subscriber settings, see [Modifying bridging logicals on page 410](#).
- Enable or disable **IGMP Join And Leave**. Enable or disable MALC/MXK/XP to send Join and Leave requests to the Multicast router.
- Enable or disable **IGMP Respond to Query**. Allow or not allow MALC/MXK/XP to send query reports to the Multicast router.
- Modify **IGMP Custom IP**. Enable the MALC/MXK/XP to send the custom IP address used for IP on a bridge instead of 0.0.0.0.
- Select **IGMP DSCP**. Specify the source IP and DSCP bits to use when sending IGMP packets to the network.
- Select **Force IGMPv2 Down** or **Force IGMPv2 Up** to disable or enable forced IGMPv2 on the network and the subscriber sides for the uplink bridge-path.
- Click **Modify**.

A confirmation box appears verifying that the bridge path was successfully added.

For details on the settings in this dialog box, refer to the online help.

Related topics:

- 6 To delete a bridge path, select the desired path and click **Delete**.

The selected bridge path is deleted.

Bridge filter groups and members

Bridge filter groups (also known as packet rule groups) can be configured to hold one or more bridge filter members (also known as packet rule members). Bridge filter members specify the filter type and value.

Packet-rule-records are typically assigned to bridge configuration groups on downlink bridge interfaces. Each packet-rule-record contains settings for type and value. The **Type** parameter in the **Packet Rule Group Configuration** dialog box specifies the variety of filter to be applied to the interface. The following filter types are supported:

- [Access Control List, page 419](#)
- [Rate Limit Discard, page 419](#)
- [Color Aware Rate Limit Discard, page 420](#)
- [Bridge Storm Detect, page 421](#)
- [Destination Mac Swap Static, page 422](#)

- [Dhcp Relay, page 423](#)
- [DscpToCos, page 424](#)
- [Forbid Oui, page 424](#)
- [Insert Option 82, page 424](#)
- [Insert PPPoE Vendor Tag, page 425](#)
- [Filter First Encapsulation Vlan, page 428](#)
- [Promote First Encapsulation Vlan, page 428](#)
- [Filter Second Encapsulation Vlan, page 428](#)
- [Promote Second Encapsulation Vlan, page 429](#)

To create the bridge filter groups and members with different filter types, refer to the following section:

[Configuring bridge filter groups and members, page 431](#)

Access Control List

Packet rule value contains the ACL. The Access Control List (ACL) filters allow you to block access or allow access based on the source MAC address, Destination MAC address or Ethernet type. The ACL filters are configured using packet rule records.

The ACL filtering options include

- allow/deny based on Ethernet types
- allow/deny based on destination MAC address
- allow/deny based on source MAC address

The ACL filtering is supported on:

- system with FE/GE or GE uplink/controller cards,
- the ingress upstream port of line cards only and does not block any traffic on egress port (towards the subscriber),
- downlink and TLS bridges.

Rate Limit Discard

The Rate Limit Discard (i.e. Color Blind Rate Limiting) is one of the two packet-based rate limiting options. The another option is Color Aware Rate Limit Discard.

Rate limiting on the MXK allows for two types of policing for both color blind and color aware rate limiting:

- Single rate (CIR)
- Dual Rate (CIR and PIR)

Single rate, allows service providers to provide customers services with limited bandwidth with the Committed Information Rate (CIR) as the committed rate and all traffic up to the CIR is guaranteed.

Dual rate limiting allows service providers to configure rate limitations based on two rates, the CIR and the Peak Information Rate (PIR). In this case, all traffic up to the CIR is guaranteed and all traffic above the PIR is discarded. Traffic between the CIR and the PIR is handled on a best effort basis.

Both single rate limiting and dual rate limiting are configured per VLAN ID.

After configuring an interface with rate limiting, the traffic rate is monitored and metered to verify conformity with an established contract. Non-conforming traffic is discarded, while conforming traffic passes through the interface without any changes. The MXK follows RFC 2697 and RFC 2698 for rate limiting.

The mode of the Rate Limit Discard packet rule is:

- Single and dual rate limiting color blind.
- Dual rate limiting is allowed on the egress only.
Color blind policing works on both the ingress and egress for single rate limiting.
- Rate limiting is performed on the interface without using the frame's Class of Service (CoS) by assuming that all packets of a flow are “uncolored” and are treated equally when in the range of the CIR.
- For color blind dual rate limiting, packets are treated equally up to the CIR and are treated on a best effort basis between the rates set by the CIR and the PIR.
- You can configure yellow markings on dual rate packet rules. In this case, a CoS value is inserted into packets that exceed the CIR.
- Color blind mode is most commonly used for a single service per VLAN.

Color Aware Rate Limit Discard

The Color Aware Rate Limit Discard is one of the two packet-based rate limiting options. The another option is Rate Limit Discard.

The mode of the Color Aware Rate Limit Discard packet rule is:

- Single and dual rate limiting color aware
- Rate limiting observes that the incoming packet flow is colored and each packet is marked green, yellow, or red to signify if a packet has high, medium, or low priority. The color field maps to the priority CoS value in tagged packets and the IP precedence ToS value in untagged packets.
- Color aware mode is most commonly used for multiple services on a single VLAN to ensure that the higher priority packets get through if there is bandwidth contention.



Note: Not commonly used except when performing advanced configurations.

Color aware bandwidth limiting is usually used when multiple services with different priorities are offered on a single VLAN. The colors green, yellow, and red are used for metering traffic and the colors correspond to CoS values that range from 0-7. You can set which colors correspond to which CoS value.

Color Aware Policing is based on the idea that upstream devices are policing and marking frames based on a set of rules. A green packet is well behaved. A yellow packet has misbehaved at some point so if there is a bandwidth congestion it should be dropped before a green frame. A red packet has violated a rule and should be dropped. This means that green packets are serviced first, then if there is enough room, the yellow packets are serviced. Red packets are always dropped.

Table 11 shows the default mapping of CoS value to color.

Table 11: Default Color to CoS values

CoS value	Color
7	green
6	green
5	green
4	green
3	yellow
2	yellow
1	yellow
0	yellow

Bridge Storm Detect

The Bridge Storm Detect packet rule record provides a way to analyze packets by capturing discarded packets when a certain threshold is reached and is configured only on the ingress of a bridge interface.

The packet rule will capture the first N packets after the target packets-per-second threshold is reached. Since all discarded packets are not captured, and there may be multiple interfaces with a broadcast storm, some packets on the first interface with a broadcast storm are captured, then some packets on the next interface with a broadcast storm are captured, and so on.

If you selected **Discard** in the **Discard Type** field, only the **Packets Per Second** field is set. It means that when the packets exceed the packets-per-second threshold, the overall traffic on the bridge will be limited.

If you selected **Discard and Alarm** in the **Discard Type** field, both the **Packets Per Second** and the **Consecutive Seconds** fields must be set. It means that when the packets exceeds the packets-per-second threshold over a configured number of seconds, the overall traffic on the bridge will be limited and a bridge storm alarm will be sent. When the bridge storm is cleared, a clearing alarm will be sent.

If you selected **Discard and Alarm and Block** in the **Discard Type** field, both the **Packets Per Second** and the **Consecutive Seconds** fields must be set. It means that when the packets exceeds the packets-per-second threshold over a configured number of seconds, the overall traffic on the bridge will be completely blocked and a bridge storm alarm will be sent. When the bridge storm is cleared, a clearing alarm will be sent. The Discard and Alarm and Block in the Bridge Storm Detect packet rule automatically configured the **Auto Enable Interval 1** to 300 seconds, the **Auto Enable Interval 2** to 600 seconds, the **Auto Enable Interval 3** to 1200 seconds. The first value indicates that the bridge will automatically unblock after 300 seconds (five minutes). The second value indicates that when the next bridge storm occurs, the bridge will unblock after 600 seconds (ten minutes), and after the third bridge storm detection, the bridge will unblock after 1200 seconds (20 minutes). After the third time, if the storm continues, the bridge remains blocked and must be unblocked manually.

Note that blocked bridge interfaces must be unblocked by clicking **UnBlock** button in the **Modify Logical Bridge Configuration** dialog > **Status** window.

If the card reboots, the captured packets are lost.

Destination Mac Swap Dynamic

For Destination Mac Swap Dynamic, packet rule value is greyed out and displayed as 00:00:00:00:00:00.

In Destination Mac Swap Dynamic option, the MALC/MXK/XP retrieves the MAC address of the next hop router to correctly swap into unicast frames through dynamic snooping DHCP ACK messages.

The MALC/MXK/XP snoops DHCP ACK messages received on the bridge interface that is configured as the default (VLAN or global bridge). The source MAC address from this frame is swapped into for frames received on interfaces configured for destination MAC swapping. This address is stored in the database and persists across reboots. When a new DHCP ACK message is received in the same VLAN, its source is checked, and if different, the newer MAC address is used.

This option requires that DHCP server services are used in the network and that the next hop router is the default router between the MALC/MXK/XP and the DHCP server.

Destination Mac Swap Static

After selecting Destination Mac Swap Static type, packet rule value represents a user-specified valid 6-byte hexadecimal MAC address.

When destination MAC address swapping enabled, this feature modifies the destination MAC address portion of unicast frames (Ethernet frames not using a multicast or broadcast destination MAC) that traverse the MALC/MXK/XP so that the destination MAC is changed to the MAC address of the next-hop IP gateway in the access network. This ensures that all frames in the access network are forwarded to the access router regardless of how the frame originated. Broadcast, multicast, and Ethernet frames with a destination MAC address of the next hop router are forwarded without MAC swapping.



Note: For MXK, destination MAC swapping is only supported on the uplink cards.



Note: Destination MAC swapping is not supported on TLS bridge. It is also not supported if the downlink traffic is PPPoE.



Note: Only one destination MAC swap packet rule can be configured per rule group.

In Destination Mac Swap Static option, the MALC/MXK/XP retrieves the MAC address of the next hop router to correctly swap into unicast frames through a static user-specified entry.

Dhcp Relay

Packet rule value contains the DHCP subnet group ID. If only the DHCP relay option is used, option82 information is displayed in hex format.

In DHCP relay scenarios, the MALC/MXK/XP serves as a DHCP relay agent that forwards broadcast DHCP discover and DHCP request packets to external DHCP server(s). It then forwards the unicast DHCP offer and DHCP ack/nak replies to the requesting DHCP host.

By default, DHCP broadcast messages cross the router interfaces. To solve the problem of DHCP broadcast messages on multiple subnets, the MALC/MXK/XP can be configured as a DHCP relay agent that communicates with DHCP server(s) and acts as a proxy for DHCP broadcast messages that need to be routed to remote downstream segments.

In DHCP relay mode, you can add, delete, modify the primary DHCP server or an alternate DHCP server. The alternate DHCP server can be added only the primary DHCP server contains IP address. The alternate DHCP server will be forwarded DHCP requests and DHCP discoveries as well as the primary DHCP server.



Note: When using the alternate DHCP server option, you should configure your DHCP servers in a mirrored configuration so they are communicating with each other and that both are not giving out the same address to different clients.

DscpToCos



Note: DSCP to COS (802.1p) mapping applies to all MXK cards.

Some network architectures require QoS prioritization at layer 2 and others at layer 3. In order to maintain QoS between Layer 2 Ethernet and Layer 3 IP protocols, the NetHorizon now supports mapping Differentiated Services Code Points (DSCP) to Classes of Services (CoS) as defined by IEEE 802.1p.

CoS is Layer 2 QoS marking mechanism and involves manipulating the Ethernet 802.1p tag. CoS uses 3 bits and therefore values can be anything from 0 to 7. DSCP involves manipulating the IP header info (specifically the ToS field). DSCP uses 6 bits and value range from 0 to 63. Therefore, the following standard mapping table can be used as a reference when provisioning DSCP to COS (802.1p). The default mapping values are shown in [Table 12](#).

Table 12: Default DSCP to CoS (802.1p) mapping

DSCP	0–7	8–15	16–23	24–31	32–39	40–47	48–55	56–63
CoS	0	1	2	3	4	5	6	7

Forbid Oui

Packet rule value contains a 3-byte hexadecimal vendor code used with the Forbid OUI to forbid access on the interface.

Insert Option 82

Packet rule value contains an identification text used with Insert option 82 to identify the DHCP host. When this option is specified, option82 information is displayed in standard text format. DHCP option 82 provides the means for a DHCP relay agent to insert circuit specific information into DHCP messages which are forwarded on to the upstream DHCP server. There are two sub-options for DHCP option 82 insert — Local ID and Remote ID.

Local ID is meant to provide information about the circuit which the request came in on. It is normally the port and interface information.

RFC 3046 describes possible uses of the Local ID field:

- Router interface number
- Remote Access Server port number
- Frame Relay DLCI
- ATM virtual circuit number
- Cable Data virtual circuit number

Remote ID is meant to provide information about the remote host end of the circuit, however in practice the sub-option usually contains information about the relay agent.

RFC 3046 describes possible uses of the Remote ID field:

- a "caller ID" telephone number for dial-up connection
- a "user name" prompted for by a Remote Access Server
- a remote caller ATM address
- a "modem ID" of a cable data modem
- the remote IP address of a point-to-point link
- a remote X.25 address for X.25 connections

Since both fields support textual insertions on the MALC/MXK/XP, please research RFC 3046 for further details regarding field format.

The MXK supports three ways to configure the Local ID and Remote ID for the **Insert Option 82** rule type:

The first is leaving the two fields blank for the default information.

The default information inserted into the packet during the DHCP discovery process is formatted as:

```
System 0_ip:IfName
```

The systemIP address is taken from the IP address configured in the **system 0** profile. If the IP address is not defined in the system 0 profile, *0.0.0.0* is inserted.

The second way is entering the information without macro defined strings. You can specify one field, or specify both the Local ID and Remote ID fields.

The third way is entering the macro defined strings. You can specify one field, or specify both the Local ID and Remote ID fields. Refer to the [Table 13](#) for the description of macro names and macro formats

Insert PPPoE Vendor Tag

PPP headend servers (also known as Broadband Remote Access Servers or BRAS) authenticate and manage predominately DSL customers. TR-101 defines information which is entered into the packets when creating Point to Point Protocol over Ethernet connection via an Intermediate Agent (PPPoE Intermediate Agent).

PPP sessions take place two ways on the Mxk, MALC, Raptor-XP-150A and MALC-XP-150A. First using PPPoE-IA, the PPP intermediate agent snoops PPPoE packets and inserts information as needed through user provisioning. The second way is when PPPoA is enabled, the XP converts PPPoA sessions that take place with the customer CPE, and initiates a PPPoE session with the BRAS.

When the Insert PPPoE Vendor Tag packet rule is entered both upstream and downstream ADSL line rate information is added into the PPPoE Active Discovery Initiation (PADI) and PPPoE Active Discovery Request (PADR) packets going to the server. This line rate information gives the headend BRAS system visibility to individual line rates important for bandwidth management.

The packet rule value contains the optional tag. This is a customized identification string to be inserted into the PADI and PADR packets.

The MXK supports three ways to configure the customized string for the **Insert PPPoE Vendor Tag** rule type.

The first is leaving it blank for the default information. The second one is entering the custom string without macro defined strings. The third one is entering the macro defined strings.

The second is entering customized string without macro defined strings, PPPoE behavior prepends as much text of the custom string as will fit in the field (from 0 to 48 characters) and the output text is truncated if required to fit into the **Optional Tag** field.

The third way is entering macro defined strings, the macro string including the information pulled in by the macro, are limited to 48 characters. The **Optional Tag** field could contain one or more macro names, for example: \$SystemName\$Shelf\$Slot\$Port.

This section discusses how to insert customized strings with the use of supported macro formats as shown in [Table 13](#). Note that the profiles mentioned in the table are CLI profile.

- When a dollar sign character is encountered, the text following the dollar sign is compared to [Table 13](#).
- If no match is found the dollar sign character is replaced with the text "Unknown".
- If a match is found the dollar sign character and the associated text is replaced by the text indicated.
- The macro name and abbreviations are both case sensitive.
- The \$macro strings may be imbedded in literal text. This text is copied to the output without change.
- The supported macro formats may be entered in the text as either \$macroname or \$abbreviation. Thus \$SystemName and \$NM give the same result, which is to substitute the system name from the **system 0** profile.

Some of the macros vary in effect depending on the value they are intended to display.

- \$Gem and \$Onu IDs are displayed or not depending on whether or not they have a non-zero value.

- \$Vlan displays -SLAN-VLAN if the SLAN is non-zero, -VLAN if the -SLAN is zero but the VLAN is non-zero, or nothing if they are both zero.
- \$VC displays -vpi-vci if either value is non-zero and nothing if they are both zero.



Note: Macro names are case sensitive.

Table 13: Supported macro formats for macro defined strings

Macro name	Abbreviation	Varies	Result
\$SystemName	NM	NM	sysname from the system 0 profile.
\$SystemIP	IP	No	ipaddress address from the system 0 profile.
\$IfName	IF	IF	ifName from the bridge IfTranslate profile.
\$Address	AD	No	<i>shelf-slot-port-subport-type</i> of the underlying physical interface. Where the interface is a GPON OLT interface the type is given as <i>gponport</i> and the subport is the GEM port.
\$Shelf	SH	No	Shelf (currently always 1).
\$Slot	SL	No	<i>slot</i> from the IfTranslate profile of the underlying physical interface.
\$Port	PT	No	<i>port</i> (see \$Slot).
\$SubPort	SP	No	<i>subport</i> (see \$Slot.) For GPON this is the GEM port
\$Gem	GM	Yes	-GEMPort (or nothing)
\$Onu	ON	Yes	-ONUnumber (or nothing)
\$Type	TY	No	Type (for GPON this is <i>gponport</i>).
\$Vlan	VN	Yes	-SLAN-VLAN (or -VLAN or nothing).
\$Svlan	SV	No	SLAN
\$Cvlan	CV	No	VLAN
\$Vc	VC	Yes	-VPI-VCI (or nothing)
\$Vpi	VP	No	-VPI
\$Vci	VI	No	-VCI
\$Null	NL	No	Nothing (used to change PPPoE handling of constant strings).



Note: For configurations with bridge intralinks or subtended MXK/MALC/XP devices, ensure that the PPPoE intermediate agent feature is enabled on only the subtended devices.

VLAN Encapsulation

VLAN encapsulation allows the device to add additional VLANs beyond double tagging on TLS bridge interfaces (Q-in-Q-in-Q or Q-in-Q-in-Q-in-Q) using the **Add Packet Rule Group Configuration** dialog box. Without VLAN encapsulation the device can configure two tags (Q-in-Q) per Ethernet frame using the **Bridge Logical on Device** dialog box.

The MXK implements Q-in-Q-in-Q (3Q) with packet rule records **Promote First Encapsulation Vlan** and **Filter First Encapsulation Vlan** on tagged TLS bridges. The packet rule promotes the third tag by inserting the tag to the network and stripping the tag to the access.

The MALC implements Q-in-Q-in-Q-in-Q (4Q) using packet rule records **Promote First Encapsulation Vlan** and **Filter First Encapsulation Vlan** to define the third tag (3Q), **Promote Second Encapsulation Vlan** and **Filter Second Encapsulation Vlan** to define the fourth tag (4Q). Not only can the third and fourth tags be promoted, but also be filtered, so that the frame with the specific third tag, or fourth tag would be the only tags accepted on that interface. To add third and fourth tags the first and second tags must already exist.

Filter First Encapsulation Vlan

To filter the third tag, use the packet rule record Filter First Encapsulation Vlan.

You can enter VLAN ID and TP ID for this packet rule.

Promote First Encapsulation Vlan

To promote the third tag, use the packet rule record Promote First Encapsulation Vlan.

You can enter VLAN ID, TP ID, and Class-Of-Service (COS) value for this packet rule.

Filter Second Encapsulation Vlan

To filter the fourth tag, use the packet rule record Promote Second Encapsulation Vlan.

You can enter VLAN ID and TP ID for this packet rule.

Promote Second Encapsulation Vlan

To promote the fourth tag, use the packet rule record Promote Second Encapsulation Vlan.

You can enter VLAN ID, TP ID, and COS value for this packet rule.

Requirements and restrictions for Q-in-Q-in-Q-in-Q in MALC

VLAN encapsulation provides for third and fourth tags, but do not change the way first tags (tagged vlan) and second tags (staged vlan slsn) operate. However there are a number of requirements and restriction which must be met when using VLAN encapsulation.

Requirements:

- VLAN encapsulation can only be assigned to a TLS bridge interface
- VLAN encapsulation can only be assigned to a bridge interface which is defined to receive double tagged packets, also known as **staged** in the **Bridge Logical on Device** dialog box. (You cannot have a third tag, or a third and fourth tag without having a first and second tag.)
- promote or filter for fourth tags requires the usage of third tags (You cannot have a fourth tag without a third tag).
- **Promote First Encapsulation Vlan** and **Filter First Encapsulation Vlan** cannot exist in the same packet rule group.
- **Promote Second Encapsulation Vlan** and **Filter Second Encapsulation Vlan** cannot exist in the same packet rule group.
- **Promote First Encapsulation Vlan** should only be used on an access (downstream) port.
- **Promote Second Encapsulation Vlan** should only be used on an (downstream) access port.
- **Filter First Encapsulation Vlan** should only be used on a upstream port.
- **Filter Second Encapsulation Vlan** should only be used on a upstream port.

Restrictions:

- Acceptable values for the third tag will be limited from 1 to 4094, and no wild card values are allowed. (The **vlanid** keyword in the **Add Packet Rule Group Configuration** dialog box for first encapsulation and second encapsulation is required and the value for **vlanid** is required.)
- Acceptable values for the fourth tag will be limited from 1 to 4094, and no wild card values are allowed. (The **tpid** keyword in the **rule add** command for first encapsulation or second encapsulation is optional. If the **tpid** keyword is omitted from the command, the default **tpid** will be **0x8100**. If the **tpid** keyword is in the command, then the value for **tpid** is required.)

- If a physical interface has a triple tag rule (added via a packet rule), then the 3Q value should not match the 1Q value (vlan) of any other single tag rule on any other physical interface.
- If a physical interface has a quad tag rule (added via a packet rule), then the 4Q/3Q tag value should not match the 2Q/1Q tag (slan/vlan) value of any other double tag rule on any other physical interface.
- When adding a triple tag rule on a set of TLS bridges, the 3Q tag value should be unique for this TLS set of bridges, for the shelf, regardless of the slan or vlan (second tag/first tag) values.
- When adding a quad tag rule on a set of TLS bridges, the fourth tag/third tag value should be unique for this TLS set of bridges, for the shelf, regardless of the slan or vlan (second tag/first tag) values.
- Use of wild cards on 1Q and 2Q tags (vlan and slan) with third and fourth tags (3Q and 4Q) limit the use of wild cards on staged bridge interfaces which do not have third and fourth tags on the same physical interface.

It's expected that an uplink will be a shared physical interface used by various unique (distinct) TLS or asymmetric set of untagged and tagged bridges. Triple and quad tagged bridges have higher priority when it comes to vlan id matching (filtering) over double tagged bridges, which can cause a situation where the staged bridge will become useless because the 4Q/3Q bridge interface will take priority. This situation affects wild cards on the vlan and slan of staged bridges.

Figure 12: QQQQ bridge interface interoperability with staged bridge interfaces

Note that wildcards will limit the number of bridge interfaces which can be on a physical interface.

- With two wild cards on a bridge interface with VLAN encapsulation, there can only be one bridge interface on that physical interface.
- With one wild card on a bridge interface with VLAN encapsulation there is one case where the vlan or slan will not match because the QQQQ bridge interface takes priority.
- With two wild cards on an staged bridge interface WITHOUT VLAN encapsulation and all tags in the bridge interfaces with VLAN encapsulation (no wild cards), all the staged frames will be accepted except those which match the 2Q/1Q of the QQQQ interface. QQQQ frames will only be accepted where all four tag IDs match when ingressing with 4 tags at uplink, or accepted where 2Q/1Q tag IDs match when ingressing with 2 tags at downlink.

Requirements and restrictions for Q-in-Q-in-Q in MXK

Rules for applying a **packet-rule record** for Q-in-Q-in-Q:

- The line cards for access on the MXK that support Q-in-Q-in-Q are:

- MXK-AEX20-FE/GE (single-slot)
- The uplink cards on the MXK that support Q-in-Q-in-Q are:
 - MXK-UPLINK-2X10G-8X1GE
 - MXK-UPLINK-8X1GE
 - MXK-UPLINK-4X1GE
- TLS is the only bridge type that supports the Q-in-Q-in-Q packet rules.
- Both the access facing and the network facing TLS bridges must be *staged* with matching VLAN and SLAN IDs.
- Valid VLAN and SLAN IDs are between 1-4094. Wildcard VLAN ID 0 is supported. Wildcards are not supported on the SLAN ID.
- The packet rules **Promote First Encapsulation Vlan** and **Filter First Encapsulation Vlan** cannot exist in the same **packet-rule-record** group.
See [Configuring bridge filter groups and members, page 431](#) for information on creating packet rules.
- The packet rules for Q-in-Q-in-Q can only be assigned on the ingress of the bridge interface.
- *promotefirstencapsulationvlan* can only be used on an access port.
- *filterfirstencapsulationvlan* can only be used on a uplink port.

Configuring bridge filter groups and members

To configure the bridge filtering group and its member(s), perform the following tasks:

- 1 In the Manage Bridge Logicals dialog box, click the **Bridge Filtering** tab.
The **Manage Bridge Logicals** dialog box appears with the bridge filtering options.
- 2 To add a packet rule group, click **Add** in the **Packet Rule Group** portion of the dialog box. The **Add Packet Rule Group Configuration** dialog box for adding a bridge filter appears.
- 3 Specify the desired packet rule group and member settings. The specified group will be created along with the specified member.
 - a Specify the bridge filter group name in the **Group Name** field.
 - b Select the desired member filter type from the **Type** pull-down menu and complete the corresponding parameters:

Insert Option 82

Local ID — Specify the information about the circuit which the request came in on. It is normally the port and interface information.

Remote ID — Specify the information about the remote host end of the circuit, however in practice the sub-option usually contains information about the relay agent.

Dhcp Relay

Subnet Group Index — Click browse button to select the subnet group index.

Add DHCP Server Configuration dialog — Click **Add** button that appears to the right of the **Subnet Group Index** field to open the **Add DHCP Server Configuration** dialog. Specify the DHCP server information then click **Add** button.

Note the following requirements for DHCP relay while configuring the **Add DHCP Server Configuration** dialog:

- The external DHCP server must be configured to assign addresses on the same subnet as the floating IP address used by the remote device.
- The external DHCP server must be configured with a static route for the remote device's subnet back to the NetHorizon on which the relay agent is running. (The DHCP server will send DHCP unicast packets to the relay agent's address.)
- A separate DHCP server can be specified per subnet.
- The Alternate External Server only can be added if the External Server contains an address.

Insert PPPoE Vendor Tag

Optional Tag — A customized identification string. It can be empty, a customized string without macro defined string, or a customized string with macro defined string.

Forbid Oui

MAC Address Prefix — A 3-byte hexadecimal vendor code used with the Forbid OUI to forbid access on the interface.

Rate Limit Discard

Rate (in kbps) — Specify the Committed Information Rate (CIR) for color blind rate limit discarding. The average rate guaranteed for a virtual circuit. If the actual rate goes above the CIR the packets will be dropped.

Peak Rate(in kbps) — Specify the Peak Information Rate (PIR) for color blind rate limit discarding. The peak rate in which traffic above this rate is discarded and traffic between the CIR and PIR is handled on a best effort basis. It is used for dual rate limiting.

Committed Burst Size (in bytes) — The maximum data rate that the circuit will attempt to carry. After you specified the Rate, system will calculate the Committed Burst Size for optimal performance.

Extended Burst Size (in bytes) — The maximum data rate that the circuit will attempt to carry. After you specified the Rate, system will calculate the Extended Burst Size for optimal performance.

Yellow Priority —Specify the value for the yellow packets. When the parameter is not configured, yellow packets are untouched. The range is 0-7. It is used for dual rate limiting.

Color Aware Rate Limit Discard:

Rate (in kbps) — Specify the Committed Information Rate (CIR) for color aware rate limit discarding. The average rate guaranteed for a virtual circuit. If the actual rate goes above the CIR the packets will be dropped.

Peak Rate(in kbps) — Specify the Peak Information Rate (PIR) for color aware rate limit discarding. The peak rate in which traffic above this rate is discarded and traffic between the CIR and PIR is handled on a best effort basis. It is used for dual rate limiting.

Committed Burst Size (CBS), Extended Burst Size (EBS) — The CBS is the maximum data rate that the circuit will attempt to carry. The EBS is maximum data rate that the circuit will attempt to carry. The values for CBS and EBS are caculated by the system and are varied based on the value assigned in Rate field:

- 1) rate (strictly) less than 1Mbps: CBS=65536, EBS=100000
- 2) rate less (or equal) to 6Mbps: CBS=120000, EBS=130000
- 3) rate less (or equal) to 10Mbps: CBS=200000, EBS=200000
- 4) rate (strictly) larger than 10Mbps: CBS=400000, EBS=400000

Yellow Priority —Specify the value for the yellow packets. When the parameter is not configured, yellow packets are untouched. The range is 0-7. It is used for dual rate limiting.

High Priority —Packets are marked according to the colors that correspond to CoS values. See [Table 11](#). For dual rate limiting.

Low Priority —Packets are marked according to the colors that correspond to CoS values. See [Table 11](#). For dual rate limiting.

Destination Mac Swap Static:

Destination MAC Address — Specify a valid 6-byte hexadecimal MAC address in the Destination MAC Address field.

Destination Mac Swap Dynamic:

Group Name — Specify the bridge filter group name.

Destination MAC Address — This field is greyed out and displayed as 00:00:00:00:00:00.

ACL deny:

Value — Specify the ACL deny filtering based on Ethernet types, destination MAC address, or source MAC address. Here are some examples for the values: all, dstmac *IPaddress*, srcmac *IPaddress*, ethtype pppoedata, ethtype pppoedisc etc.

ACL allow

Value — Specify the ACL allow filtering based on Ethernet types, destination MAC address, or source MAC address. Here are some examples for the values: all, dstmac *IPaddress*, srcmac *IPaddress*, ethtype pppoedata, ethtype pppoedisc.

– **DSCP to COS**

Dscp Index— Select the Dscp index from the selection dialog. The default DSCP to CoS (802.1) mapping could be viewed in the **Modify Device Configuration** dialog > **DscpToCos** window. You can also change the mapping in the **DscpToCos** window as desired and save it to Dscp index 1. There is only one Dscp index. DSCP to COS mapping and packet rule applies to all MXK cards.

– **Bridge Storm Detect**

Discard Type— If you selected **Discard** in the **Discard Type** field, only the **Packets Per Second** field is set. It means that when the packets exceed the packets-per-second threshold, the overall traffic on the bridge will be limited.

If you selected **Discard and Alarm** in the **Discard Type** field, both the **Packets Per Second** and the **Consecutive Seconds** fields must be set. It means that when the packets exceeds the packets-per-second threshold over a configured number of seconds, the overall traffic on the bridge will be limited and a bridge storm alarm will be sent. When the bridge storm is cleared, a clearing alarm will be sent.

If you selected **Discard and Alarm and Block** in the **Discard Type** field, both the **Packets Per Second** and the **Consecutive Seconds** fields must be set. The range for **Consecutive Seconds** field is 5 to 30 seconds. It means that when the packets exceeds the packets-per-second threshold over a configured number of seconds, the overall traffic on the bridge will be completely blocked and a bridge storm alarm will be sent. When the bridge storm is cleared, a clearing alarm will be sent.

The **Discard and Alarm and Block** in the **Discard Type** field automatically set **Auto Enable Interval 1** parameter to 300 seconds, **Auto Enable Interval 2** parameter to 600 seconds, and **Auto Enable Interval 3** parameter to 1200 seconds (five minutes). After the third time, if the storm continues, the bridge remains blocked and must be unblocked manually.

Note that blocked bridge interfaces must be unblocked by clicking **UnBlock** button in the **Modify Logical Bridge Configuration** dialog > **Status** window.

– **Promote First Encapsulation Vlan**

VLAN ID— The third tag to be promoted by inserting it to the network TLS bridge.

TP ID— The Ether Type value are 0x8100 and 0x9100, with 0x8100 as the default.

COS Vlaue(0..7)— The CoS value for the packet rule.

– **Filter First Encapsulation Vlan**

VLAN ID— The third tag to be stripped going to the access TLS bridge. This VLAN ID of the third tag must match the VLAN ID of the **Promote First Encapsulation Vlan** packet rule record.

TP ID—The Ether Type value are 0x8100 and 0x9100, with 0x8100 as the default .

– **Promote Second Encapsulation Vlan**

VLAN ID— The fourth tag to be promoted by inserting it to the network TLS bridge.

TP ID— The Ether Type value are 0x8100 and 0x9100, with 0x8100 as the default.

COS Vlaue(0..7)— The CoS value for the packet rule.

Filter Second Encapsulation Vlan

VLAN ID — The fourth tag to be stripped going to the access TLS bridge. This VLAN ID of the fourth tag must match the VLAN ID of the **Promote Second Encapsulation Vlan** packet rule record.

TP ID— The Ether Type value are 0x8100 and 0x9100, with 0x8100 as the default.

c Click **Add**.

The packet rule group and member are added. The packet rule group index must be assigned to the bridge interface during bridge configuration.

d Click **Help** to access the online help.

e Click **Close** to exit the dialog.

- 4 To remove a packet rule group, select the desired group and click **Delete**.
- 5 To add additional members to a group, select the desired group and click **Add** in the **Packet Rule Member** portion of the dialog box. The **Add Packet Rule Member Configuration** dialog box appears with the member options. The group name is grayed.
 - Select the desired member filter **Type**.
 - Input / select the desired member filter values.
 - Click **Add**.
The bridge member is added to the selected group.
 - Click **Close** to exit the dialog.
 - Click **Help** to access the online help file.
- 6 Click **Modify** to change group name or member settings.
- 7 Click **Delete** to remove the selected member.

For details on the settings in this dialog box, refer to the online help.

Viewing Bridge IGMP tables

The bridge IGMP table is used to access the IGMP data for bridges when IGMP is in proxy mode and the IGMP status must be obtained from the linecards. It contains the IGMP multicast data information for a bridge.

- 1 Right-click a device and select **Manage Bridging**.
The **Manage Bridge Logicals** dialog box appears.
- 2 Select any bridge in the **Bridge Logical** portion of the dialog box. The Bridge IGMP tables along with the Bridge Paths of this bridge appear.
- 3 The Bridge IGMP table returns the following MAC addresses along with other pertinent information:
 - IP address
This field shows the IGMP Multicast IP address.
 - VLAN ID
This field shows the IGMP VLAN identifier. Maximum value is 4090.
 - SLAN ID
This field shows the IGMP SLAN identifier. Maximum value is 4090.
 - Host MAC address
This field shows the MAC address of end device receiving multicast packets.
 - Multicast MAC address

This field shows the IGMP Multicast MAC address.

- Timer

This field shows the count down timer before IGMP entry ages out.

Bridge template

ZMS supports bridge template.

Note that any customer-defined bridge templates will need to be edited and the **Bridge Type** field set to the correct bridge type. This editing of customer-defined bridge templates should be done after the upgrade is complete, and before creating new bridges using those templates. Again, this only need to be done to bridge templates which the customer has created. The default bridge templates will continue to work without requiring a change.

Adding a bridge template

To create a bridge template in the ZMS server, perform the following task:

- 1 Select **Tools > Configure Templates**.

The **Template Configuration** dialog box appears.

- 2 Right click **Bridge Templates** and select **Add**.

The **Add Logical Bridge Configuration** dialog box appears.

In the **Add Logical Bridge Configuration** dialog box, specify the desired values.

- 3 When finished, click **Add**.

External DHCP subnet template

ZMS supports external DHCP subnet template.

When creating the DHCP relay type of packet rule member template, the external DHCP subnet template must be specified.

Adding a DHCP subnet template

To create a DHCP subnet template in the ZMS server, perform the following task:

- 1 Select **Tools > Configure Templates**.

The **Template Configuration** dialog box appears.

- 2 Right click **External DHCP Subnet Templates** and select **Add**.

The **Add External DHCP Server Configuration** dialog box appears.

- 3 In the **Add External DHCP Server Configuration** dialog box, specify the desired values for the following fields:

Template Name — The name of the template, it will appear in the template selection dialog boxes.

Description — Brief description of the template.

Name — Enter a unique name for the DHCP subnet

External Server — IP address of the external DHCP server to be used for this subnet.

Alternate External Server — IP address of the alternate external DHCP server to be used for this subnet. It only can be assigned if external server field contains IP address.

Subnet Group — Specify the number of the DHCP subnet group this pool is a member of. A value of 0 (default) indicates not a member of any DHCP group.

- 4 When finished, click **Add**.

Packet rule member template

ZMS supports packet rule member template.

When creating or modifying a packet rule group template, the packet rule member template must be specified.

Adding a packet rule group member template

To create a packet rule group member template in the ZMS server, perform the following task:

- 1 Select **Tools > Configure Templates**.

The **Template Configuration** dialog box appears.

- 2 Right click **Packet Rule Member Templates** and select **Add**.

The **Add Packet Rule Member Configuration** dialog box appears.

- 3 In the Add Packet Rule Member Configuration dialog box, enter the template name and description. Select the desired member filter type, and then input/ select the desired member filter values.

If you select **Dhcp Relay** type, you can click the browse button to open the **Select Template** dialog. Select the desired external DHCP server template in the **Select Template** dialog, and click **OK**

Holding down the Shift key to select multiple templates.

- 4 When finished, click **Add**.

Packet rule group template

ZMS supports packet rule group template.

When creating or modifying a bridge, you can select existing packet rule group IDs or packet rule group templates.

If a packet rule group template is selected for a bridge, device searches all the existing packet rule group to see if a matching packet rule exists. If it does not, the device will automatically create a corresponding packet rule group and assign a index to the bridge.

Adding a packet rule group template

To create a packet rule group template in the ZMS server, perform the following task:

- 1 Select **Tools > Configure Templates**.

The **Template Configuration** dialog box appears.

- 2 Right click **Packet Rule Group Templates** and select **Add**.

The **Packet Rule Group Template Configuration** dialog box appears.

- 3 In the Packet Rule Group Template Configuration dialog box, specify the desired values for the following fields:

Template Name — The name of the template, it will appear in the template selection dialog boxes.

Description — Brief description of the template.

Packet Rule Group Name — Enter a unique name for the packet rule group.

Packet Rules In Group — Click the browse button to open the **Select Template** dialog. Select the desired packet rule member template in the **Select Template** dialog, and click **OK**.

Holding down the Shift key to select multiple templates.

- 4 When finished, click **Add**.

IGMP Snooping with Proxy Reporting

IGMP snooping applies to bridged video. Enabling IGMP snooping reduces traffic between the MALC/MXK/XP and the upstream multicast headend device. IGMP snooping with proxy reporting also supports the following:

- Solicited or unsolicited query reports.
- Ability to configure the MALC/MXK/XP to send queries to hosts; by default the NetHorizon does not.
- Queries are sent only to hosts that have sent a join request.
- Compliance with rfc4541 regarding IGMP forwarding and data rules.
- Information table is available during redundant uplink card switchovers.
- Membership reports on downlink bridges are not forwarded.

- When join requests are received without a leave, it is assumed that the set top box is watching both channel.
- IGMP snooping supports existing Max Video Streams and Multicast Control List functionality.
- Using the IP on a bridge IP address when a join request is sent to the upstream multicast headend device.

Join and leave requests

For IGMP snooping without proxy reporting enabled, join requests from downstream hosts are simply forwarded by the MALC/ MXK/ XP to the multicast headend device. For IGMP snooping with proxy enabled, join requests from downstream hosts are not forwarded by the MALC/ MXK/ XP to the multicast headend device in the network, but are tracked by the MALC/ MXK/ XP in an information table where hosts are organized into a group.

When a host sends a leave request that is the last leave request of the group, the MALC/ MXK/ XP terminates the leave request from the host and originates a new leave request and sends it to the multicast headend device in the network. All leave requests, regardless of whether they are the last leave request of the group, or any earlier leave requests, are terminated on the MALC/ MXK/ XP.

In this way, the multicast headend device starts and stops video transmission by processing requests sent directly from the MALC/ MXK/ XP and not from downstream hosts. Proxy is when the MALC/ MXK/ XP sends join and leave requests to the network and snooping is when the MALC/ MXK/ XP monitors the join and leave requests from hosts to the MALC/ MXK/ XP.

Enabling IGMP snooping with proxy reporting and custom IP address

To enable IGMP snooping with proxying in the **Add Bridging Path** dialog box, perform the following tasks:

- 1 Right-click a device and select **Manage Bridging**.
The **Manage Bridge Logicals** dialog box appears.
- 2 Click **Add** in the **Bridge Path** portion of the **Manage Bridge Logical** dialog box. The Add Bridge Path dialog box for adding a bridge path appears.
- 3 Specify the desired bridge path settings:
 - Select the path **Type** to VLAN Address.

- Enter a **Multicast Aging** time (if filtering has been configured and is required). Multicast Aging period in tenths of seconds for the specified VLAN. After the specified aging period is met, the VLAN address is deleted from the routing table. A value of 0 indicates that aging is turned off. Maximum value is 2147483647 tenths of seconds, which equates to approximately 2485.51 days. Usually, this value is more than twice of the IGMP query interval.
- Select the desired **Flap Control** option.
Options are Default, Dis-allow learned MAC to move, Allow learned MAC to move after 60 second hold time, or Allow learned MAC to move without a hold time.
- Enter a **Unicast Aging** time for data bridges (if filtering has been configured and is required).
- Enter an **IGMP Query Interval** (seconds). The number indicates both the query interval (how often IGMP query values are injected in the video stream) and membership report interval. Usually, this value is less than one half the multicast aging period.
- Enable **IGMP Join And Leave** to enable MLC/MXK/XP to send Join and Leave requests to the Multicast router.
- Enable **IGMP Respond to Query** to allow MLC/MXK/XP to send query reports to the Multicast router.
- Enter **IGMP Custom IP**. Enable the MLC/MXK/XP to send the custom IP address used for IP on a bridge instead of 0.0.0.0.
- Click **Add**.

A confirmation box appears verifying that the bridge path was successfully added.

- 4 To modify IGMP snooping settings, select the desired path and click **Modify**.

The **Modify Bridge Path Configuration** dialog box appears.

- 5 Specify the desired bridge path settings. And click **Modify**.

IGMP DSCP

This section describes IGMP DSCP and includes:

- [IGMP DSCP overview, page 442](#)
- [Default IGMP IP address and Custom IGMP IP address, page 443](#)
- [Configuring IGMP DSCP and IGMP proxy reporting and IGMP IP address, page 443](#)

IGMP DSCP overview

The bridge-path can be used to specify the source IP and DSCP bits to use when sending IGMP packets to the network. The source IP is required by some routers to uniquely identify the origin of IGMP packets. The DSCP bits prioritize the IGMP packets through the edge/core network. The value range is from 0 to 63. See [Table 14](#) for common DSCP core values.

To specify IGMP DSCP value on a bridge path of an uplink bridge, use the IGMP DSCP field in the **Modify Bridge Path Configuration** dialog box, and make sure IGMP Join and Leave and IGMP Respond to Query fields are enabled.

Table 14: common DSCP code values

String	Value
10(af11)	Mark packets with AF11 dscp (001010)
12(af12)	Mark packets with AF12 dscp (001100)
14(af13)	Mark packets with AF13 dscp (001110)
18(af21)	Mark packets with AF21 dscp (010010)
20(af22)	Mark packets with AF22 dscp (010100)
22(af23)	Mark packets with AF23 dscp (010110)
26(af31)	Mark packets with AF31 dscp (011010)
28(af32)	Mark packets with AF32 dscp (011100)
30(af33)	Mark packets with AF33 dscp (011110)
34(af41)	Mark packets with AF41 dscp (100010)
36(af42)	Mark packets with AF42 dscp (100100)
38(af43)	Mark packets with AF43 dscp (100110)
8(cs1)	Mark packets with CS1(precedence 1) dscp (001000)
16(cs2)	Mark packets with CS2(precedence 2) dscp (010000)
24(cs3)	Mark packets with CS3(precedence 3) dscp (011000)

Table 14: common DSCP code values (Continued)

String	Value
32(cs4)	Mark packets with CS4(precedence 4) dscp (100000)
40(cs5)	Mark packets with CS5(precedence 5) dscp (101000)
48(cs6)	Mark packets with CS6(precedence 6) dscp (110000)
56(cs7)	Mark packets with CS7(precedence 7) dscp (111000)
0(default)	Mark packets with default dscp (000000)
46(ef)	Mark packets with EF dscp (101110)

Default IGMP IP address and Custom IGMP IP address

When IGMP proxy is enabled on a static uplink bridge, the default source IP address in the Ethernet packet sent from the bridge is 10.10.10.0. In certain cases there may be a need to replace 10.10.10.1 with a custom Ethernet IP address. For example when a router in the network has implemented Reverse Path Forwarding and expects an IP address in the subnet of the router or when different IP addresses in the same subnet are inserted for different SLMS devices for the purposes of debugging.

By using the **IGMP Custom IP** field in the **Modify Bridge Path Configuration** dialog box, you can configure the MXK to send a custom IP address or a default IP address used in proxy on the bridge path along with IGMP DSCP for IGMP priority to the network.

Configuring IGMP DSCP and IGMP proxy reporting and IGMP IP address

After creating the uplink bridge, use the **Modify Bridge Path Configuration** window to enable IGMP proxy to pass video traffic and configure DSCP priority in IP packets for JOIN and LEAVE requests to the network, and you can configure the MXK to send a custom IP address used in proxy on the bridge path along with IGMP DSCP for IGMP priority to the network, otherwise IGMP proxy sends 10.10.10.1.

- 1 Right-click a device and select **Manage Bridging**.
The **Manage Bridge Logicals** dialog box appears.
- 2 Click **Add** in the **Bridge Logical** portion of the **Manage Bridge Logical** dialog box. The **Bridge Logical on Device** dialog box for adding a bridge appears.
- 3 In the **Bridge Logical on Device** window, create an *tagged* uplink bridge on a n Ethernet port, designate a VLAN ID.

The default bridge path is created with IGMP proxy disabled. This bridge path is displayed in the **Bridge Path** portion of the **Manage Bridge Logicals** dialog box.

- 4 Select this bridge path, and click **Modify** in the **Bridge Path** portion of the **Manage Bridge Logical** dialog box. The **Add Bridge Path** dialog box appears.
- 5 In the **Modify Bridge Path Configuration** window:
 - Enable the IGMP proxy by selecting Enabled for both **IGMP Join and Leave** field and **IGMP Respond to Query** field.
 - Select the **igmpDSCP** sets the DSCP priority for IGMP messages to the network.
 - Specify **IGMP Custom IP** sends a custom IP address. To revert to sending the default IP address of 10.10.10.1, enter 10.10.10.1.
- 6 Click **Modify**, then click **Close**.

ADSL fall-back Mode for VDSL 2 card

The 24-port VDSL2 card supports ADSL2+ fallback to provide interoperability with different xDSL CPEs and to support existing networks as well as new Packet Transfer Mode (PTM) networks.

ADSL2+ fallback in PTM mode

Not designating a VPI/VCI range (i.e. the values in the VPI and VCI fields are 0) when configuring a bridge interface on a VDSL2 port means that when ADSL2+ fallback is invoked, all VLANs will operate in PTM mode.

The following bridge configuration puts ADSL2+ fallback in PTM mode.

ADSL2+ fallback in ATM mode

Designating a VPI/VCI range (36 to 1024) when configuring a VDSL2 bridge interface on a VDSL2 port means that when ADSL2+ fallback is invoked, all VLANs will operate in ATM mode within the designated VPI/VCI range.

The following bridge configuration puts ADSL2+ fallback in ATM mode.

Secure DHCP, Secure IP without DHCP

The secure bridge (also called secure DHCP) feature saves MAC and IP information from a DHCP message exchange, and only allows traffic from the device with that IP address on the bridge. Traffic from a different device with the same IP is blocked.

The secure IP without DHCP configure static IP and MAC information as well as the DHCP (dynamic) method. This update allows customers who use

static addresses instead of DHCP to take advantage of the secure bridge feature.

Case 1: Configuring secure DHCP

Enable secure DHCP settings on downlink bridges, subscriber facing TLS bridges, and GPON ports to prevent a user with a statically configured IP address from bypassing DHCP security enforcement. This filter blocks users from accessing the network using anything other than the valid DHCP offered IP address.

To enable secure DHCP settings on bridges in ZMS, you can either select a bridge template with the keyword **DynamicSecure** or select **secure** keyword when creating bridges in the **Bridge Logical on Device** dialog box.

That bridge template has the format as:

*<bridge type>***DynamicSecure***<tagged mode>*

bridge type could be Downlink or TransparentLAN

tagged mode could be DoubleTagged, SingleTagged, Untagged.

After selected a bridge template for the secure DHCP, the settings in the following fields in the **Bridge Logical on Device** dialog box will be changed automatically.

Table 15: Bridge settings for secure DHCP bridge templates

Fields	Values
Dynamic MAC Filtering	Enabled
Dynamic IP Filtering	Enabled
DHCP MAC Learning	Enabled
DHCP IP Learning	Enabled

Case 2: Configuring secure static MAC + IP

This filter blocks users from accessing the network using anything other than the valid user statically configured MAC or IP address.

To enable secure static settings on bridges in ZMS, select a bridge template with the keyword **StaticMACnIPSecure** when creating bridges.

After selected a bridge template for the secure static, the settings in the following fields in the **Bridge Logical on Device** dialog box will be changed automatically.

Table 16: Bridge settings for secure static bridge templates

Field	Value
Dynamic MAC Filtering	Enabled

Table 16: Bridge settings for secure static bridge templates

Dynamic IP Filtering	Enabled
DHCP MAC Learning	Disabled
DHCP IP Learning	Disabled

Case 3: Configuring secure static MAC

This filter blocks users from accessing the network using anything other than the valid user statically configured MAC address.

To enable secure static settings on bridges in ZMS, select a bridge template with the keyword **StaticMACSecure** when creating bridges.

After selected a bridge template for the secure MAC, the settings in the following fields in the **Bridge Logical on Device** dialog box will be changed automatically.

Table 17: Bridge settings for secure static MAC bridge templates

Field	Value
Dynamic MAC Filtering	Enabled
Dynamic IP Filtering	Disabled
DHCP MAC Learning	Disabled
DHCP IP Learning	Disabled

Case 4: Configuring secure static IP

This filter blocks users from accessing the network using anything other than the valid user statically configured IP address.

To enable secure static settings on bridges in ZMS, select a bridge template with the keyword **StaticIPSecure** when creating bridges.

After selected a bridge template for the secure IP, the settings in the following fields in the **Bridge Logical on Device** dialog box will be changed automatically.

Table 18: Bridge settings for secure static IP bridge templates

Field	Value
Dynamic MAC Filtering	Disabled
Dynamic IP Filtering	Enabled
DHCP MAC Learning	Disabled
DHCP IP Learning	Disabled

Multiple Spanning Tree Protocol (MSTP)

This section covers the implementation of MSTP on the NetHorizon:

- [MSTP overview, page 447](#)
- [MSTP instances, page 447](#)
- [MSTP port role, page 447](#)
- [MSTP port state, page 448](#)
- [Plan the VLAN mapping for MSTP, page 449](#)
- [Configure MSTP uplinks on two MXKs in a MSTP network for load balancing, page 451](#)

MSTP overview

Multiple Spanning Tree Protocol (MSTP) on the MXK includes both IEEE 802.1S Multiple Spanning Tree Protocol (MSTP) and IEEE 802.1w Rapid Spanning Tree Protocol (RSTP). MSTP allows the grouping of VLANs to be mapped to multiple spanning tree instances (forwarding paths)

RSTP (Rapid Spanning Tree Protocol) on the MXK is configured per interface even when multiple VLANs are configured on the interface. This means that if four VLANs are configured on an interface on a port which is the active root port, and a loop is detected on just one of the VLANs, the entire port is blocked and all the data is switched to the alternate port which changes from a blocked state to become the active root port.

MSTP on the MXK differs from RSTP in that MSTP is configured on the VLAN and not on the interface. Therefore, when a fault is detected on an instance, only that VLAN is put into a blocked state and traffic is forwarded to a forwarding path.

MSTP allows multiple forwarding paths for data traffic and enables load balancing. Using MSTP also improves the fault tolerance of the network because a failure in one instance (the forwarding path) does not affect other instances (forwarding paths).

MSTP instances

Multiple Spanning Tree Instance(s) (MSTI) support groups of VLANs. Each MSTI can be configured with different root switches and different STP parameters.

MSTP port role

There are five port roles assigned by the STA to the port:

- ROOT: Root port

The root port is the closest to the root switch (also as root bridge. The root bridge is the only switch/bridge in the network that does not have a root port because it is the central bridge and root ports are defined by their relationship to the root bridge). The root port will receive the best BPDU from the root switch on a bridge.

For the STA to determine the root port for a device, five MSTP priority parameters are compared in the following priority sequence:

- 1) root bridge priority
- 2) root path cost
- 3) designated bridge priority
- 4) designated port ID
- 5) port priority

Only one MSTP port can be chosen as the root port per device. The port with the lowest value of MSTP priority parameters wins. If the first MSTP priority parameter have the same values on the ports, then the system will compare the next one, until it finds the root port.

- DSNT: Designated port

The designated port is the best port to send BPDU from the MSTP device to networked device.

- ALT: Alternate port

The alternate port is a port that is blocked because it is receiving more useful BPDUs from another bridge. The alternate port can change to an active root port.

- BKP: Backup port

The backup port is a port that is blocked because it is receiving more useful BPDUs from the same bridge it is on. A backup port is only providing connectivity to the same network segment, so it cannot change to a root port.

- N/A: Not applicable

It means MSTP is not in the functional state yet. It usually will appear right after system bootup.

- Master

To view MSTP port roles, use **bridge show** command or **stp-bridge show** command.

MSTP port state

IEEE 802.1w defines three port states in MSTP:

- DIS: MSTP discarding
- LRN: MSTP learning (a transitional state)

- FWD: MSTP forwarding (a normal operational state)

In operation there is no difference between a port with state DIS and one with state LRN as they both discard frames and do not learn MAC addresses. Ports which are blocking must keep transmitting BPDUs to retain maintain its port role and port state.

To show the MSTP port states, select **Status** in the tree view of the **View Logical Bridge Configuration** window, and use the **bridge state** field in that window.

Plan the VLAN mapping for MSTP

When implementing MSTP on the MXK, you must carefully design the network topology before creating MSTP bridges.

Configuring MXKs for MSTP

- 1 Configure the upstream routers.

The routers upstream from the MXK(s) must be configured to accept the data coming from the MSTP MXK bridges.

- 2 Create the MSTP network topology by configuring the MSTP profiles **stp-params 0** and **mstp-instance**.

The **stp-params 0** profile defines the MSTP region, the bridge priority, and the force version. There is just one **stp-params 0** file configuration for each device. The **stp-params 0** file for all devices in the same MSTP network *must* have the same MSTP region, bridge priority, and force version. This is because each MSTP bridge will reference the same parameter definitions in the **stp-params 0** file. To access the **stp-params 0** profile, right-click a device in the NetHorizon tree, then click **Modify**, in the tree view of the **Modify Device Configuration** window, select **STP Params Configuration**.

The user configurable parameters in the **stp-params 0** profile are *Name*, *Bridge Priority*, and *Force Version*.

Table 19: STP Params 0 profile parameters

Parameter	Description
Name	Field must be set to use MSTP, use the name of the bridge as a key.
Revision	This parameter is used if you are running MSTP only. The MXK does not currently support any revisions to MSTP, so revision 0 is default. Default: 0
Bridge Priority	The priority ID that will be advertised for this bridge. Must be a multiple of 4096. Default: 36864

Table 19: STP Params 0 profile parameters (Continued)

Parameter	Description
Force Version	The protocol to initiate with. 3- MSTP 2- RSTP 0- STP
Forward Delay	The delay used by STP bridges to transition Root and Designated ports to Forwarding. Default: 15
Hello Time	The interval between periodic transmissions of Configuration Messages by designated ports. We only support a hello time of 2 currently. Default: 2
Migrate Time	The initial value of the mdelayWhile and edgeDelayWhile timers. 3 is the only supported value for this timer. Default: 3
Hold Count	The transmit hold count is used by the Port Transmit state machine to limit transmission rate. Default: 3
Max Age	The maximum age of the information transmitted by the bridge when it is the Root Bridge. Default: 20

The **mstp-instance** profile binds the instance and the VLAN ID. An MXK can support up to fifty instances. When planning the MSTP network, the **mstp-instance** for every VLAN must be configured on each MXK in the network. This is because when a link in the MSTP network goes down, the state becomes blocked, and traffic is switched to the next MXK in the MSTP network in a forwarding state. That MXK must be configured to pass the traffic on the VLAN. To add or view the MSTP instance profile that binds MSTP instances with VLAN IDs on the device, select **MSTP Instance Profile** from the tree view of the **Modify Device Configuration** window.

The **stp-bind** profile is created by the system when the MSTP bridge is added. To view the binding between MSTP instance ID and Port Priority on each bridge, select **STP Bind**s from the tree view of the **View Logical Bridge Configuration** window. The port priority is used to specify the STP priority of this port.

Configure MSTP uplinks on two MXKs in a MSTP network for load balancing

Configure MSTP uplinks on the first MXK

Configuring the stp-params 0 profile on the first MXK

Each **stp-bridge add** command will reference the same **stp-params 0** profile on the first MXK.

The **stp-params 0** profile must match on all MXKs in the MSTP network.

- 1 View the existing **stp-params 0** profile.
To access the **stp-params 0** profile, right-click a device in the NetHorizon tree, then click **Modify**, in the tree view of the **Modify Device Configuration** window, select **STP Params Configuration**
- 2 Enter the **name** parameter, and set the **Bridge Priority** to a multiple of 4096, and set the **Force Version** parameter to 3 for MSTP.
- 3 Click **Modify**.

Configuring the mstp-instance profile on the first MXK

After designing the MSTP network, create **mstp-instance** profiles on the first NetHorizon for *each* VLAN ID in the MSTP network.

For this sample MSTP network, instance 1/100 provides the VLAN on the first NetHorizon and instance 2/200 provides the VLAN on the second NetHorizon. Both instances/vlans must exist on both NetHorizons for MSPT to function properly. Once an instance is defined, the packet can only travel that route.

- 1 In the **Modify Device Configuration** window, select **MSTP Instance Profile**.
- 2 Click **Add**, the **Add MSTP Instance Profile** window appears.
- 3 In the **Add MSTP Instance Profile** window, create **MSTP ID 1** with **VLAN 100**, click **Add**.

And create **MSTP ID 2** with **VLAN 200**, then click **Add**.

Configuring the uplink(s) on the first MXK

When configuring a MSTP network on more than one MXK, the connection between the MXKs is established by using the *rlink* keyword in the **stp-bridge add** command. The RSTP *rlink* creates the ring in the MSTP configuration that allows traffic to pass through a forwarding uplink bridge on the next SLMS device in the same MSTP network when a link on the first MXK goes down.

In this MSTP configuration, if a link on the first MXK goes down and the state of that link becomes blocked, the data path is switched to the next MXK with a forwarding data path.

- 1 Create the *rlink* on the first MXK with VLAN 100 and instance 1.

The mechanism for setting MSTP port priority occurs the first time the port and VLAN ID are declared in the MSTP bridge configuration.

- a Right-click a device, and select **Manage Bridging**.

The **Manage Bridge Logicals** dialog appears.

- b In the **Manage Bridge Logicals** dialog, click Add.

The **Bridge Logical on Device** dialog appears.

- c In the **Bridge Logical on Device** dialog, select uplink port 1-a-2-0/eth in the Select Physical Ports pane, and select RLink as bridge type, and specify VLAN ID 100, and then select MSTP Instance as 1.

- d Click **Add**.

- 2 Create the *rlink* on the first MXK with VLAN 200 and instance 2.

- a In the **Bridge Logical on Device** dialog, select uplink port 1-a-3-0/eth in the Select Physical Ports pane, and select RLink as bridge type, and specify VLAN ID 200, and then select MSTP Instance as 2.

- b Click **Add**.

Configure MSTP uplinks on the second MXK

Configuring the stp-params 0 profile on the second MXK

Each **stp-bridge add** command will reference the same **stp-params 0** profile on the second NetHorizon.

The **stp-params 0** profile must match on all MXKs in the MSTP network.

- 1 View the existing **stp-params 0** profile.

To access the **stp-params 0** profile, right-click a device in the NetHorizon tree, then click **Modify**, in the tree view of the **Modify Device Configuration** window, select **STP Params Configuration**

- 2 Enter the **name** parameter, and set the **Bridge Priority** to a multiple of 4096, and set the **Force Version** parameter to 3 for MSTP.

- 3 Click **Modify**.

Configuring the mstp-instance profile on the second MXK

After designing the MSTP network, create **mstp-instance** profiles on the second NetHorizon for *each* VLAN ID in the MSTP network.

For this sample MSTP network, instance 1/100 provides the VLAN on the first NetHorizon and instance 2/200 provides the VLAN on the second

NetHorizon. Both instances/vlans must exist on both NetHorizons for MSPT to function properly. Once an instance is defined, the packet can only travel that route.

- 1 In the **Modify Device Configuration** window, select **MSTP Instance Profile**.
- 2 Click **Add**, the **Add MSTP Instance Profile** window appears.
- 3 In the **Add MSTP Instance Profile** window, create **MSTP ID 1** with **VLAN 100**, click **Add**.

And create **MSTP ID 2** with **VLAN 200**, then click **Add**.

Configuring the uplink(s) on the second MXK

When configuring a MSTP network on more than one MXK, the connection between the MXKs is established by using the *rlink* keyword in the **stp-bridge add** command. The RSTP *rlink* creates the ring in the MSTP configuration that allows traffic to pass through a forwarding uplink bridge on the next SLMS device in the same MSTP network when a link on the first MXK goes down.

In this MSTP configuration, if a link on the first MXK goes down and the state of that link becomes blocked, the data path is switched to the next NetHorizon with a forwarding data path.

- 1 Create the *rlink* on the second MXK with VLAN 200 and instance 2.

The mechanism for setting MSTP port priority occurs the first time the port and VLAN ID are declared in the MSTP bridge configuration.

 - a Right-click a device, and select **Manage Bridging**.
The **Manage Bridge Logicals** dialog appears.
 - b In the **Manage Bridge Logicals** dialog, click **Add**.
The **Bridge Logical on Device** dialog appears.
 - c In the **Bridge Logical on Device** dialog, select uplink port 1-a-3-0/eth in the Select Physical Ports pane, and select RLink as bridge type, and specify VLAN ID 200, and then select MSTP Instance as 2.
 - d Click **Add**.
- 2 Create the *rlink* on the second NetHorizon with VLAN 100 and instance 1.
 - a In the **Bridge Logical on Device** dialog, select uplink port 1-a-2-0/eth in the Select Physical Ports pane, and select RLink as bridge type, and specify VLAN ID 100, and then select MSTP Instance as 1.
 - b Click **Add**.

Create MSTP redundant uplinks by configuring two bridges with the same VLAN ID on two different uplink ports with two different instances. Many VLANs can share the same instance.

The mechanism for setting MSTP port priority occurs the first time the port and VLAN ID are declared in the MSTP bridge configuration.

Once an instance is defined, the packet can only travel that route.

Configuring redundant MSTP uplinks

- 1 Create the first MSTP bridge and set the port priority by entering following parameters in the **Bridge Logical on Device** dialog:
Select uplink port 1-a-6-0/eth, select Uplink as bridge type, specify VLAN ID 100, and specify MSTP instance 1.
- 2 Create the redundant MSTP bridge by entering following parameters in the **Bridge Logical on Device** dialog:
Select uplink port 1-a-7-0/eth, select Uplink as bridge type, specify VLAN ID 100, and specify MSTP instance 2.
- 3 Create the another MSTP bridge redundancy and set the port priority by entering following parameters in the **Bridge Logical on Device** dialog:
Select uplink port 1-a-6-0/eth, select Uplink as bridge type, specify VLAN ID 101, and specify MSTP instance 1.
- 4 Create the redundant MSTP bridge by entering following parameters in the **Bridge Logical on Device** dialog:
Select uplink port 1-a-7-0/eth, select Uplink as bridge type, specify VLAN ID 101, and specify MSTP instance 2.

Configure MSTP uplinks for load balancing

Configuring MSTP uplinks for load balancing

- 1 Create the MSTP bridge and set the port priority by entering following parameters in the **Bridge Logical on Device** dialog:
Select uplink port 1-a-6-0/eth, select Uplink as bridge type, specify VLAN ID 200, and specify MSTP instance 1.
- 2 Create the nest MSTP bridge by entering following parameters in the **Bridge Logical on Device** dialog:
Select uplink port 1-a-6-0/eth, select Uplink as bridge type, specify VLAN ID 200, and specify MSTP instance 2.

IPV6 bridges

Added support in ZMS for MXK IPv6 bridging.

If the system is running IPv6, you will see the IPv6 type of IP addresses in the **bridge path** pane of the **Manage Bridge Logicals** window, and when you are adding a downlink secure static bridge, the **IPv6 Address** field will be available for configuration in the **Add Bridge Path** window.

Multicast control list configuration

Multicast control lists enable IP hosts to send packets to a single IP address that references a control list of multiple addresses. Multicast control lists contain a starting IP address, ending IP address, and increment value.

Devices use the Internet Group Management Protocol (IGMP) to discover whether neighboring devices are configured in multicast control lists.



Note: A multicast control lists contains one or more multicast control lists. A multicast control list contains one or more configured IP addresses. To add a multicast control list in the **Add Multicast Control List** dialog or modify an existing multicast control list in the **Modify Multicast Control List** dialog, the Precedence of the configured IP address must be a unique value in this multicast control list, otherwise the adding or modification operation will be rejected.

Topics:

[Configuring multicast control lists](#)

[Adding an ATM VCL to multicast map](#)

Configuring multicast control lists

- 1 Right-click a device and select **Manage Multicast Control Lists**.
The **Manage Multicast Control Lists** dialog box appears.
- 2 Click **Add** in the **Manage Multicast Control Lists** dialog, the **Add Multicast Control List** dialog box appears.
- 3 Click **Add** in the **Add Multicast Control List** dialog. The **Add Multicast Control List** dialog box with the multicast control list details appears.

Specify the following control list data:

- **Name** : The name of the multicast control list.
- **Start IP Address** and **End IP Address**: The IP address range. Note that IP addresses can not be more than 256.
- **Precedence**: The precedence value has to be unique in the multicast control list.
- **Increment**: The fixed increment of precedence value
- **List Type** : Multicast control list type.

Normal means join and leave when desired. This option is used for video.

Always On means always joined. This option is used for EBS, not for video.

Periodic means join and leave after task complete. This option is used to download the TV guide, not for video.

- 4 Click **Add** to configure the specified multicast control list.

The configured IP Addresses appear in the Add Multicast Control List screen.

The configured multicast control list appears in the Manage Multicast Control Lists screen

- 5 Click **Modify** in the **Manage Multicast Control Lists** dialog box to modify the settings of the selected multicast control list.

The **Modify Multicast Control List** dialog box appears with all the configured IP addresses in that multicast control list.

- 6 To modify the detail information on each IP address, select an IP address and click **Modify**. The **Modify Multicast Control List** dialog box with the multicast control list details appears.

- 7 Enter the desired changes and click **Modify**. The multicast control list changes are saved and appear in the **Manage Multicast Control Lists** screen.

Note when modifying precedence of the IP address, the value should be unique in the multicast control list.

- 8 Click **Delete** in the **Manage Multicast Control Lists** dialog box to remove the selected multicast control list.

Click **Close** to exit the dialog without creating the multicast control list.

Click **Help** to display the related help topic.

For details on the settings in this dialog box, refer to the online help.

Related topics:

[Adding IP interfaces on page 391](#)

Adding an ATM VCL to multicast map

An ATM VCL to multicast map creates a mapping between the ATM VCL and the multicast address space.

- 1 Right-click a device and select Modify.
- 2 Select the **Video Source Config** tab.
- 3 Click **Add**.

The **Add ATM VCL to Multicast Map** dialog box.

- 4 Click the browse button and specify an IP address.

5 Click **Add**.

Redundancy overview

Note the following about redundancy:

- Redundant cards must be installed in adjacent slots.
- For redundant systems, you must configure the physical interfaces on both the active and standby cards. In addition, you must manually keep the configuration of the physical interfaces on the active and standby cards in sync. For other types of configuration, such as ATM or voice connections, as configuration changes are made to the active card, the standby card is automatically updated.
- When a card is made redundant to an adjacent card, and the adjacent card is already part of a card group, the new card is added as a member of that group.
- When a card is made redundant to an adjacent card, and the adjacent card is not already part of a card group, a new card group is created and both cards are added as members to that group.
- If the user does not choose a redundant slot, no card group is created for that card.



Note: The redundancy group number assigned by ZMS may differ from the **card-group-id** set by the CLI.

How active and standby cards are selected

Weights are used to specify a preference for a particular card to become active. By default, all cards have the same weight.

When the cards boot up, they elect an active and a standby card based on their respective weights. If the weights are equal, the card in the lower numbered slot becomes active.

If an active card fails, the standby takes over and becomes active. Note that redundancy is non-revertive. That is, a previously active card does not become active when it starts up again.

When the standby card comes up, the active card copies over the configuration database, routing tables, and software binaries to the standby card. As configuration changes are made to the active card, the standby card is automatically updated.

How NetHorizon displays redundant cards

In the tree and graphical display, cards in a redundancy group are labelled with the same group number. The active card is labelled with the **A** (active) icon; the standby card is labelled with the **S** (standby) icon. In the tree display, when you select one redundant card, NetHorizon selects both cards in the redundancy group.

Related topics:

[Adding redundant MALC, MXK and Raptor cards on page 133](#)

[Modifying redundant MALC, MXK, or Raptor cards on page 134](#)

[Redundancy overview on page 457](#)

Automatic protection switching (MALC and Raptor only)

The MALC and Raptor supports Automatic Protection Switching (APS) when 2 cards are installed in the system to provide card-level redundancy for the optical interfaces. If, for any reason, an interface on the working (active) card goes down, the protection (standby) card becomes active. After a switchover, the working card is rebooted. Note that APS is non-revertive. That is, the working card in slot does not automatically become active again if it's no longer in a fault state. A manual switchover is required for the working card to become active again.

The system automatically creates the following profiles:

The MALC and Raptor supports 1+1 (compatible with 1:1), unidirectional and bidirectional APS.

- **Channel:** configures the APS channels. There are four APS channels on the system (two per card). There are two APS groups on the system.
- **Group:** configures the APS groups. There are two APS groups on the system.

The following table describes how OC3-C/STM1 cards and ports are assigned to APS groups and channels. These values cannot be changed.

Slot	Port	APS group	APS channel
1	1	1	1
2	1	1	0
1	2	2	1
2	2	2	0



Note: The APS protocol runs on the second OC3-c/STM1 card.

Configuring APS

To configure APS:

- 1 Verify both OC3-c/STM1 interfaces are configured identically, and both are active.
- 2 Verify that the working OC3-c/STM1 ports are connected to the working ports on the SONET switch and the protection OC3-c/STM1 ports are connected to the protection ports on the SONET switch.

- 3 Activate the APS channels for the APS groups:
- 4 Activate the APS groups.

Administration procedures

Topics:

[Managing Users](#)

[Changing your NetHorizon password](#)

[Locating the version number of the NetHorizon application](#)

[Logging out of NetHorizon](#)

[Displaying objects in group](#)

[Configuring audio alarm notification](#)

[Finding ATM VCLs and cross connects](#)

[Viewing alarm history](#)

[Viewing the audit log](#)

[Viewing the task log](#)

[Printing or exporting log entries](#)

[Printing or exporting configuration data](#)

[Filtering alarms](#)

[Adding notes to alarms](#)

[Displaying Inventory Manager](#)

[Updating Display from Database](#)

[Telnetting/ SSH to ZMS server](#)

Managing Users

NetHorizon enables user management through the Manage Active Users dialog. Users with administrative access can view user data, logout and de-activate other users.

Click **Tools > Manage Active Users**. The Manage Active Users dialog appears.

To logout/de-activate or logout users, select the desired users and click the Logout&Inactive or Logout button.

Logging out of NetHorizon

Click **File > Exit** (or click the close button icon in the upper right corner of the display window).

The NetHorizon application closes.

Changing your NetHorizon password

Initially the ZMS administrator defines your NetHorizon password.

- 1 Click **Tools > Change My Password** from the menu bar.
NetHorizon displays the **Change Password** dialog box.
- 2 Enter your current password in the **Current Password** box.
- 3 Enter a new password in the **New Password** and the **Confirm Password** boxes.
- 4 Click **OK**.

Locating the version number of the NetHorizon application

- 1 Click **Help > About NetHorizon**.
NetHorizon displays version number and copyright information.
- 2 To close the window, click **Close** (or click the close button icon in the upper right corner of the window).

Changing your NetHorizon preferences

Displaying objects in group

By default, NetHorizon displays objects in your group only. If you have permission to view objects in other groups, you can set preferences to also display other objects in the graphical display and the tree display. NetHorizon lists those other objects in the tree display in smaller-sized italic text.

If you change your preference from the default setting, NetHorizon changes your display for the current NetHorizon session only.

You can choose to have NetHorizon display the following objects in the tree display and the graphical display:

- Objects in all groups
 - Objects in your group only
- 1 Click **Tools > Preferences** from the menu bar.
NetHorizon displays the **Set User Preferences** dialog box.
 - 2 Set your **Show objects in my group only** preference:
 - Mark the checkbox to have NetHorizon limit objects in the tree display and the graphical display to those in your group only.

- Unmark the checkbox to have NetHorizon show objects in all groups the tree display and the graphical display.

3 Click **Apply and **Close**.**

Keep in mind that your preference reverts back to the default setting when you log out of NetHorizon.

Configuring audio alarm notification

NetHorizon enables you to configure audio alarm notification (beep). By default, audio alarm notification is turned off.

To configure audio alarm notification:

1 Select **Tools > **Preferences**.**

The Preferences dialog appears.

2 Click the **Turn On Alarm Beep and click **Apply**.**

The audio alarm (beep) notification is turned on.



Note: The user must have permissions to view alarms in the main window for the alarm beep feature to be available. See Tools > Configure Users.

Finding ATM VCLs and cross connects

To search a region, subregion, or a device to find ATM VCLs or cross connects:

1 Right click a device and select **Find.**

The **Find** dialog box appears.

2 Specify the search criteria:

For a simple search:

- a** Select a region, subregion, or device to search.
- b** Select the type of VCLs or cross connects to find.

For an advanced search

- a** Select a region, subregion or device to search.
- b** Select the type of VCLs or cross connects to find.
- c** Click the **Advanced Filter** tab.

The **Advanced Filter** dialog box appears. The search criteria are different depending on the objects you are searching for. You can enter some or all of the search criteria:

- For **All VCLs**, **AAL5 VCLs**, or **Other VCLs**: enter the VPI/VCI to find.

- For **AAL2 VCLs**: enter the VPI/VCI and the **Application ID** to find.
- For **VC Cross Connects**: enter the Name, the Admin Status, and the upstream and downstream VCLs.

3 Click Find.

The **Find** dialog box displays the VCLs or cross connects it has found. From here you can view, modify, or delete the object, or get statistics (for VCLs only).

Pinging ATM VCL endpoints

To ping ATM VCL endpoints:

- 1** Select the desired device and on the uplink card, navigate through the tree objects to locate the ATM VCL Endpoints folder under ATM interfaces.
- 2** Right-click the desired ATM VCL endpoint and from the menu choose the desired ATMping command.

The selected segment or end-to-end OAM F4/F5 loopback is performed and a Message box appears with the ping status.

Viewing alarm history

ZMS supports an Alarm History Viewer. This window allows the operator to view alarms that were generated by system events and/or traps. When an alarm has been cleared in the system, the operator still has the ability to view the alarm in the alarm history window.



Note: By default, the Alarm History Viewer holds up to 5,000 alarm log records. To modify the maximum number of alarm log records, change the **maxAlarmLogRecords** parameter in the FaultService.properties file.

This is the same information captured in the `/opt/weblogic/yyyy_mm_dd_alarm.log` on the server.

To access the Alarm History viewer, select **View > Faults > Alarm History**.

The Alarm History Viewer window appears.

- 3** To filter the displayed alarms, specify the desired filter criteria such as device, description, date/time, and severity levels and click **Retrieve Data**.

Related topics:

[Viewing the audit log on page 463](#)

Viewing the audit log

ZMS supports an Audit Log viewer. This window allows you to view the requests that were made to the ZMS server. These requests indicate the time of the request and the user name for each request. The audit log also contains records for when a new user was added to the system.



Note: The information displayed in the Audit Log viewer can be modified in the ADS.properties file (located in `/install_directory/lib/com/zhone/zms/properties`). Refer to the *ZMS Administrator's Guide* for more information.

This is the same information captured in the `/opt/weblogic/yyyy_mm_dd_ZMSAudit.log` on the server.

- 1 To access the Audit Log Viewer, select **Tools > Audit Log Viewer**.

The **Audit Log Viewer** dialog box appears.

- 2 Select the log to view and click **View File**.

The log appears in the display field. To browse through the logs, click the **Prior Day** or **Next Day** buttons.

- 3 Select a log entry to display the details for the log.

- 4 When finished viewing the logs, click **Close**.

Related topics:

[Viewing alarm history on page 462](#)

[Printing or exporting log entries on page 464](#)

Viewing the task log

ZMS supports a Task Log viewer. This window allows you to view the tasks that were performed to the ZMS server. The task types are ALL, Auto Discovery, Device Backup, ConfigSync, and Download Image. These logs indicate the start time or finish time, task type, status, and brief description for each task.



Note: The information displayed in the Task Log viewer can be modified in the ADS.properties file (located in `/install_directory/lib/com/zhone/zms/properties`). Refer to the *ZMS Administrator's Guide* for more information.

This is the same information captured in the `/opt/weblogic/yyyy_mm_dd_ZMSTask.log` on the server.

- 1 To access the Audit Log Viewer, select **Tools > Task Log Viewer**.

The **Task Log Viewer** dialog box appears.

- 2 Select the log to view, and select task type from the **Select Task Type** pull-down menu, and then click **View File**.

The task type could be: ALL, Auto Discovery, Device Backup, ConfigSync, or Download Image.

The log appears in the display field.

- 3 To browse through the logs, click the **Prior Day** or **Next Day** buttons.
- 4 Select a log entry to display the details for the log.
- 5 When finished viewing the logs, click **Close**.

Related topics:

[Viewing alarm history on page 462](#)

[Printing or exporting log entries on page 464](#)

Printing or exporting log entries

You can now export or print NetHorizon logs. The following types of logs support exporting and printing:

- Alarm log
- Alarm forward history log
- Alarm history log
- Audit log
- Task log
- Trap forward history log
- Trap history log

The following example shows how to print and export log entries for the audit log:

- 1 To access the Audit Log Viewer, select **Tools > Audit Log Viewer**.

The **Audit Log Viewer** dialog box appears.

- 2 Select the log to view and click **View File**.

The log appears in the display field. To browse through the logs, click the **Prior Day** or **Next Day** buttons.

- 3 Select a log entry or entries.



Tip: Select multiple entries by clicking and dragging the mouse or by holding down the CONTROL key and clicking.

- 4 Right click and select **Export Data** or **Print > As Text** or **Print > As Table**.

– If you chose to export the data, the **Data Export** dialog box appears.

From this dialog box, select whether you want a tab delimited file or a comma separated file, specify a path, then click **Export**.

- If you chose to print the file, specify whether you want to print the data as text or as a table. The print dialog box for your system will appear.

Printing or exporting configuration data

You can export or print lists of configuration data from NetHorizon. This includes cross connects, IP interfaces, and statistics.

- 1 From a dialog box that lists configuration data (for example, the IP **Configuration Manager**), select the rows of data you want to print or export.



Tip: Select multiple entries by clicking and dragging the mouse or by holding down the CONTROL key and clicking.

- 2 Right click and select **Export Data** or **Print > As Text** or **Print > As Table**.
 - If you chose to export the data, the **Data Export** dialog box appears. From this dialog box, select whether you want a tab delimited file or a comma separated file, specify a path, then click **Export**.
 - If you chose to print the file, specify whether you want to print the data as text or as a table. The print dialog box for your system will appear.

Filtering alarms

NetHorizon enables you to filter the alarms displayed in the alarm viewer dialog box. You can view alarms by any combination of the following criteria:

- Device
- Description
- Severity
- Time

To filter alarms:

- 1 Select **View > Faults > View Alarms**
The **Alarm Viewer** dialog box appears.
- 2 Click the filter button.
- 3 Enter the filter criteria. NetHorizon allows you to filter alarms based on multiple devices and severity levels as well as description, date, and other alarm criteria. The alarm filter settings also apply to new alarms that are received after the filter settings are set.
- 4 Click **Apply**.

Only the alarms that match the filter criteria are displayed.

Adding notes to alarms

NetHorizon enables you to add notes to the alarms for additional alarm clarification and description.

To add or view an alarm note:

- 1** Select the desired alarm in the Alarm Viewer.
A **N** appears in the Note column if a note has not been added to this alarm.
A **Y** appears in the Note column if a note has already been added to this alarm.
- 2** From the right-click menu choose **Alarm Notes**.
The **Alarm Note** dialog box appears.
- 3** Enter the desired note description and click **OK**.
A **Y** appears in the Note column to indicate the note has been added.

Displaying Inventory Manager

NetHorizon enables you to display inventory data for one or more specific devices. Detailed information is available for selected objects.

To display inventory data:

- 1** In the ZMS tree, select the desired devices for which to display inventory management data.
- 2** Select **Tools > Inventory Manager** from the menu bar.
The **Inventory Manager** dialog box appears with the data for the selected devices.
- 3** To display new data, click the **Retrieve Data** button.
- 4** To export data to a file that takes a .csv extension, click the **Export Data** button.
- 5** To print the displayed data, click the **Print** button.
- 6** To filter displayed data, enter the desired criteria and click the **Apply** button.
 - Module Name
 - Part Number
 - Software Version
 - Hardware Version
- 7** To view details of a device, double-click the device.
The **Inventory Details** dialog box appears.
- 8** Click the **Close** button to exit the dialog box.

Updating Display from Database

NetHorizon enables you to refresh the client's navigation tree with information from the database. It retrieves all information about the selected node and makes sure that the correct children exist under the selected node.

Update Display From Database is available on every type of node in the tree (Regions, Region, Sub-region, Device, Card, Physical, ATM etc.)

To update display from database:

- 1 In the ZMS tree, right-click the desired node for which to update display from database.
- 2 Select **Update Display from Database**.

Telnetting/ SSH to ZMS server

NetHorizon enables you to telnet or SSH to the ZMS server.

The SSH to ZMS server action invokes the following command:

```
c:/Program Files/putty/putty.exe
```

Note that if putty is not installed on the PC at the above location, the command will fail.

- 1 To telnet to the ZMS server, select **Tools > Telnet to ZMS Server** from the menu bar.
- 2 To SSH to the ZMS server, select **Tools > SSH to ZMS Server** from the menu bar.

Running diagnostics

Diagnostic test information is useful for detecting and addressing network problems.

Topics:

[TAC Metallic Line Tests](#)

[Single-End Loop Test \(SELT\)](#)

[Dual-End Loop Test \(DELT\)](#)

[T1 BERT](#)

[802.3ah Ethernet OAM loopback](#)

TAC Metallic Line Tests

The TAC cards provide metallic test access to verify the local loop conditions, perform line testing on distant regions of the physical copper cable connecting the MALC/MXK and remote devices. It can assess breakages in the cable, identifying the following data:

- **Distance.** Identifies the amount of distance between the MTAC card and the location of the break or open that occurred on the copper cable.
- **Shorts.** Identifies the port to which a cable containing an electrical short is connected.
- **Unbalance.** Identifies if one side is longer between the tip and the ring, creating an unbalance in the connection.
- **Metallic noise.** Identifies any impairments on the cable that indicate an interruption on the ring.

Metallic loop testing

The TAC cards support metallic loop testing for T1, POTS, and DSL loops, providing preventive measures for potential line breaks.

TAC cards support external test sets. External test sets supported include Tollgrade, Harris/Fluke, and Teradyne 4-Tel components.

The MTAC/RING-ENH card also provides internal look-out line testing.

Internal look out line test

Internal line testing is supported by the MTAC/RING-ENH card. With its own integrated test set, the MTAC/RING-ENH card in each shelf can perform test out session without the external test set.

Cards supporting look-out test access

The MTAC cards provide access to external test equipment through an RJ45 connector for look-out test access. All ADSL-48, POTS, ULC, and 2-wire DSL cards support look-out test access. The following table provides examples of common instances of these card types.

Table 20: Examples of common cards supporting look-out test access

Card Type	Example
ADSL-48	MALC-ADSL+POTS-PKT-48A/M-2S
	MALC-ADSL+POTS-TDM/PKT-48-2S
	MALC-ADSL+SPLTR-48A/M-2S
	MALC-ADSL-48A
	MALC-ADSL-BCM-48A
	MALC-ADSL-BCM-48B
DSL	MALC-ReachDSL-24
EFM	MALC-EFM-SHDSL-24
	MALC-EFM-T1/E1-24

Table 20: Examples of common cards supporting look-out test access

Card Type	Example
POTS	MALC-POTS-GBL-TDM/PKT-24 (ULC)
	MALC-POTS-TDM/PKT-48
SHDSL	MALC-SHDSL-48
	MALC-G.SHDSL-24
	MALC-EFM-SHDSL-24
	MALC-EFM-SHDSL-24-NT
	MALC-EFM-SHDSL-24-NTP
VDSL2	MALC-VDSL2-24

The test relays can be controlled by the command line interface (CLI) and Zhone Management System (ZMS). Test relays on the POTS, DSL, or ULC cards can connect any POTS pair to an RJ45 metallic test access port on the MTAC card using the back plane to allow test access to any POTS, DSL, or ULC line.

View line state before testing

Before initiating a test for a POTS port, you usually need to verify a call is active on the line and the line is idle. You can view the current state of the line in the **Hook Status** field, this field only appears after selecting a POTS port for the loop testing.

Viewing the line state for a POTS port

To view the line state for a POTS port:

- 1 Right-click the MTAC card in the ZMS tree and select **MTAC Access**. The MTAC Access Test dialog appears.
- 2 Select the desired POTS port, the **Hook Status** field appears.

MTAC-FC / MTAC-RING card line testing

To perform metallic tests on MTAC/RING-FC card or MTAC-RING card:

- 1 Right-click the MTAC/RING-FC or MTAC-RING card in the ZMS tree and select **MTAC Access**. The MTAC Access Test dialog appears.
- 2 Select the desired port and test mode.
 - Port
 - Test Mode
 - None, Look Out, Look In, Bridge

3 Click **Apply**.

MTAC-ENH card internal line testing

To perform MTAC/RING-ENH card internal line tests:

- 1 Right-click the MTAC/RING-ENH card in the ZMS tree and select **MTAC Access**. The MTAC Access Test dialog appears.
- 2 Select the desired port, test mode, and test id. Click **Start**.
 - Port
 - Test Mode
None, Look Out.
 - Test Id

[Table 21](#) lists the detailed description of the Test IDs that supported by MTAC/RING-ENH card.

Table 21: MTAC/RING-ENH Internal Line Tests

Test ID	Description
Three Element Capacitance Test	This test measures tip-to-ground (T-G), ring-to-ground (R-G), and tip-to-ring (T-R) capacitance and impedance.
Three Element Resistance Test	This test measures tip-to-ground (T-G), ring-to-ground (R-G), and tip-to-ring (T-R) resistance.
Abort	Terminate the running test.
DC Feed Self-Test	This procedure verifies that the test hardware can drive currents into a load and measure the voltage across a load.
DC Loop Resistance Test	This test measures DC loop resistance using one of the following algorithms: Forward/Reverse Polarity or Offset Compensation.
Distance To Open Test	This test estimates the distance to an open-circuit by analyzing the results of a 3 elements resistance test and a 3 elements capacitance test.
Draw and Break Dial Tone	This test verifies the capability of the line circuit to detect off-hook and on-hook, the communication channel to the switching center, and the voice path from the switching center. This test is performed with the call-processing function enabled on the line under test. Note that, this test will be supported in the future release.
DTMF and Pulse Digit Measurement	This test detects and measures a DTMF digit, pulse digit, or hook-switch flash. Only one digit or flash is reported for each invocation of this test. By default, a single tone is output on the line during this test.
Foreign AC Currents	This test measures foreign AC currents.
Foreign DC Voltage	This test examines the loop for the existence of DC voltage leaking into a line form an external source.

Table 21: MTAC/RING-ENH Internal Line Tests (Continued)

Test ID	Description
Foreign AC Voltage	The foreign AC voltage test is examining the loop for the existence of AC voltage leaking onto a line from an external source.
Howler Test	This procedure generates a Howler (Receiver Off-Hook) tone until the phone goes on-hook or a timeout condition is detected.
Metering Self-Test	This procedure verifies that the line card can generate a metering pulse. It drives a metering signal into both a resistive load and an open-circuit using the current Metering Profile applied to the line.
None	No test. May used when changing test modes.
Noise Measurement Test	This procedure performs an active or passive noise test. Various filters may be applied to the received signal during this test. The application can apply special AC transmission coefficients during this test if desired.
On/Off Hook Self-Test	This procedure verifies that the line circuit can detect on-hook and off-hook events.
Read Loop and Battery Conditions	This procedure measures the instantaneous loop resistance, loop currents, and loop and battery voltages. No filtering is done during the measurement, so the results may fluctuate from one reading to the next in the presence of AC induction on the line.
Receiver Off-Hook	This test determines whether the receiver is off-hook by running the DC Loop Resistance Test twice with different test currents and analyzing the results.
Ringer Equivalency Number Test	This test calculates the Ringer Equivalency Number (REN) for the telephone attached to the line. The test supports both the regular and electronic phone REN measurement techniques.
Ringing Self-Test	This procedure verifies that the line circuit can generate high level differential signals such as those used during line testing or application of internally generated ringing to the loop. It generates a sinusoidal waveform with the requested amplitude and drives this signal into a test load of known resistance.
Ringing Monitor Test	This test is useful in checking the external ringing voltage given the loop cannot be disconnected while applying ringing and the ringing signal voltage cannot be reduced. This test is expected to be called on a line that has a terminating call (thus the need for applying ringing). This test uses about 3 cycles of the ringing waveform to carry out the test and then places the line to ringing state. Thus, a test is complete and we have placed ringing on the line as well to terminate the call. Please note that no ring trip would be detected during the first three cycles of the ringing signal.
Tone Generation Test	This test generates up to four sinusoidal tones simultaneously.
Trans-Hybrid Loss	This test measures trans-hybrid loss by generating a tone and measuring the reflected signal.
Transmission Self-Test	This procedure verifies that the line card can pass signals in the digital to analog and analog to digital directions. It measures trans-hybrid loss with open-circuit and a load impedance applied to the line. These trans-hybrid loss results are checked against expected values to generate a pass/fail result.

- 3 The test status changes to 'In-Progress'. After the test status changes to 'Completed', click **Results**. The Test Results window appears. The test result output is displayed in this window.

Single-End Loop Test (SELT)

SELT is a single-ended test. A copper loop can be tested from the MALC/MXK/Raptor XP 170, without the need for any external test equipment in either the CO or at the remote end of the loop. SELT is primarily used for proactive loop pre-qualification. For example, by checking in advance if a loop is capable of supporting ADSL2+ by determining distance, wire gauge and noise, any loop conditions can be fixed prior to rolling a truck to the customer premise.



Note: SELT and DELT are ADSL specific tests. To run SELT/DELT on a Raptor XP 170 SHDSL line, SELT/DELT uses a one-port ADSL chip internally to test the loop. To perform DELT test from Raptor XP 170, an ADSL modem must be temporarily installed at the customer premise.



Note: SELT and DELT can not be running while Admin Status of the DSL port is up or in testing mode.

Running SELT

The ZMS screenshots below show SELT tests provisioned for the MXK.

To run a SELT test:

- 1 Select a DSL port in the ZMS tree.
- 2 From the right-click menu, select **SELT**.
The SELT dialog appears.
- 3 Select the desired SELT command and specify the test duration. Click **Start** to initiate the test. Click **Stop** to terminate the tests.
Test status is displayed for status, time, and time to complete.
- 4 To display Loop Characteristic Results, click the **Loop Results** button.
The Loop Results dialog appears.
- 5 To display Noise Floor Results, click the **Noise Result** button.
The View Noise Floor Results dialog appears.
- 6 Right click the **View Noise Floor Results** dialog, you can select to export or print data.
- 7 After clicking Export Data, the **Data Export** dialog appears.
You can select a file format to Tab or CSV..
- 8 Click **Export** to export the data to your desired destination.

Dual-End Loop Test (DELT)

DELT is a dual-ended test that requires equipment at both ends of the copper loop. While this prevents DELT from being used on loops where no CPE has yet been deployed, DELT offers a deeper set of loop tests, and can provide very valuable information on the condition of a copper loop. DELT is primarily used for reactive tests on a loop after a modem has been deployed to either help troubleshoot a line or capture a baseline of loop characteristics. In addition, DELT can assist in predetermining line capability to support new services, such as voice and video.



Note: SELT and DELT are ADSL specific tests. To run SELT/DELT on a Raptor XP 170 SHDSL line, SELT/DELT uses a one-port ADSL chip internally to test the loop. To perform DELT test from Raptor XP 170, an ADSL modem must be temporarily installed at the customer premise.



Note: SELT and DELT can not be running while Admin Status of the DSL port is up or in testing mode.

Running DELT

The ZMS screenshots below show DELT tests provisioned for the MXK.

To run a DELT test:

- 1 Select a DSL port in the ZMS tree.
- 2 From the right-click menu, select **DELT**.
The DELT dialog appears.
- 3 Click **Start** to start the DELT test.
Test status is displayed for status and time to complete.
- 4 To stop the test, click the **Stop** button.
- 5 To display a general report, click the **Summary** button.
The DELT Summary dialog appears with upstream and downstream results.
- 6 To display detailed test results, click the **Details** button.
The DELT Details dialog appears with upstream and downstream results.
- 7 Right click the DELT Detail dialog, you can select to export or print data.
- 8 After clicking Export Data, the **Data Export** dialog appears.
You can select a file format to Tab or CSV..
- 9 Click **Export** to export the data to your desired destination.

T1 BERT

BER Testing for T1 EFM

The BER testing in this section applies only to the MALC-EFM-T1/E1-24 line card and *only when operating in T1 mode*.

BERT (Bit Error Rate Test) tests digital communication circuits using predetermined stress patterns which are a sequence of logical ones and zeros generated by a pseudo-random binary sequencer (PRBS). A BER Test typically consists of a test pattern generator and a receiver that can be set to the same pattern, or the BER test can be set in a loopback where the device which sends the pattern is the same device which receives the pattern. On receipt the pattern returned from the far end device is measured to determine a bit error count.

A BER Test can be used with pairs of devices, with one device at each end of a transmission link, or singularly with a loopback at the remote end, so the originating device receives the transmitted BER test.

The BER test for T1 EFM is a two part process. First you actually run the test, then display the results.

Before running the actual test a loop code is sent to the far end device, so the device will know how to respond to the BER test.



Note: BER tests are disruptive to data on the line. The user must first manually place the target DS1 port into test mode.

Running a BER test

To run a BERT test on a MALC or MxK.

- 1 Select an MTAC Enhanced card in the ZMS tree.
- 2 From the right-click menu, select **BERT**.

The BERT dialog appears.

- 3 Select the desired BERT type, Duration, and whether the line should be in loopback mode. Click Start to initiate the test. Click Stop to terminate the tests.
 - There are three supported codes: lineloop, payloadloop and noloop.
 - There are three types of test patterns: qrss, prbs20 and prbs15.
 - The BER test can be run for a selectable amount of time (between 10-300 seconds)

Test status is displayed for status, time, and BERT errors.

- 4 Click **Close** to exit the dialog.

802.3ah Ethernet OAM loopback

The Ethernet OAM loopback feature is available on all SLMS devices that support Ethernet 802.3ah OAM. You can use Ethernet 802.3ah OAM loopback to test link integrity.

Configuring Ethernet OAM loopback on a link interrupts normal service on the link. All traffic that is received, except for OAMPDUs, will either be looped back onto the transmit or dropped depending on which end is set to local loopback. When configuring loopback, the interface set to local loopback loops all received packets back out the transmit side of the interface. The interface set to remote loopback transmits traffic normally bridged or routed out this interface, and drops all received traffic.

Because there is no traffic generation, it is recommended that you enable loopback on the peer device, clear statistics, then watch to see if packet counters increase on the local receiver. Before setting a peer device to loopback mode, a connection must exist between the devices.

Configuring Ethernet OAM loopback

To configure Ethernet OAM loopback, the device that sends the loopback must be set to active mode, and the device that receives the loopback must be set to passive mode.

For Ethernet OAM loopback to work, parameters on both the CO device and remote device must be set as follows:

- 1** To set the mode to active in the ether-oam profile on the CO device:
 - d** Right-click the desired bond group on a MALC or MXK in the ZMS tree, and select **OAM**, and then click **Add**.
 - e** The **Add Ethernet OAM profile** dialog appears.
 - f** In the **Add Ethernet OAM profile** dialog box, specify active in the **Mode** field, and click **Add**.
 - g** Click **Close** to close the dialog.
- 2** To set the mode to passive in the ether-oam profile on the peer device, in this case an EtherXtend:
 - a** Right-click the desired bond group on an EtherXtend in the ZMS tree, and select **OAM**, and then click **Add**.
The **Add Ethernet OAM profile** dialog box appears.
 - b** In the **Add Ethernet OAM profile** dialog box, specify passive in the **Mode** field, and click **Add**.
 - c** Click **Close** to close the dialog.
- 3** To modify the local and remote status of the OAM loopback status parameter on the MALC, use the Modify Ethernet OAM profile dialog box on existing ether-oam profile interfaces.

- d** Right-click the desired bond group on the local or remote device in the ZMS tree, and select **OAM**, and then click **Modify**.
- e** The **Modify Ethernet OAM profile** dialog appears.
- f** In the **Modify Ethernet OAM profile** dialog box, specify the desired settings, and click **Modify**.
- g** Click **Close** to close the dialog.
- 4** To view the remote status of the OAM loopback, use the **View Ethernet OAM profile** dialog box.
 - h** Right-click the desired bond group on the local or remote device in the ZMS tree, and select **OAM**, and then click **Remote Status**.
The **View Ethernet OAM profile** dialog box appears.
 - i** Click **Close** to close the dialog.
- 5** To view the statistics the OAM loopback, use the **View Physical Performance Statistics** dialog box.
 - j** Right-click the desired bond group on the local or remote device in the ZMS tree, and select **OAM**, and then click **Statistics**.
The **View Physical Performance Statistics** dialog box appears.
 - k** Click **Close** to close the dialog.

Traps

A trap is an SNMP PDU containing real-time information about a predefined event occurring on a network device. A trap can indicate a problem such as a power supply failure or a performance problem. Or, a trap can indicate other dynamic information about network activity, such as a network object being brought down by a system administrator or a threshold level being exceeded. Traps exist for all objects, including devices, cards, physical ports, logical interfaces, permanent virtual circuits (PVCs), and so on.



Note: For the IPDSLAM devices (2600, 4200, 8620, 8820, 4000, and 12000), double-clicking the device in the ZMS tree launches the Web Interface tool for that device. To receive traps in ZMS, add the ZMS server IP address as one of the trap destinations.



Note: For the detailed description of traps and alarms, refer to the *ZMS Administrator's Guide, Appendix B Traps and Alarms*.

Topics:

[Viewing traps](#)

[Viewing trap details](#)

Viewing traps

When you access the **Trap Viewer** dialog box, the dialog box is empty. The trap list dynamically updates with traps as they are generated on the network. As new traps are received, they are added to the list.

The **Trap Viewer** dialog box displays traps only while it is open. Once you close the dialog box, you lose information on the previous traps. The next time you access the **Trap Viewer** dialog box, the dialog box begins listing new traps as they are generated on the network.

- 1 To view all traps on the network, click **View > Faults > View Traps** from the menu bar.

NetHorizon displays the **Trap Viewer** dialog box.

- 2 When you have finished viewing traps, click **File > Close**.

To clear the dialog box and start displaying new traps, select **File > Clear**.

The following table describes the information in the **Trap Viewer** dialog box.

Parameter	Description
Severity	Severity of the trap: • Critical • Major • Minor • Warning
Device	Name or IP address of the device that generated the trap.
Time	Time that the trap was created.
Event Name	Description of the trap.
Shelf ID	Shelf that generated the trap. A zero value indicates that the trap was generated on a device.
Slot ID	Card slot that generated the trap. A zero value indicates that the trap was generated on a shelf.
Port ID	Physical port that generated the trap. A zero value indicates that the trap was generated on a card.
Port Type	Type of physical port that generated the trap.

Parameter	Description
Event Type	Type of event: Trap: trap that is generated by a device Event: trap that is generated by a non-device source
Total Number of Traps	Total number of traps in the list.
Total Traps by Severity	Number of traps in the list, by severity level.

By default, traps are sorted by time, with the most recent trap being displayed first.

You can use the column headers to resort the trap information or change the order in which the traps are displayed.

The following table describes the trap row colors, which represent the severity of the traps.

Row color	Severity level
Red	Critical
Red-Orange	Major
Orange	Minor
Yellow	Warning

Viewing trap details

To view additional information about a trap, highlight a trap in the Alarm Details area of the Alarm Viewer and select Trap Details.

NetHorizon displays the **Variable Bindings** dialog box, listing the varbinds of the trap.

The following table lists the varbinds that are standard to all Zhone traps. The **Variable Bindings** dialog box may also display other trap-specific varbinds.

Table 22: Trap variable bindings

Parameter	Description
zhoneTrapsSequenceNumber	Sequence number of the trap.
snmpTrapOID	The trap OID.
zhoneTrapVersion	Version number of the format of the trap.
sysObjectID	The name of the system.

Table 22: Trap variable bindings (Continued)

Parameter	Description
zhoneTrapsAllowedCategories	The allowed categories to be sent to this particular trap destination.
zhoneTrapsSeverity	Severity of the trap (critical, severe, moderate, or low).
sysUpTime	Elapsed time the device has been running when it generated the trap.
zhoneTrapFlags	A flag value: trapAcknowledge (the trap must be acknowledged), trapOutOfSequence (trap was sent out of sequence. This value indicates that the trap receiver detected lost traps and requested that traps be resent. However, the system did not have all the requested traps), or trapResetSequenceNumber (the sender reset the trap sequence number for the trap destination)
zhoneZmsBlockCli	Indicates whether the CLI has been blocked or unblocked. When unblocked, changes to the device configuration can be made from the CLI or from NetHorizon.

Alarms

As alarms are generated on the network, you can view:

- All active alarms on the network.
- All active alarms generated for a particular object (and all its children, optionally).

For information on modifying ZMS alarms handling, see the properties file information in the *ZMS Administrator's Guide*.

Topics:

[Viewing all alarms on the network](#)

[Viewing all alarms for a particular object](#)

[Viewing alarm history](#)

[Viewing alarm details](#)

[Acknowledging alarms](#)

[Clearing alarms](#)

[Forwarding alarms](#)

[Assigning alarms](#)

[Identifying objects with alarms](#)

[Receiving mail notification of alarms](#)

[Configuring external alarms](#)

Alarm manager overview

ZMS synchronize alarms on managed devices. This keeps the alarms NetHorizon reports synchronized with the alarms actually present on the device. It also prevents active alarms from being deleted using NetHorizon.

Managed devices maintain all active traps. ZMS reconciles alarms based on the information from device whenever the device is rebooted, device connectivity is lost and regained, after a config sync, or after a device database restore.

- 1 To manually synchronize alarms with a single device, right-click a device, region or sub-region node and select **Synchronize Alarms**. This command is available on all device, region, and sub-region nodes.
- 2 If you right-click a region or sub-region node and select **Synchronize Alarms**, all devices under that node will have their alarms synchronized.



Note: Synchronize Alarms is not supported on the top level “Regions” node.

Viewing all alarms on the network

The **Alarm Viewer** dialog box displays active alarms. As new alarms are received, they are displayed in the list. As alarms are cleared, they are dropped from the list.

To view all alarms on the network, click **View > Faults > View Alarms** from the menu bar.

NetHorizon displays the **Alarm Viewer** dialog box, listing all the alarms generated on the network.

The following describes the information in the **Alarm Viewer** dialog box.

Table 23: Alarm information

Parameter	Description
Severity	Severity of the alarm: • Critical • Major • Minor • Warning • Normal (informational)
Device	Name or IP address of the device that generated the alarm.
Time	Time that the alarm was created.
Description	Description of the alarm.
Troubleshooter	Operator to which this alarm has been assigned.
State	State of the alarm (received, assigned, acknowledged, cleared)
Event Type	Object on which the alarm is generated
Operator	The name of the operator is included in acknowledged or cleared alarms. If the system itself cleared the alarm, this displays system .
Total Number of Alarms	Total number of alarms in the list.
Total Alarms by Severity	Number of alarms in the list, by severity level.

By default, alarms are sorted by time, with the most recent alarm being displayed first.

To select the display you want, click **View > View Child Alarms**, or click the **View Child Alarms** icon.

When you have finished viewing alarms, click **File > Close** (or click the close button icon in the upper right corner of the **Alarm Viewer** dialog box).

The following describes the alarm row colors, which represent the severity of the alarms.

Row color	Severity level
Red	Critical
Red-Orange	Major
Orange	Minor

Row color	Severity level
Yellow	Warning
White	Normal

Viewing all alarms for a particular object

- 1 Navigate to the object that generated the alarms.
- 2 Right-click the object and click **View Alarms**.

NetHorizon displays the **Alarm Viewer** dialog box, listing all the alarms generated for the object (and all its children, optionally).

Viewing alarm history

ZMS supports an Alarm History Viewer. This window allows the operator to view alarms that were generated by system events and/or traps. When an alarm has been cleared in the system, the operator still has the ability to view the alarm in the alarm history window.



Note: By default, the Alarm History Viewer holds up to 5,000 alarm log records. To modify the maximum number of alarm log records, change the **maxAlarmLogRecords** parameter in the FaultService.properties file.

This information is the same information captured in the `/opt/weblogic/yyyy_mm_dd_alarm.log` on the server.

- 1 To access the Alarm History viewer, select **View > Faults > View Alarm History**.

The Alarm History Viewer window appears.

- 2 To filter the displayed alarms, specify the desired filter criteria such as device, description, date/time, and severity levels and click **Retrieve Data**.
- 3 To save the alarm filter template settings for re-use, click the **SaveAs** button and specify the desired filename.

Related topics:

[Viewing the audit log on page 463](#)

Viewing alarm details

To view additional information about an alarm, right-click the alarm entry and click **Alarm Cause**.

NetHorizon displays information about the alarm and the trap that generated it in the **Alarm Details** area of the **Alarm Viewer** dialog box.

For descriptions of the trap information in the dialog box, see [Parameter on page 477](#).

From the **Alarm Details** area of the **Alarm Viewer** dialog box, you can view varbinds of the trap that generated the alarm. Right-click the trap entry and click **Trap Details**.

For descriptions of the trap varbinds, see [Table 22](#).

From the **Alarm Viewer** dialog box, you can also assign alarms to a troubleshooter, add notes to alarms, acknowledge alarms, and clear alarms. These tasks are described in the following sections.

Acknowledging alarms

As alarms are generated on the network, you can view and acknowledge them. By acknowledging an alarm, you notify other operators that someone has seen the alarm. Such information helps other operators know what network issues are being addressed.

- 1 Access the **Alarm Viewer** dialog box (using either of the methods described in [Alarms on page 479](#).)
- 2 From either the alarm list or the **Alarm Details** area of the **Alarm Viewer** dialog box, select one or more alarm entries that have the same State value, right-click, and click **Acknowledge Selected**.

NetHorizon updates the **State** parameter with the value **Acked** and updates the color of the alarm entry:

- Background color returns to the default color.
- Outline color represents the alarm severity.

Once you have acknowledged all alarms generated by an object:

- The object background color returns to the default color.
- The object outline color represents the highest severity of outstanding alarms (including those you acknowledged).
- In the graphical display, the message balloon disappears.
- In the graphical display, the object alarm count represents the total number of outstanding alarms (including those you acknowledged) of highest severity. If the object also generates lower-severity alarms, the alarm count contains a plus sign (+).

Clearing alarms

As alarms are generated on the network, you can acknowledge and clear them (you must acknowledge an alarm before you can clear the alarm; see [Acknowledging alarms on page 483](#).) You should clear alarms when the network issues they represent have being addressed.

Note that the following alarms cannot be cleared until the alarm condition no longer exists:

- Link down alarm (LINK_DOWN_ALARM) on any physical interface
- SONET line AIS alarm (SONET_LINE_AIS_ALARM)

- SONET line RDI alarm (SONET_LINE_RDI_ALARM)
- SONET section LOS alarm (SONET_SECTION_LOS_ALARM)
- SONET section LOF alarm (SONET_SECTION_LOF_ALARM)
- SONET path LOP alarm (SONET_PATH_LOP_ALARM)
- SONET path AIS alarm (SONET_PATH_AIS_ALARM)
- SONET path RDI alarm (SONET_PATH_RDI_ALARM)
- SONET path unequipped alarm (SONET_PATH_UNEQUIPPED_ALARM)
- SONET path signal label mismatch alarm (SONET_PATH_SIGNAL_LABEL_MISMATCH_ALARM)

Once you have cleared all of alarms generated by an object:

- The object background color and outline color return to the default color.
- In the graphical display, the object alarm count resets to zero.

To clear alarms:

- 1 Access the **Alarm Viewer** dialog box (using either of the methods described in [Alarms on page 479](#).)
- 2 From either the alarm list or the **Alarm Details** area of the **Alarm Viewer** dialog box, select one or more alarm entries that have the State value Acked and click Clear Selected.

NetHorizon clears the alarms and removes them from the **Alarm Viewer** dialog box.

Forwarding alarms

You can configure the fault manager to forward alarms to specific IP addresses. The fault manager forwards an alarm when the alarm is generated and when the alarm is cleared.

The fault manager forwards alarm information wrapped in special traps to particular fault system(s) for processing.

The special traps defined for alarm forwarding are:

- alarmReceived, which is sent when a new alarm is generated in response to a trap from device.
- alarmCleared, which is sent when an existing alarm is cleared (either by a clearing trap or explicitly by an operator).

These traps are defined in *zmsAlarm.mib*. The following table lists the varbinds included in these traps.

The first five varbinds are standard to all Zhone traps.

The last nine varbinds are defined for alarmReceived and alarmCleared traps defined in *zmsAlarm.mib* (faultServiceTraps).

Table 24: Trap information

Parameter	Description
SysUpTime	Elapsed time the device has been running when it generated the trap. This a standard SNMP varbind. Some SNMP tools may display this information in the trap header, rather than in the trap itself.
Trap OID	The trap OID. This a standard SNMP varbind. Some SNMP tools may display this information in the trap header, rather than in the trap itself.
Trap Version	Version number of the format of the trap.
Trap Sequence Number	Sequence number of the trap.
Trap Severity	Severity of the trap (critical, severe, moderate, or low).
Alarm Name	Name of the alarm.
Alarm Description	Description of the alarm.
Alarm Type	Type of the alarm.
Alarm Severity	Severity level of the alarm.
Alarm Timestamp	Time that the alarm was created.
Alarm Device	Name or IP address of the device that generated the alarm.
Alarm Shelf	Shelf that generated the alarm. A zero value indicates that the alarm was generated on a device.
Alarm Slot	Card slot that generated the alarm. A zero value indicates that the alarm was generated on a shelf.
Alarm Port	Physical port that generated the alarm. A zero value indicates that the alarm was generated on a card.

Environment variables in the *FaultService.properties* file specify alarm forwarding, including destination hosts by alarm severity level and specific alarms to be excluded from forwarding. For details on setting the environment variables in the *FaultService.properties* file, see the *ZMS Administrator's Guide*.

Assigning alarms

As alarms are generated on the network, you can assign them to troubleshooters. By assigning an alarm, you notify the operator of the network issue to be addressed.

- 1 Access the **Alarm Viewer** dialog box (using either of the methods described in [Alarms on page 479](#).)
- 2 From either the alarm list or the **Alarm Details** area of the **Alarm Viewer** dialog box, use any of the following methods to assign an alarm to a troubleshooter:

Menu bar: Select one or more alarm entries and click **Edit > Assign Alarm to Troubleshooter**.

Toolbar: Select one or more alarm entries and click the **Assign Alarm to Troubleshooter** icon.

Pop-up menu: Select one or more alarm entries, right-click, and click **Assign Alarm to Troubleshooter**.

NetHorizon displays the **Assign Troubleshooter** dialog box, listing operators from which you can specify a troubleshooter.

- 3 Select the operator you want and specify and notes related to the alarm in the Notes area. Then, click **OK** (**OK** appears dimmed until you select an operator).

NetHorizon updates the **Troubleshooter** field with your selection and updates the **State** field with the value **Assigned**.

You can re-assign an alarm to another operator at any time.

Identifying objects with alarms

NetHorizon dynamically updates its display with current fault information. Every time an alarm is generated, your display informs you with the following changes:

Adds (or removes) a message balloon to the object—The message balloon identifies the alarms generated for the object:

- In the tree display, the balloon background color and letter represent the highest severity of newly generated (unacknowledged) alarms. The balloon outline color represents the highest severity of outstanding alarms (acknowledged and unacknowledged).
- In the graphical display, the balloon background color and letter represents the highest severity of newly generated (unacknowledged) alarms. The balloon also lists the number of unacknowledged alarms of highest severity. If the object also generated lower-severity alarms, the alarm count contains a plus sign (+).

Color codes the object (*graphical display only*)—The color represents alarm severity:

- The object background color represents the highest severity of newly generated (unacknowledged) alarms.
- The object outline color represents the highest severity of outstanding alarms (acknowledged and unacknowledged).

Adds (or updates) a total alarm count to the object (*graphical display only*)—The count represents the total number of outstanding alarms (acknowledged and unacknowledged) of highest severity. If the object also generated lower-severity alarms, the alarm count contains a plus sign (+).



Note: For many alarms, this display information is propagated to a parent of the object. That is, the display information appears on the particular object for which the alarm was generated and also appears on a parent of the object (in most cases, the parent device).

The following table describes the colors and letters that represent the severity of the alarms.

Table 25: Colors and letters of alarm severity

Severity level	Letter	Color
Critical	C	Red
Major	M	Red-Orange
Minor	m	Orange
Warning	W	Yellow

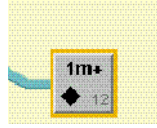
For example, in the graphical display, a device with one unacknowledged critical alarm looks like this:



A device with one unacknowledged minor alarm and one acknowledged critical alarm looks like this:



A device with one acknowledged minor alarm plus one or more warning alarms looks like this:



Receiving mail notification of alarms

In addition to using NetHorizon to manage faults on your network, you can configure the fault manager to send a mail message notifying individuals that an alarm has occurred on the network. The mail message indicates:

- Alarm severity level
- Alarm description
- The component that generated the alarm, including device name, shelf ID, card slot ID, and port ID. A shelf ID, slot ID, or port ID value of zero indicates that the alarm was generated on the parent of that object.

The following sample illustrates an alarm notification mail message:

```
Subject: Critical Alarm Notification!!!
Date: Mon, 11 Jun 2001 12:50:13 -0400
From: "Samantha Randell" <srandell@xyz.com>
To: cmcintire@xyz.com
```

```
ALARM: Carrier Equipment out of service on
PhysicalAlarmSet
```

```
Device: BAN_162
Shelf: 1
Slot: 2
Port: 1
```

Environment variables in the *FaultService.properties* file specify the operator(s) to receive the mail message, by alarm severity level, and specific alarms to be excluded from notification. For details on setting the environment variables in the *FaultService.properties* file, see the *ZMS Administrator's Guide*.

Configuring external alarms

The MXK alarm board have a 8 pin connector that provides sensing of alarm relay contacts for external devices. When an alarm condition occurs on the external device, the NetHorizon sends a trap. Each of the 8 pairs of pins can be assigned to a different alarm. Use the **Modify External Relay** to assign a

description to an alarm relay. The description is included in traps and log messages.

- 1** Click the MXK in the tree view, expand the device level.

- 2** Click **External Relay**, expand the relay level.

Eight relay contacts appear.

- 3** Right-click a relay, and select **Modify**.

The **Modify External Relay** dialog box appears.

- 4** In the **Modify External Relay** dialog box, view or specify the following information:

Relay Name: Add a description to the alarm contact of the MXK I/O alarm board.

Normal State: Add a default state for each alarm relay. The normal-state field has three value options: notspecified, normallyclosed, normallyopen.

Click **Modify**.

INDEX

Numerics

12000 55, 56, 476
2600 55, 56, 476
4000 55, 56, 476
4200 55, 56, 476
8620 55, 56, 476
8820 55, 56, 476

A

access list, device configuration 88
access list, how to configure 66
access lists
 SNMP 66
account status for NetHorizon operators 28
acknowledging alarms, procedure for 483
action parameters 38
active users, management 459
adding
 card 131
 multiple cards 132
adding a device
 autodiscovery 56
 described 55
adding a trap forwarding address, procedure for 65,
 66, 67, 68, 395
adding objects
 synchronizing elements 81, 82
ADSL2+ bond card
 ADSL2+ bonding 193
ADSL2+ bonding 193
alarm dialog box, use of 479
alarm levels, device configuration 87
alarm suppression 87
alarms
 beep notification 461
 clearing 483
 filtering 465, 466
 manager overview 480
 receiving mail notification of 488
 severity levels 481
 viewing 479
 viewing history 43

APS

configuration 458

assigning alarms, procedure for 486

ATM

autocreate VCLs 364, 367, 376
autocreate VPLs 369
autoincrementing VPIs 365, 377
CES connections 374
CES cross connections wizard 376
configuring bandwidth for cards 144
cross connect templates 362
modify VCL rates 40
multicast map 456
SCR and PCR, configuring allowable values
 for 141
traffic descriptor templates 361
UBR and usage-parameter-control 142
VC cross connect advanced mode 367
VC switched connections 364, 366
VCL endpoints 372
VP switched connections 369
VPI profile 143
VPL endpoints 373

ATM cross connect, how to configure 363

ATM cross connections and associated traffic
 descriptors, configuring 363

ATM ping command 462

Audit Log

changing information displayed in 463

autodiscovery, devices 56

B

backup

saving configurations 76, 77

backup configurations 75

bandwidth

configuring ATM bandwidth for 144

bond groups, G.SHDSL 190

bridge video 408, 415, 417

bridging

intralinks 404

overview 403

RLink 405

bulk statistics settings, device configuration 95

C

call conferencing, SIP 324

card status, viewing 33

cards

adding 131

adding multiple 132

configuring ATM bandwidth 144

configuring redundant MALC cards 133

deleting 138

deleting software image 138

enabling 133

rebooting 136

redundancy overview 457

re-enabling 133

re-enabling a card 133

re-enabling cards 133

setting default card image 137

setting default image 137

state after adding 131, 132

viewing state 136

CES

circuit, modifying 378

configuration wizard 376

cross connect, adding 374

CES over IP, configuring 390

clearing alarms, procedure for 483

clock

viewing status 140

clocking

clock source weights 139

device 139

community name

adding 64, 65

configuring 65

default 55

community names, device configuration 87

config sync

initiated when adding device 56

initiating with device 81, 82

ConfigBridgeCfgGroup 383, 431

ConfigModPhysicalBondedDsl 100, 113, 180

ConfigModPortRPR 200

configuration

restoring device 80

viewing requests received by ZMS 44

configuration backups 75

configuration, GPON OLT 203

configuration, GPON OLT, DDM 210

configuring 40

configuring ATM cross connections and associated traffic descriptors 363

configuring cards, shortcut 132

configuring subscribers

description 347

ConfigViewPhysicalBondedDsl 100, 113, 180

container, definition of 30

cross connects

autocreate VCLs 364, 367, 376

autocreate VPLs 369

CES 374

CES, wizard 376

optical cross connects, optical cross connection, GigaMux 379

templates 362

using advanced mode to create 367

VC switched 364, 366

VP switched 369

D

date and time, using NTP 141

deleting

card 138

card software image 138

device 57

trap forwarding 68

deleting a trap forwarding address, procedure for 65, 66, 67, 68, 395

deleting software image

description 138

procedure 138

DELT 473

device

adding 55

autodiscovering 56

clocking 139

config synch 81, 82

deleting 57

editing configuration 79

editing configuration file 79

finding 58

managing 58

obtaining general information about shelf 40

rebooting 80

restoring configuration 80

- saving configuration 76, 77
 - viewing card state 136
- device configuration
 - access lists settings 88
 - admin settings 82, 85
 - alarm levels settings 87
 - bulk statistics settings 95
 - community names settings 87
 - DSCP TO COS settings 93
 - EtherXtend settings 120
 - GigaMux 1600/3200 settings 97
 - identity 82
 - location settings 92
 - Malc XP settings 119
 - MX settings 121, 123, 124
 - MXK settings 120
 - NTP settings 95
 - Port Access Control, device configuration 86
 - RSTP settings 96
 - system clock settings 95
 - trap configuration settings 88
 - video source settings 95
 - voice DSP settings 92
 - ZMS connectivity settings 87
- DHCP
 - relay 382
- DHCP server 384
- DHCP, description of 384
- display windows, launching multiple 36
- display, updating 38
- DS3 fanout 143, 367
- DSCP To CoS settings, device configuration 93
- DSP settings, device configuration 92
- Dual-ended loopback test (DELT) 473
- Dynamic Host Control Protocol, see DHCP

E

- EBS
 - templates 315
- EFM SHDSL 24 NTP/NT cards, configuring 145
- Emergency Standalone (ESA) service 359
- Emergency Standalone feature 356
- Emergency Standalone (ESA) voice connection 330
- enabling
 - card 133
- ESA 356, 359
- ESA, configure dialplan 356

- ESA, voice connection 330
- Ethernet, double tagged frames 409
- EtherXtend settings, device configuration 120

F

- fault manager
 - processing 488
- fax, T.38 option 323, 346
- finding, locating objects 59
- flap control, setting 415, 416, 417, 441
- flash image
 - menu 41
- flash software image 77
- forwarding alarms 484

G

- G.SHDSL 24 NT card, modifying 145
- G.SHDSL 24 NTP card, modifying 145
- G.SHDSL bond groups 190
- getting started with NetHorizon 25
- GigaMux
 - optical cross connects 379
- GigaMux 1600/3200 settings, device configuration 97
- GigaMux cards, configuring 145
- GigaMux port configuration 201
- GPON DBA, configuring 216
- GPON OLT port configuration 203, 210
- GPON OLT serial numbers 207, 229
- GPON OMCI configuration
 - CPE profile configuration 245
 - OMCI file configuration 223
 - OMCI ONU configuration 232
 - OMCI profile configuration 225
 - Generic profile 226
 - ME profile 225
 - Specific profile 227
 - OMCI statistics 243
- GPON ONU GEM, configuration 211
- GPON ONU, configuring 203, 212
- GR-303
 - templates 308
 - voice connection 348
- graphical display
 - description 31
 - navigating 36
 - navigating through objects 35

H

Help, accessing 46
hitless upgrades 74

I

identifying alarms
 adding a message 486
 color-coded objects 486
 description 486
 display colors 487
identity, device configuration 82
immediate upgrading ONTs. 239
instances, definition of 30
Intralinks
 configuring 404
Inventory Manager 466
IP 40
 adding host routes to MALC 387
 DHCP relay 382
IPDSLAM 55, 56, 476
IPSLA configuration 397
 CoS action map 399
 DSCP to CoS action index mapping 400
 Global IPSLA settings 397
 Historical IPSLA statistics 401
 IPSLA static path 398
 Real time IPSLA statistics 401
IsPPPoA option 408

L

launching multiple display widows
 description 36
 procedure 36
Line status change traps 164
location settings, device configuration 92
logging in 26
logging out of NetHorizon 459
logical links 62

M

MALC
 configuring redundant MALC cards 133
Malc XP settings, device configuration 119
managing faults
 forwarding alarms 484

 receiving mail notification of alarms 488
 viewing alarm details 482
 viewing trap details 478
 viewing traps 477
map display, repositioning objects in 35
map, logical links 62
map, physical links 61
maps
 changing default 50
menu bar
 options 39
 using 39
 zooming in and out of view 34
message console window, using 37, 62
ModifyBridgeCfgGroup 431
MSTP 447
 configure MSTP uplinks 451
 instances 447
 overview 447
 port role 447
 port state 448
 VLAN mapping planning 449
multicast
 creating map 456
multiple display windows, launching 36
Multiple Spanning Tree Protocol (MSTP) 447
MX settings, device configuration 121, 123, 124
MX-150
 models 120
MXK settings, device configuration 120
MXP-180/280
 overview 123

N

NAT
 description 395
navigating
 a tree 35
 graphical display 36
 launching multiple display widows 36
 objects in graphical display 35
 updating display 38
navigating NetHorizon
 description 30
 graphical display 31
 tree 35
 tree display 30
 views 35

NetHorizon

- accessing Help 46
- account 26
- acknowledging alarms 483
- assigning alarms 486
- changing password 46, 460
- clearing alarms 483
- configuring ATM cross connections and associated traffic descriptors 363
- container 30
- display updates 38
- getting started 25
- graphical display 31
- identifying alarms 486
- instances 30
- launching multiple display windows 36
- logging out 459
- login failure 27
- menu bar 39
- menu options 39
- navigating 30
- navigating a graphical display 36
- navigating through objects 35
- operator account status 28
- operator password 28
- operator user name 28
- product version number 460
- repositioning objects 35
- running diagnostics 467
- toolbar 45
- toolbar options 45
- tree display 30
- updating display 38
- using the message console window 37, 62
- viewing card status 33
- zooming in and out of views 34

NetHorizon account, about 26

NetHorizon User's Guide

- about this guide 3
- audience 3
- contacting customer support 5
- organization 3
- related documentation 5

NetHorizon, getting started with 25

Network Address Translation, see NAT

NTP

- configuration 141

NTP settings, device configuration 95

O

OAM F4 loopback 43

OAM F5 loopback 43

object

- finding 59

OC3-c/STM1

- APS 458

OLT serial numbers 207, 229

ONT upgrade

- s immediate upgrading single ONT. 237
- scheduled upgrading ONTs 239

operator accounts

- creating (as user administrator) 28

P

password

- changing 46, 460
- NetHorizon operators 28

PAT 396

PAT binding

- NAT 396

performing a full synchronization, procedure for 81, 82

PerfViewPhysicalN2NBond 184, 191

physical links 61

ping ATM VCL endpoints 462

port configuration, GigaMux 201

port status, displaying ports per card 146

POTS

- templates 312, 313, 314

POTS phone, ringing 319

POTS to GR303 ESA voice connection 330

PPP

- configuring 40

PPPoA to PPPoE internetworking 408

preferences 461

preferences, specifying 460

product version number, locating 460

Q

Q-in-Q 409

R

RADIUS authentication 89

RADIUS configuration 88

- RADIUS client profile configuration 90
- RADIUS index 92
- RADIUS index configuration 92
- user authentication method 89
- ReachDSL, configuring 135, 145
- rebooting
 - card 136
 - device 80
- redundancy
 - overview of card 457
- redundant cards
 - group number 133
- redundant cards, configuring 133
- re-enabling, procedure for 133
- regions
 - changing maps 50
- repositioning objects in map display 35
- Resilient Packet Ring (RPR) configuration 200
- Ring phone test 319
- ring source, device configuration 82
- Rlink
 - configuring 405
- RPR port configuration 200
- RPR, topology links 61
- RSTP Parameters, device configuration 96
- running diagnostics
 - description 467

S

- SABR 393
- scheduled config sync 82
- scheduled synchronizing elements 82
- secure mode, device configuration 85
- SELT 472
- serial numbers OLT 207, 229
- server
 - telneting to ZMS 44
- setting default card image
 - description 137
 - procedure 137
- SFTP, device configuration 85
- Single End Loop Tests (SELT) 472
- SIP dial plans 356
- SIP timers 351, 352
- SIP, call conferencing 324
- SNMP
 - access lists 66
 - community name 55

- community names 64, 65
- deleting trap forwarding address 68
- trap forwarding address 66, 67
- software
 - flashing image 77
 - setting default image for card 137
- software downloads
 - deleting software image 138
 - setting default card image 137
- software image
 - deleting software image 138
- software, hitless upgrades 74
- SONET
 - APS configuration 458
- source address based routes (SABR) 393
- specifying preferences 460
- S-tag 409
- static routes 393
- static routes, adding 394
- statistics
 - Bond group 191
 - Link Aggregation Group 184
- subscriber, how to configure 347
- subscribers
 - adding 347
 - assign to voice ports 40
- synchronizing elements
 - performing a full synchronization 81, 82
- synchronizing with device 81, 82
- system clock settings, device configuration 95

T

- T.38 fax option 323, 346
- tagged bridging
 - described 403
- Task Log
 - changing information displayed in 463
- templates
 - cross connect 362
 - EBS 315
 - GR-303 308
 - POTS 312, 313, 314
 - traffic descriptor 361
 - V5.2 POTS 307
 - V5.2 PSTN 306
- three-way call conferencing 324
- toolbar
 - icons 45

- options 45
- using 45
- topology links 61
- traffic descriptor
 - templates 361
- trap configuration settings, device configuration 88
- trap forwarding
 - adding a trap forwarding address 65, 66, 67, 68, 395
 - deleting a trap forwarding address 65, 66, 67, 68, 395
- trap forwarding address
 - deleting 68
- trap viewer dialog box, description of 477
- traps
 - display colors 478
 - forwarding address 66, 67
- tree display, description of 30
- tree, navigating 35

U

- UBR
 - modem train rates and 142
- untagged bridging
 - described 403
- update display from database 467
- updates following action parameter changes 38
- updating display
 - description 38
 - entire display 38
 - object and children 38
- upgrades, software 74
- upgrading
 - flashing image 77
- user management 459
- user name for NetHorizon operators 28
- user preferences 461

V

- V5.2
 - templates 306, 307
 - voice connection 348
- variable binding dialog box, description of 478
- VCLs
 - creating 364, 367, 376
 - endpoints 372
- video bridging 408, 415, 417

- video source settings, device configuration 95
- viewing alarms
 - alarm dialog box 479
 - alarms on an object 479
 - all alarms on a network 479
 - display colors 481
- viewing alarms, alarm details 482
- viewing card status 33
- viewing system messages 37, 62
- viewing traps, trap viewer dialog box 477
- viewing traps, variable binding dialog box 478
- viewport, launching multiple 36
- views, navigating through 35
- voice
 - adding connections to MALC 317, 332, 333, 344
 - EBS templates 315
 - GR-303 templates 308
 - POTS templates 312, 313, 314
 - V5.2 POTS templates 307
 - V5.2 PSTN templates 306
- voice bandwidth check, device configuration 82
- voice connection
 - adding 347
 - adding to MALC 317, 332, 333, 344
 - GR-303 348
 - V5.2 348
- VOIP
 - SIP timers 351, 352
- VPI
 - autoincrementing 365, 377
- VPI profile 143
- VPLs
 - creating 369
 - endpoints 373

Z

- ZMS
 - description 3
 - telneting to server 44
- ZMS connectivity, device configuration 87
- zooming in and out of views
 - description 34
 - menu bar 34

