User Manual

ML700

Release 7.14

Revision No. A04

Document No. 520R70714E

Document Identification

ML700 Release 7.14
Document No. 520R70714E
Revision No. A04
Date: APR 2016

Copyright

Disclaimer of Warranties and limitation of Liabilities

Actelis Networks, Inc. (hereafter referred to as Actelis Networks, Inc. or Actelis Networks), makes no representation or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for a particular purpose. Further, in no event, shall Actelis Networks be liable for incidental or consequential damages in connection with or arising from the use of the ML700 series, cards and modules, accessories kits, this manual or any related materials. Actelis Networks reserves the right to revise this publication from time to time and to make changes in the content hereof without obligation to notify any person of such revisions or changes.

Trademarks

Actelis, Actelis Networks, EFM*plus*, Carrier Ethernet over Copper and related logos and icons are the registered trademarks or copyrights of Actelis Networks. Other identifiers may be trademarks or marks of their respective owners.

Patent protection

The products described in this document are protected by U.S. Patent No. 6,744,811 and other U.S. patents, foreign patents, and/or pending applications.

Document Objectives

This manual provides a general description of the ML700 device, detailed instructions for the deployment and maintenance of the ML700 device.

Intended Audience

The intended audience for this document is both technical and non-technical staff within Network Service Provider (NSP) organizations, and it is assumed that the reader has a general understanding of voice and data communications, the xDSL industry and high-speed digital services.

Symbols Used in this Manual

 **Warning:** Indicates information on how to avoid personal injury.

 **Caution:** Indicates information on how to avoid damage to the equipment or to avoid possible service disruption.

 **ESD:** Indicates information on how to avoid discharge of static electricity and subsequent damage to the Actelis system.

Actelis supplies each product with the following system documentation and applications, (for Documentation and Software Applications ordering contact Customer Support):

- **ML User Manual** – provides a general description, detailed instructions for the deployment, configuration and maintenance of the product. The User Manual is available in PDF format and as Online Help. A hard copy can be ordered separately.
- **ML Quick Installation Guide** – provides summary explanations of the procedures for installing the Actelis system. The Quick Installation Guide is included in each Actelis product package and also can be ordered separately.
- **MetaASSIST View** – software and MetaASSIST View documentation. MetaASSIST view installation files are available both for Windows (*.exe) and Unix (*.bin).
  The two files are also available with *.mft extension. These files can be stored on and downloaded from the ML device as explained in **Updating Software Versions** (on page 14-13).

Contact Information

Please contact your local sales representative, service representative or distributor directly for any help needed. For additional information concerning warranty, sales, service, repair, installation, documentation, training or distributor locations, use any one of the following:

- **Internet:** Visit the **Actelis Networks World Wide Web site http://www.Actelis.com**
- **Mail to: Actelis Networks customer support Mailto: techsupport@actelis.com** for technical support.
- **Customer support:** Contact Actelis Networks Customer Support directly at one of the following numbers:
  - Belgium: (0) 800 71180
  - Denmark: 80 887 771
  - France: (0) 800 918 450
  - Germany: (0) 800 1833504
  - Netherlands: (0) 800 0225982
  - UK: (0) 800 9179049
  - USA: +1 866 638 2544 or +1 510 545 1071

For all other inquiries, please call +1 866 ACTELIS (+1 866 228 3547) or +1 510 545 1071.

Document Feedback

We welcome your comments and suggestions about this document. Please mail them to Technical Publications, Actelis Networks, 6150 Stevenson Boulevard, Fremont, CA 94538 or to **userdoc@actelis.com mailto:userdoc@actelis.com**. Include the document number, revision number and title of this document in your correspondence. Please include your name and phone number if you are willing to provide additional clarification.

ML700 Certification

FCC Class A Compliance

The ML700 complies with the limits for a Class A digital device that is marketed for use in a commercial, industrial or business environment, exclusive of a device which is intended to be used by the general public or is intended to be used in the home. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the Quick Installation Guide, may cause harmful interference to radio communications.

The authority to operate this equipment is conditioned by the requirement that no modifications will be made to the equipment unless the changes or modifications are expressly approved by Actelis Networks, Inc.

Canadian Emissions Requirements

The ML700 Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe A respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

Warning: This is a Class A product. In a domestic environment, this product may cause radio interference, in which case you may be required to take adequate measures.

CE Mark

This equipment complies with the Council Directive 89/336/EEC for electromagnetic compatibility. Conformity with this directive is based upon compliance with the following harmonized standard ETSI EN 300 386 V1.3.1 (2001- 09).

CE

This product complies with the requirements of the Low Voltage Directive 73/23/E and EMC Directive 89/336/EEC as amended by 92/31/EEC and 93/68/EEC, when it is properly installed and maintained, and when it is used for the purposes for which it is intended.

MEF Certification

The ML device has undergone testing in accordance with MEF 14 requirements and found to comply with certain requirements detailed in the Iometrix detailed test report.

VCCI Compliance

The ML700 meets VCCI Class A digital apparatus requirements.

この装置は、クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI－A

General Safety Summary

1. Read and follow all warning notices and instructions marked on this product or included in this manual.
2. All installation, repair or replacement procedures must be performed by qualified service personnel.
3. Before attempting to operate or repair this product, make sure product is properly grounded.
4. This product uses an external power source. Do not touch exposed connections, components or wiring when power is present.
5. Do **not** operate this product with panels removed or with suspected failure or damage to electrical components.
6. Do **not** operate or repair this product in wet or damp conditions or in an explosive atmosphere.
7. Keep product surfaces clean and dry.
8. Provide proper ventilation.
9. Observe all ratings and markings on the product. Before making connections to the product, consult the appropriate chapters of this manual for further ratings information.
10. Many of the cables for this product are supplied by Actelis Networks. Cables that are supplied by the customer must comply with the regulatory inspection authorities and are the responsibility of the customer. To reduce the risk of fire, make sure all cables are UL Listed or CSA Certified.
11. This equipment must be installed according to country national electrical codes. For North America, equipment must be installed in accordance with the US National Electrical Code, Articles 110–16, 110–17 and 110–18 and the Canadian Electrical Code, Section 12. If necessary, consult with the appropriate regulatory agencies and inspection authorities to ensure compliance.
12. Over-current Protection: It is recommended to incorporate in the building wiring, a readily accessible listed branch circuit overcurrent protective device rated to 2A min. and 5A max. A 5A circuit over current protective device can feed two ML700 units in rack mount sleeve.
13. The equipment shall be connected to a properly earthed supply system.
14. All equipment in the immediate vicinity shall be earthed the same way and shall not be earthed elsewhere.
15. A disconnect device is not allowed in the earthed circuit between the DC supply source and the frame/earthed circuit connection.
16. When using a fiber optic port, never look at the transmit laser while it is powered on. Also, never look directly at the fiber TX port and fiber cable ends when they are powered on.
17. In case of Fan alarm (HWFLT), it is required to replace ML700 within four (4) hours.

Prevention of Electrostatic Discharge (ESD) Damage

1. When working with electronic components, wear a commonly grounded antistatic wrist strap to discharge the static voltage from your body in accordance with approved standards.
2. Do not use any devices capable of generating or holding a static charge in the work area where you install or remove electronic components. Avoid handling electronic components in areas that have a

floor or benchtop surface capable of generating a static charge.

3. Do not slide electronic components over any surface. Do not touch exposed connector pins. Handle electronic components as little as possible.
4. Transport and store electronic components in an approved static-protected bag or container.

Consumer Notice

The purchased Actelis' product is subject to Directive 2002/96/EC of the European Parliament and the Council of the European Union on waste electrical and electronic equipment (WEEE) and, in jurisdictions adopting that Directive, is marked as being put on the market after August 13, 2005, and should not be disposed of as unsorted municipal waste. Please utilize your local WEEE collection facilities in the disposition of this product and otherwise observe all applicable requirements.

Résumé des conditions générales de sécurité

1. Lisez et suivez attentivement les notes d'avertissements et les instructions indiquées sur ce produit ou inclues dans ce manuel.
2. Toute installation, procédure d'entretien ou de remplacement doit être effectuée par un personnel de service qualifié.
3. Avant d'essayer de faire fonctionner ou de réparer ce produit, veillez à ce que le produit soit connexion de mis à la terre correctement.
4. Ce produit utilise une source de courant externe. Veuillez ne pas toucher les connections, éléments ou fils électriques découverts quand il y a du courant.
5. **Ne** faites pas fonctionner ce produit sans ses panneaux ou si vous suspectez une défaillance ou un dégât au niveau des composants électriques.
6. **Ne** faites pas fonctionner ce produit dans des conditions mouillées ou humides ou dans une situation où il y a risque d'explosion.
7. Gardez les surfaces du produit propres et sèches.
8. Fournissez une aération appropriée.
9. Observez toutes les valeurs nominales et indications sur le produit. Avant d'établir des connexions au produit, consultez les chapitres du manuel pour obtenir plus d'informations sur les évaluations.
10. De nombreux câbles de ce produit sont fournis par la société Actelis Networks. Les câbles qui sont fournis par le client doivent adhérer aux normes des autorités d'inspection et relèvent de la responsabilité du client. Pour diminuer le risque d'incendie, assurez vous que les câbles soient sur la liste UL ou certifiés CSA.
11. Cet équipement doit être installé en fonction des codes d'électricité du pays. En Amérique du Nord, l'équipement doit être installé suivant le Code National d'Electricité Américain, Articles 110-16,

110-17 et 110-18 et suivant le Code d'Electricité Canadien, Section 12. Si nécessaire, consultez les organismes de réglementation et les autorités d'inspection appropriés pour vous assurer de la conformité de l'installation.

12. Protection en cas de courant excessif: nous recommandons d'ajouter un appareil de protection 2A Min. - 5A Max., facilement accessible dans le circuit électrique de l'immeuble. Un appareil de protection à circuit 5A peut alimenter 2 unités ML700 placés l'un sur l'autre en étagères.
13. L'équipement doit être connecté à un système d'alimentation mis à la terre correctement.
14. Tout équipement à proximité immédiate doit avoir la même mise à la terre et ne doit pas avoir une mise à la terre ailleurs.
15. Ne placez pas un appareil déconnecté dans le circuit mis à la terre entre la source d'alimentation DC et la connexion au circuit mis à la terre.
16. Lors de l'utilisation d'un port fibre optique, ne regarderez plus jamais le laser d'émission alors qu'il est sous tension. Aussi, ne jamais regarder directement la fibre port TX et le câble de fibre se termine quand ils sont sous tension.
17. Dans le cas d'une alarme FAN, vous devez remplacer le ML700 dans les 4 heures qui suivent.

Prévention des décharges électrostatiques (ESD) Dommages

1. Lorsque vous travaillez avec des composants électroniques, portez un bracelet antistatique mis à la terre pour décharger l'électricité statique de votre corps en conformité avec les normes approuvées.
2. Ne pas utiliser d'appareils capables de générer ou maintenir une charge statique dans la zone de travail où vous installez ou supprimez des composants électroniques. Éviter de manipuler les composants électroniques dans des endroits qui ont un sol capable de générer une charge statique.
3. Ne pas faire glisser les composants électroniques sur une surface quelconque. Ne touchez pas les broches du connecteur exposés. Manipulez les composants électroniques aussi peu que possible.
4. Transporter et stocker les composants électroniques dans un sac ou conteneur antistatique approuvé.

Avis aux consommateurs

Le produit Actelis acheté est soumis aux dispositions de la directive 2002/96/CE du Parlement européen et du Conseil de l'Union européenne sur les déchets d'équipements électriques et électroniques (DEEE) et, dans les juridictions qui adoptent cette directive, est marqué comme mis sur le marché après le 13 août 2005, et ne doit pas être jeté avec les déchets municipaux non triés. Veuillez utiliser vos installations de collecte DEEE locales pour la disposition de ce produit et sinon observer toutes les exigences applicable.

Allgemeine Sicherheitshinweise

1. Lesen Sie alle Warnhinweise und Anweisungen zu diesem Produkt, welche in diesem Handbuch hervorgehoben sind.
2. Installation oder Austausch von Baugruppen muss von qualifiziertem Personal durchgeführt werden.
3. Bevor das Gerät eingeschaltet oder eine Baugruppe eingesetzt wird, die korrekte Erdung überprüfen.
4. Die Switche nutzen eine externe Gleichspannungsquelle. Vermeiden Sie den Kontakt mit freigelegten Anschlüssen, Kabeln oder Komponenten, wenn die Spannung eingeschaltet ist.
5. Die Switche **nicht** in Betrieb nehmen, wenn Frontplatten entfernt wurden, eine mechanische Beschädigung oder ein Defekt der elektronischen Bauteile vermutet wird.
6. Die Switche **nicht** in einer nassen, feuchten oder explosiven Umgebung in Betrieb nehmen.
7. Oberflächen sind trocken und sauber zu halten.
8. Stellen Sie die Lüftung sicher.
9. Beachten Sie die Angaben und Hinweise auf dem Produkt. Nur die für dieses Produkt empfohlenen Sicherungen verwenden. Bevor Sie Anschlüsse an die Switche durchführen, bitte sorgfältig die Hinweise in den Benutzerhandbüchern durchlesen.
10. Viele der an die Switche angeschlossenen Kabel, werden von Actelis Networks geliefert. Kabel welche nicht von Actelis Networks geliefert werden, müßen den sonstigen Sicherheitsvorschriften entsprechen. Um Risiken zu vermeiden, sollten Kabel UL oder CSA zertifiziert sein.
11. Die Switche müssen entsprechend den Ländervorgaben für elektrische Anlagen installiert werden.
12. Überstromschutz: Es wird empfohlen den Stromkreis mit mindestens 2A bis maximal 5A abzusichern. Ein Stromkreis mit 5A Absicherung kann typischerweise zwei ML700 Switche speisen.
13. Die Geräte müssen an eine richtig geerdete Speisungsquelle angeschlossen werden.
14. Benachbarte Geräte sind in der gleichen Weise zu Erden und nicht auf anderem Wege.
15. Ein Abschaltmechanismus in dem Erdungsanschluss zwischen der Gleichspannungsquelle und der Erdung ist nicht zulässig.
16. Niemals ein Übertragungslaser betrachten, während dieser eingeschaltet ist. Niemals direkt auf den Faser-TX-Anschluß und auf die Faserkabelenden schauen, während diese eingeschaltet sind.
17. Im Falle der Fehlermeldung (HWFLT- Fan Failure), wird empfohlen den Lüfter innerhalb von 4 Stunden auszutauschen.

Schutz vor elektrostatischer Entladung

1. Beim Arbeiten mit elektronischen Komponenten, muss ein entsprechendes Erdungsband getragen warden, um elektrostatische Spannungen vom Körper abzuleiten entsprechend der zugelassenen

Standards.

2. Nutzen Sie keine Geräte in dem Arbeitsbereich, welche eine elektrostatische Ladung hervorrufen können.

   Vermeiden Sie das Hantieren der Switche in elektrostatisch kritischen Fussboden -oder Tischumgebungen.
3. Vermeiden Sie die Switche auf rutschige Oberflächen zu stellen.
4. Transportieren Sie die Geräte nur in passenden antistatischen Verpackungen.

Hinweis für Endverbraucher

Das gekaufte Actelis Produkt unterliegt der Richtlinie 2002/96 / EG des Europäischen Parlaments und des Rates der Europäischen Union über Elektro- und Elektronik-Altgeräte (WEEE). Es wurde unter Anwendung der Direktive nach dem 13. August 2005 auf den Markt gebracht und sollte nicht als Haushaltsmüll entsorgt werden. Bitte nutzen Sie Ihre lokale WEEE-Sammelstelle für die Entsorgung des Produkts und beachten Sie auch alle sonstigen Vorschriften.

Contents

1 Introduction

This chapter introduces ML700 Actelis devices, the basic architecture and the most common topologies in which ML700 devices can be installed. The descriptions differentiate between various types of ML700 product models.

About ML700

Actelis Networks ML700 Ethernet Access Devices (EAD) is further complementing Actelis ML 600 product line, through offering a cost-effective delivery of Ethernet in the First Mile (EFM) high-speed Carrier Ethernet services over the existing copper infrastructure.
The ML700 is designed for point-to-point topologies as well as a CPE only product, working with approved 3rd party DSLAM vendors, serving backhauling of IP DSLAM and cellular base stations and delivering asymmetrical Ethernet traffic, using EFMPlus Bonding over multiple copper pairs with xDSL transmission.

ML700 models offers extended rate and reach performance through bonding of DMT (ADSL2, ADSL2plus and VDSL2) technologies. The choice between the technologies can be made either manually (user selected) or it can be automatically selected by the system from a list of allowed xDSL technologies.

All ML700 models support a single EFM Bonding interface – High Speed Link (HSL). The HSL represents an Ethernet-like logical port that contains up to 8 (model dependent) xDSL ports.

ML700 Link performance may be farther increased on long loops by deploying Actelis' BBA (Broadband Accelerator) amplifiers in the loop.

ML700-O and ML700-R models are not convertible; thus appropriate models should be used on Central Office and Customer Premises Equipment.

➢ ML700 Capabilities

- Ethernet traffic throughput: 500Mbps (Downstream)/250Mbps (Upstream)
- Fully configurable xDSL transport layer, using TR-165 and TR-252 Vector of Profiles management model
- Enhanced DSL robustness using SRA (Seamless rate Adaptation), G.998.4 (retransmission) and INM (Impulse Noise Monitoring)
- Ethernet ports – 4x10/100Base-TX and 2x100/1000Base-FX ports, with various SFP modules supported
- Advanced QOS features, fully compliant to MEF10.2 standard
- ML700 models support Ethernet OAM, fully compliant to 802.3ah OAM, 802.1ag CFM and Y.1731 Ethernet OAM standards
- ML700-R models – interoperable with most IP/ Ethernet DSLAM, supporting IEEE 802.3ah Ethernet Packet Transport Mode (PTM), with EFM Bonding (aggregation over multiple copper pairs), with or without vectoring.

ML700 Models

A range of ML700 models are available for special implementations. The models are either CO (-O) or CPE (-R) specific units and support either 2, 4 or 8 DSL ports. The full specifications for the ML700 models are provided in **Appendix A – Technical Specifications** (on page A-1). This section provides a general description for each model as follows:

Table 1: ML700 Models

Model	CO/CPE	DSL Copper-pairs	Part Number
ML748-O	CO	8	501RG0137
ML748-R	CPE	8	501RG0237
ML744-O	CO	4	501RG0156
ML744-R	CPE	4	501RG0256
ML742-O	CO	2	501RG0228
ML742-R	CPE	2	501RG0229

ML700 Architecture

This section describes the general architecture of ML700 family of products. ML700 architecture consists of the following main functional blocks:

- Ethernet Bridge and Control – supports Ethernet (ETH-x) and Ethernet-like (HSL-1) Service ports, provides 802.1Q VLAN-aware bridging between these ports, system control and management functionalities.
- EFM Bonding – part of HSL-1 Ethernet-like service port functionality. Supports IEEE 802.3ah /ITU-T 998.2 G.BOND/Ethernet aggregation functionality with transmission and reception of Ethernet frame via multiple modems.
- DMT Modems – 2, 4 or 8 modems options (model dependent). Modems support the following transmission modes: either ADSL2 (ITU-T G.992.3), ADSL2 Plus (ITU-T G.992.5) or VDSL2 (ITU-T G.993.2).

NOTE: ML700-R when operating in a P2MP (point-to-multipoint) system with approved DSLAM vendors will work using EFM bonding as defined in IEEE 802.3ah.

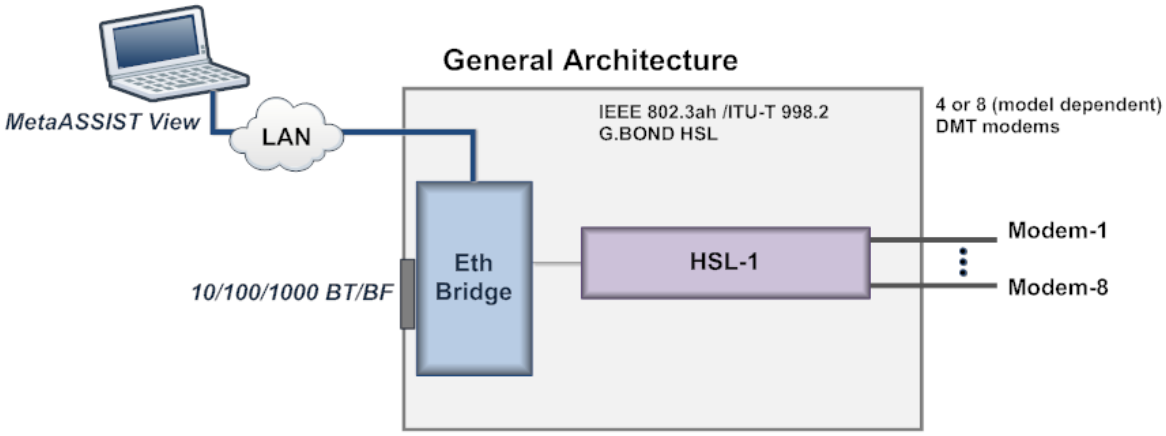


Figure 1: ML700 Architecture

ML700 Topologies

ML700 systems support the following topologies:

- Point to Point Topology, with and without BBA link accelerators
- CPE only for third party CO unit

ML700 Applications:

- Backhauling for Remote (IP) DSLAM
- Backhauling for Cellular Base Station
- Business Asymmetrical Ethernet Services

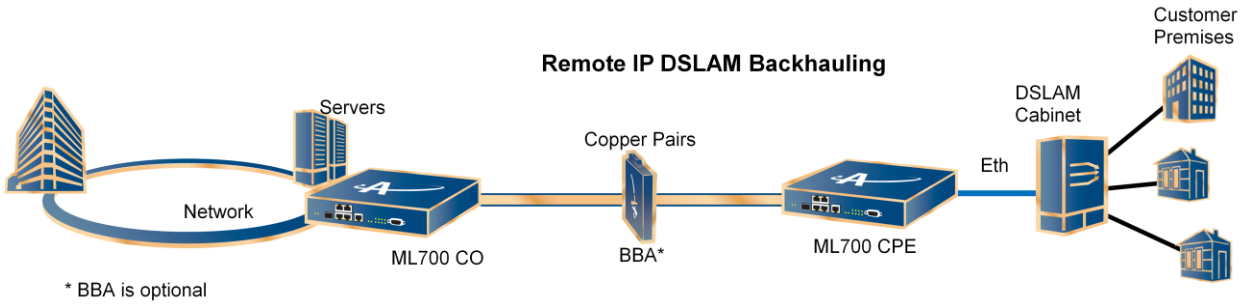


Figure 2: Remote IP DSLAM Backhauling

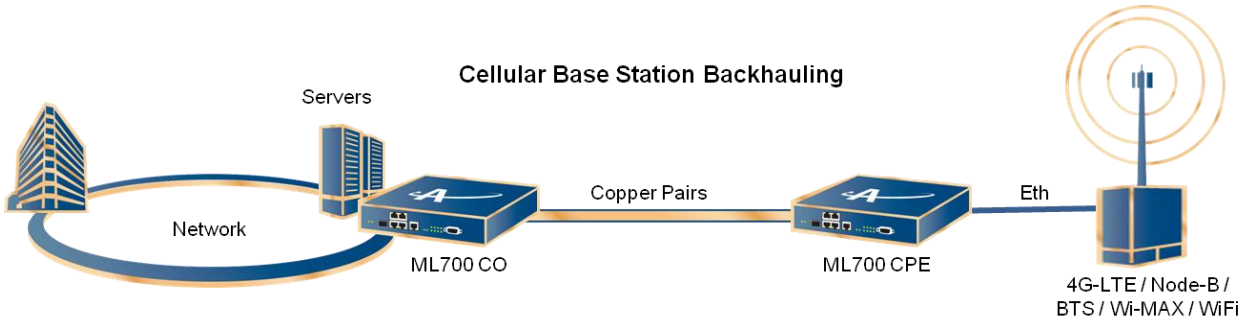


Figure 3: Cellular Base Station Backhauling

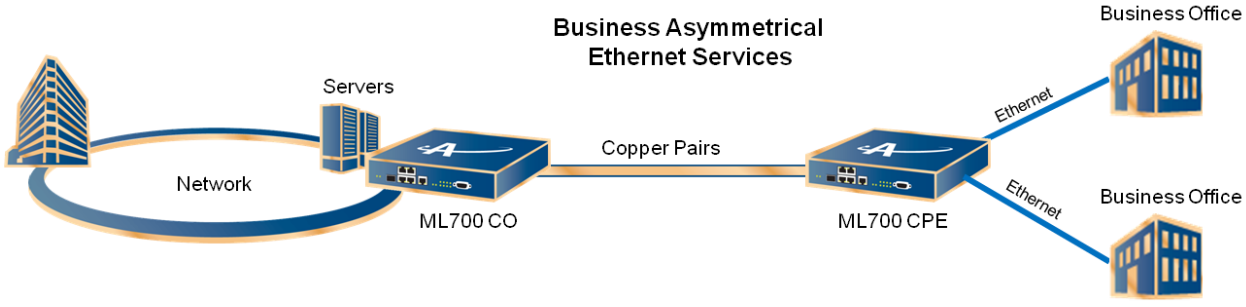


Figure 4: Business Asymmetrical Ethernet Services

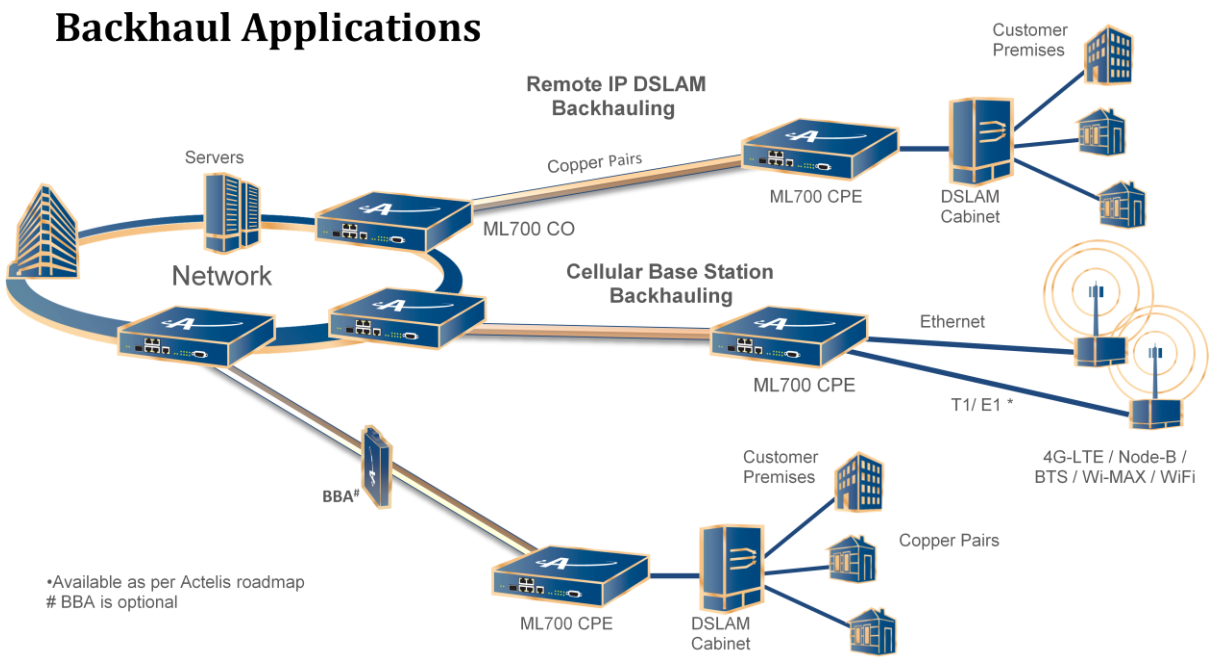


Figure 5: Mix of Applications

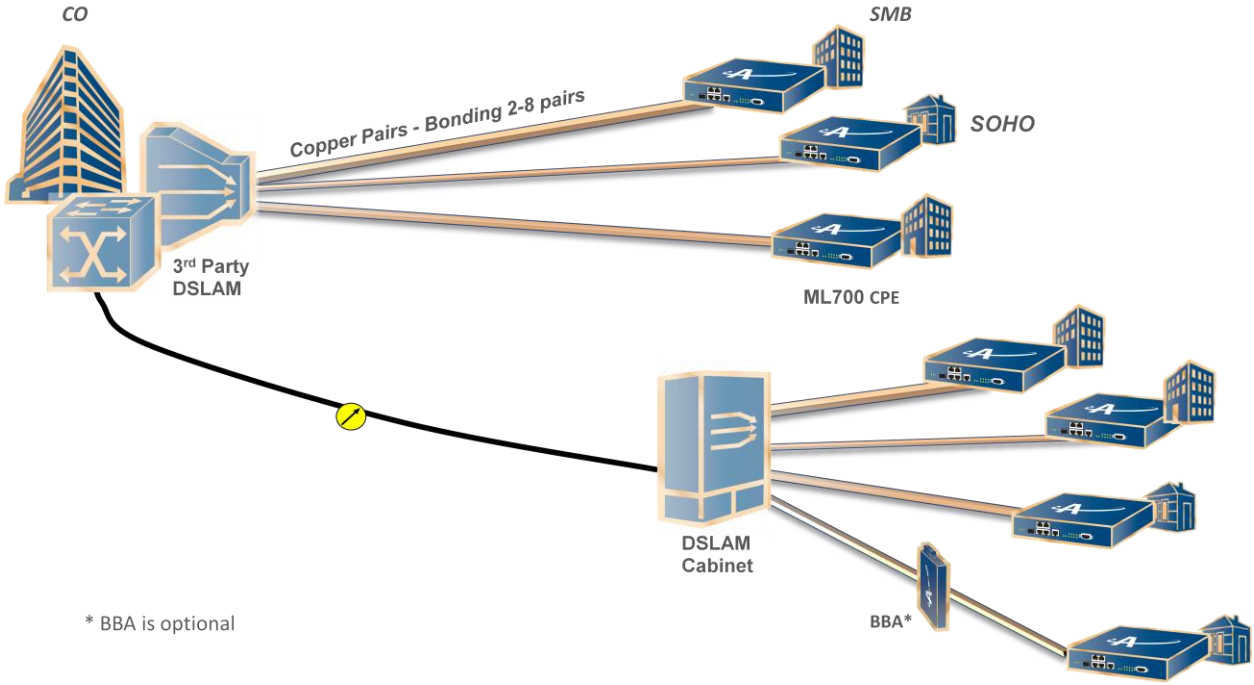


Figure 6: Business Ethernet Services with 3rd party DSLAM CO unit

Management

Actelis elements can be managed through the following range of options:

- **MetaASSIST View** (Registered Trademark) - a Java based Graphical User Interface (GUI) application used for local and remote management of a connected ML system and (in case of an ML CO) its hosted ML CPE elements. The application is distributed with the ML SW (CD) (or in case of ML2300 (SDU-400) is also available in ML file system). This manual describes the management procedures as performed through the MetaASSIST View.

  If the MetaASSIST View is not already installed on the computer to be used for the commissioning procedure, install it according to the instructions given in the *MetaASSIST View Installation Guide*.

- **MetaASSIST EMS** (Registered Trademark) - a Java-based modular and scalable Graphical User Interface (GUI) application enabling system-level management to converging Actelis systems on the entire network. MetaASSIST EMS consists of MetaASSIST EMS server and MetaASSIST EMS client and requires the MetaASSIST View application. To obtain these software applications and the MetaASSIST EMS Online Help contact your local Actelis Networks sales representative, service representative or distributor.
- **WEB Access** - enables performing basic operation on the system from any standard Web Browser, embedded with ML SW.
- **TL1** - intrinsic user interface based on Transaction Language 1 (TL1): a universal transaction language developed by Telcordia Technologies, Inc. The application is embedded with ML SW.
- **CLI** - intrinsic user interface based on Cisco-like Command Line Interface. The application is embedded with ML SW.
- **SNMP** - intrinsic user interface uses standard and Actelis proprietary MIB modules. SNMP agent embedded with ML SW supports either SNMP v1 or V2c protocol.

ML700 Front and Rear Panel Descriptions

This section describes the ML700 front and rear panel connections and LEDs.

ML700 Front Panel Description

ML700 front panel contains the Ethernet service ports and the management connection ports. The following example shows the ML700 interfaces.

Note the following:

- The front panel contains all the LED indicators including those of the rear panel (copper pair) ports
- All the Ethernet ports (10/100 BaseT, SFPs, MGMT and HSL) have dedicated ACT and LNK LEDs
- Unit level LEDs are at the side of the panel

NOTE: Refer to ML700 Quick Installation Guide for the installation procedure.

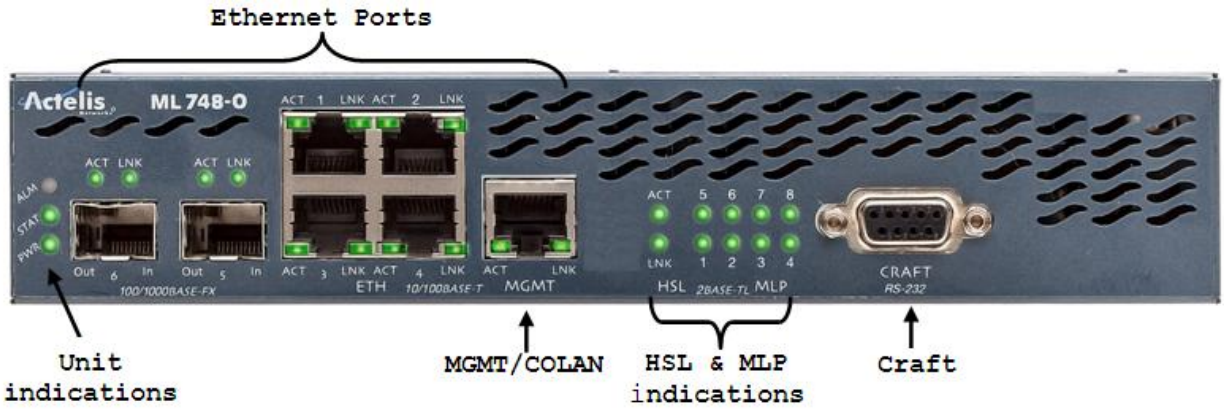


Figure 7: Front Panel Connections

Table 2: Front Panel Port Description

Interface	Description
ETH 1..4	Four 10Base-T/100Base-TX FULL/HALF/AUTO Ethernet service ports (RJ-45). Ports 3 and 4 do not support 10Base-T FULL/HALF option
ETH 5..6	Two 100Base-FX/1000Base-X FULL/AUTO Ethernet service ports with sockets for various SFP modules.
MGMT	10Base-T/100Base-TX FULL/HALF/AUTO Ethernet port (RJ-45) dedicated for IP-based management. Referred in GUI/TL1and CLI as COLAN AID
CRAFT RS232	RS232 port dedicated for IP-less management, used for initial setup and local monitoring

Table 3: Front Panel LED Description

Interface	Description
LNK, ACT Port level LEDs	Each Ethernet port has two LEDs: LNK (LINK) - status of connectivity with opposite port: UP (Green) - logically blocked , i.e. by STP (Yellow); DOWN (Off). ACT (ACTIVITY) - status of activity on port (sending or receiving frames). LED is OFF if Activity is not detected. See **ML700 LED Fault Indications** (on page 15-3).
Power, Status, Alarm, Unit Level LEDs	Unit level LEDs: • Power – Input power detection. • Status – Indicates general status of unit. • Alarm – The alarm criteria of this LED are configurable according to System Configurable Attributes. See **ML700 LED Fault Indications** (on page 15-3).
MLP LEDs	Indicate status of the copper-pair ports located on the device rear panel. Each LED indicates the synchronization status of corresponding modem.

ML700 Rear Panel Description

The ML700 rear panel contains the copper-pair connections, power, alarms and reset switch.

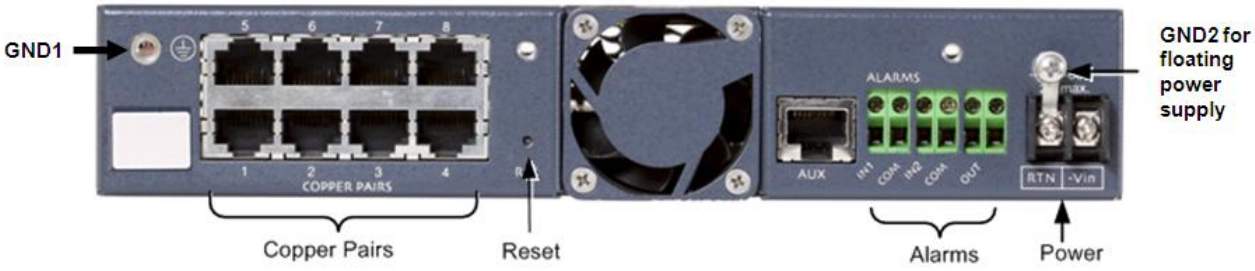


Figure 8: Rear Panel of ML-700 Model

Table 4: Rear Panel Interfaces

Interface	Description
Copper Pairs	Ports for connection of copper pair wires. 2, 4 or 8 ports (model dependent).
Reset	Reset button. Restarts software with current or factory setup depending on the time duration which it is pressed: • Pressed for up to 10 seconds - restarts with current configuration. • Pressed for more than 10 seconds - restarts with factory setup.
ALARMS inputs	IN1/IN2 - Two Normally Open (NO) inputs. OUT - one Normally Open (NO) relay output.
Power	DC Barrier Terminal Block for DC power input. Power requirement: -48 VDC nominal (-40 to -60 VDC max), 2 Amperes maximum (17W maximum for ML740).
GND1	Units' main Grounding.
GND2	Grounding option for a floating AC/DC converter, refer to ML700 Quick Installation Guide document for details.

ML700 link with BBA units

This section describes ML700 link with BBA units. ML700 Link performance may be increased on long loops by deploying Actelis' BBA (Broadband Accelerator) amplifiers in the loop. Links' performance with BBA depends on span's loop length, BBA location (distance from CO unit and BBA), spectral regulations and environmental noise.

ML700 and BBA installation

BBA unit is line power fed from the ML700-O unit, no option for local power feeding. Contact Actelis' customer support for Express powered BBA roadmap. Links' performance with BBA depends on loop topology and available location for BBA placement. Contact Actelis' customer support for BBA installations guidelines and BBA performance calculator.

2 Getting Started

This chapter provides information on how to connect to and navigate the MetaASSIST View.

In This Chapter

Commissioning Procedure

To install the ML unit and equipment properly, use the **Installation Guide** (provided on ML CD) to assist in the installation.

➢ **To start the configuration procedure**

- The management host/PC and ML unit must be connected via the CRAFT port. Since the IP addresses of ML devices are initially set (factory default) to 0.0.0.0, the COLAN port cannot be used for telnet connection.
- The CRAFT port setting on the management host/computer should match the ML device. Initially (after factory setup) all ML devices accept 9600 bps baud rate.
- See **Appendix C with Step-by-Step Commissioning procedure** (on page C-1)

Craft Connection to the ML

Craft sessions are usually used during the setup procedure. After defining the basic parameters, the unit is accessed remotely. This section briefly discusses how to open a Craft session. *For more information on all the available auto-discovery and session access parameters, refer to Management Configuration.*

The IP of the desired ML can be determined or input using he following options:

- Entering the required IP
- Selecting the IP from the available list of successfully accessed IPs
- Using **Auto-discovery** (on page 3-7)

All hosted CPEs are automatically displayed under the accessed CO. The user can determine whether sessions can be opened to the displayed CPEs.

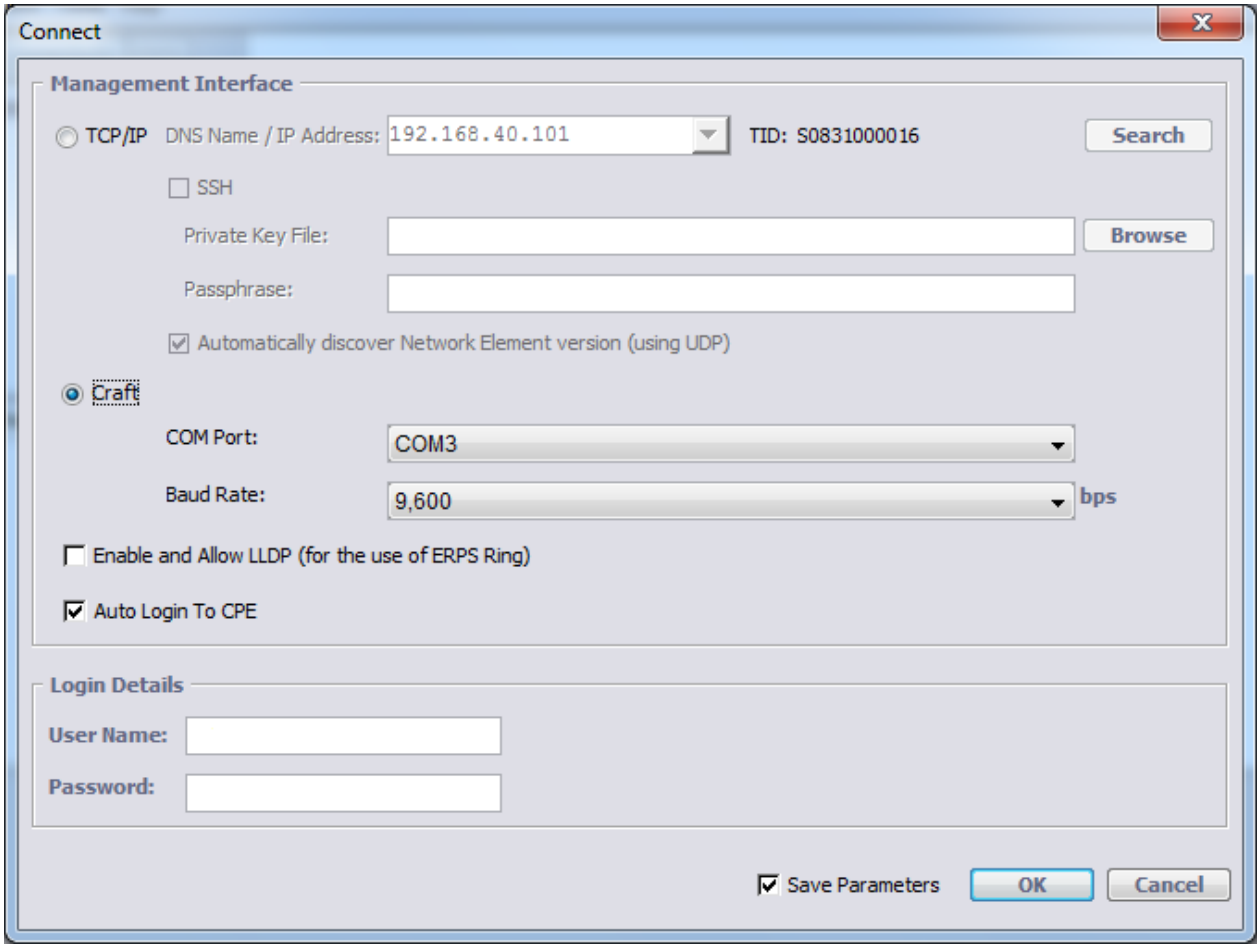
➢ To open a local session to the ML

1. Interconnect the computer's RS232 port and the ML device front panel Craft port using a standard RS232 cable.
2. Launch the MetaASSIST application by doing one of the following:

   - Click the MetaASSIST View  icon on the Desktop, or
   - From the Start menu, select Programs> Actelis Networks>MetaASSIST View.

   The MetaASSIST Main window opens and the Connect dialog is automatically invoked.

NOTE: For basic information on navigating the MetaASSIST Main window, refer to MetaASSIST View Workplace. To resolve unsuccessful connections, see Resolving Management Connection Problems.



3. Under Management Interface:
   - Enable the **Craft** option.
   - Select the computer COM port to which the ML unit is currently connected.
   - Set the Baud Rate according to your computer setting: 4,800, 9,600 (default), 19,200, 38,400, 57,600 or 115,200 (bps)

     Computer COM1/COM2 ports are usually set to 9600 baud rate. If your computer is set to operate with a different baud rate than the one configured on the ML unit, change the computer setting to match the Craft port setting. (There is no auto-negotiation on the Craft port).

     You may also change the baud-rate from the Management Interfaces: In the **Network Element** tree, open **Management Interfaces**. In the displayed pane, **Craft Interface** section, click **Configure** and set the baud-rate in the dialog to match your computer.
4. Determine how sessions will be available to the hosted CPEs displayed under the CO:
   - **Auto Login to CPE** enabled - default setting. All the hosted CPEs will be accessible.

- **Auto Login to CPE** disabled - hosted CPEs will be displayed under the CO but will not be accessible by default. Selected CPEs can be accessed by right-clicking on the CPE of interest and selecting **Auto-connect**.

NOTE: If **Save** Parameters is enabled, the Auto-login settings are saved.

5. **LLDP -** this option is relevant to ERPS. In order to configure ERPS (at a later phase), it is required to enable LLDP.
6. Under **Login Details**:
   - Enter the **User Name**: admin (to perform configuration)
   - Enter the corresponding Password: admin

NOTE: User Name and Password are case sensitive. Change passwords according to **Password Control** (on page 12-8).

7. To save parameters for the next login, checkmark **Save** Parameters.
8. Click **OK**. A new session is opened to the NE. The MetaASSIST View Main window appears.

MetaASSIST View Workplace

MetaASSIST View is a Java based GUI PC application for Configuration, Administration, Monitoring and Troubleshooting for all ML products. The application is supplied on the Installation CD.

NOTE: For more information on all types of sessions, refer to Opening a MetaASSIST View Session.

After opening a session to the ML device, either locally (via a CRAFT connection) or remotely, the MetaASSIST View Main window shows directly connected ML device and all auto-discovered indirectly (via HSL) connected ML devices. View areas are adjustable. Where applicable, panes with tables have a multiple selection feature allowing you to click-and-drag to select multiple rows.

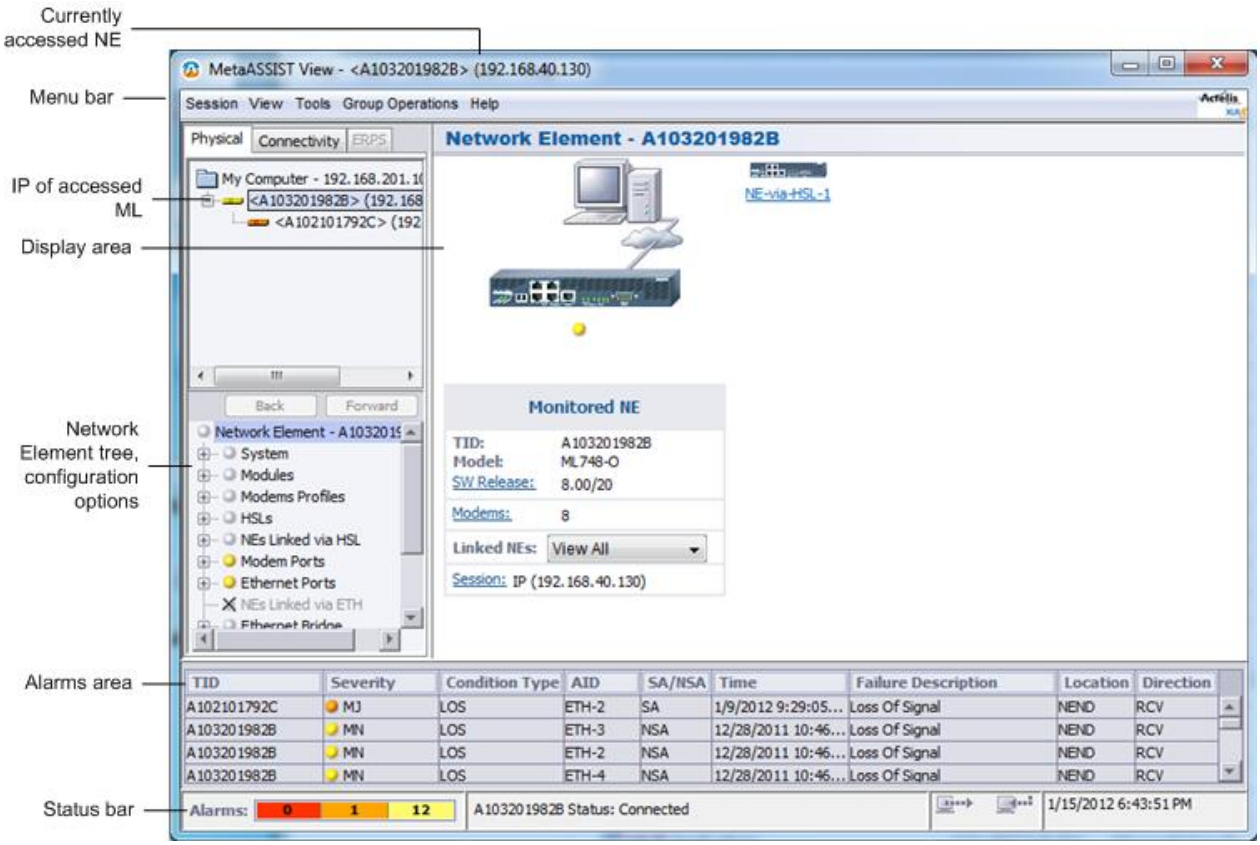


Table 5: Window area options

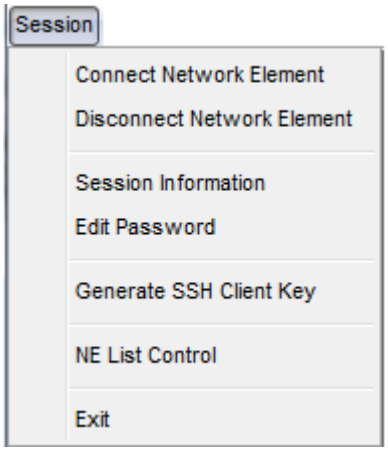
Element	Description
Menu bar	Provides a range of management options, some of which are Group management options that can be simultaneously applied to a group of NEs
Topology area	Shows the CO to which a session was opened, and all its CPEs. This area has two tabs: • Physical - shows the CO and CPEs • Connectivity - provides a range of connectivity analysis options
NE tree	Provides all the management options for the element selected in the Topology area
Alarms area	Shows alarms for ALL elements (CO and CPEs) available in the Topology are

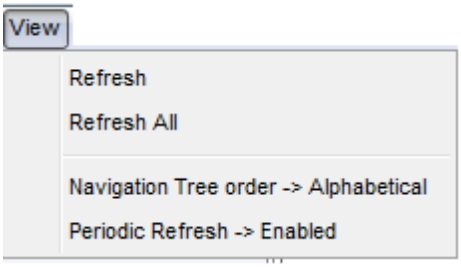
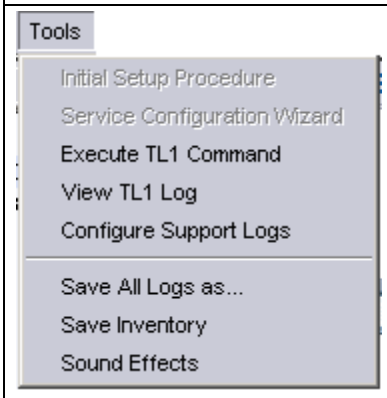
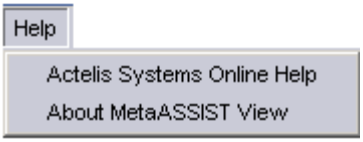
Menu Bar

The menu bar provides you access to the functions as described in the following table.

NOTE: For a description of the terms 'Directly Connected' and 'Indirectly Connected", refer to Opening a MetaASSIST View Session.

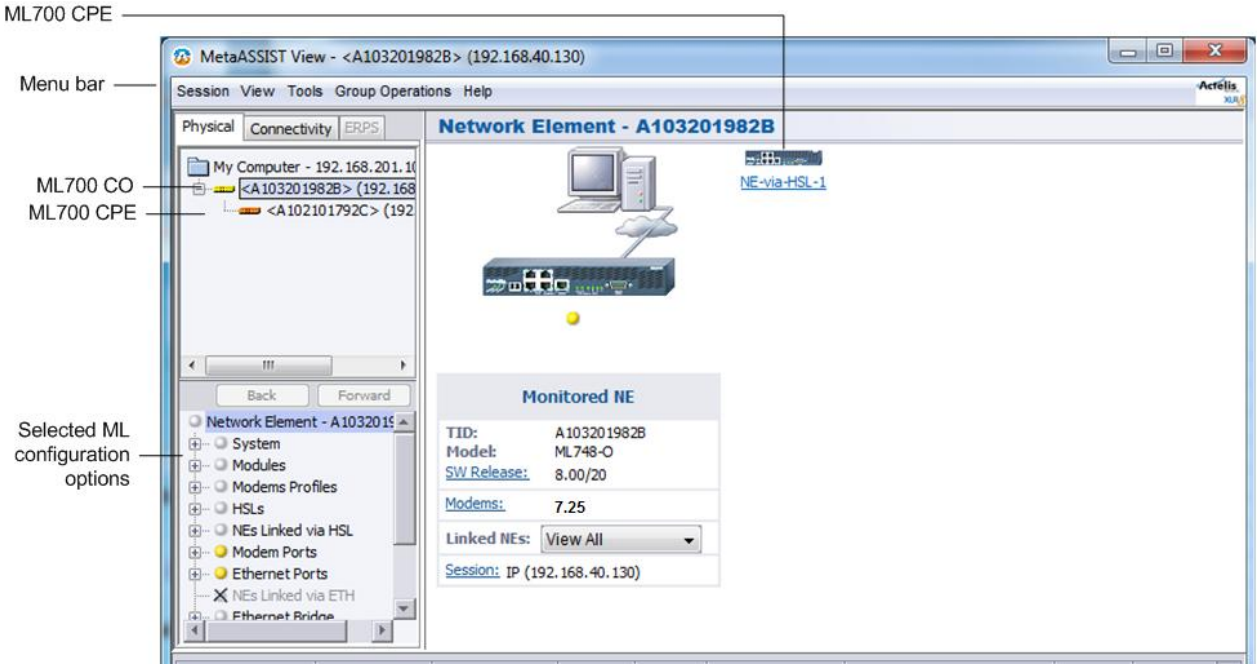
Table 6: Menu Bar Options

Menu	Description
	**Session menu.** Provides options for element connection, password and SSH key generation. • Disconnect Network Element - disconnects the currently connected element and removes it from the NE list • Connect Network Element - invokes the Connect dialog with the list of available NEs • Session information - invokes a summary of the session parameters • Edit Password - change the password of the current user. • Generate SSH Client Key - used to generate new keys for secure connection with ML device (SSHv2) with or without a passphrase • NE List Control - used to maintain updated list of NEs to which sessions have been opened. • Exit - closes the application.

Menu	Description
	**View Menu.** Provides options that determine how the information is displayed and refreshing options: • Refresh - updates information of the currently displayed pane. • Refresh All - updates information on all panes. • Navigation Tree Order - Alphabetical - use to sort the Topology tree elements alphabetically. (Option is available only when the MetaASSIST View session is disconnected.) • Periodic Refresh - when enabled, information periodically refreshed.
	**Tools menu.** Provides TL1 command and log options, in addition to other application response options. • Execute TL1 Command - accesses TL1 Command dialog. • View TL1 Log - shows TL1 Command history and autonomous messages log. • Configure Support Logs - enables field engineers to save, configure and initialize the Info, Install and Blackbox log files • Save All Logs as - used to save all log files to a specified location. • Save Inventory - saves the inventory report on the local disk. • Sound Effects - used to configure audible alarm report indications.
	**Group Operations.** Provides a range of configuration options that can be applied to a selected Group of NEs and is implemented on all NEs belonging to that group. • Users - user account management options. • IP Access Control - Access Control List management options applied to the selected NEs. • SNMP - SNMP configuration options for selected NE or Group. • SSH - **SSH** (on page 12-25) configuration and activation. • Software Release - provides S/W download, activation and SW commit options. Used for downloading new SW to the selected NEs. • Radius - sets **Radius** (on page 12-15) options for selected MLs. • Date and Time - Set Local Time - used to set the date and time to the selected NEs.
	**Help.** Provides help and MetaASSIST View version information. • Actelis Systems Online Help - contains full user manual with advanced search capabilities. • About MetaASSIST View - MetaASSIST View version information.

Physical Tab

The Physical tab is displayed by default. It provides access to monitoring and configuration options for the Network Element (NE) to which a session was opened. If the NE is a CO, this tab also provides access to the hosted CPE. The NE tab space is divided to Topology Tree and NE Navigation Tree.



Topology Tree

The Topology Tree displays the ML device (Network Element or NE), to which a session was opened. If the NE performs as CO (Central Office) device, then the corresponding connected CPE (Customer Premises Equipment) is also displayed.

When opening a new session, pointing to the NE (in the topology tree) shows the current connectivity status (e.g.: *Connecting to NE*).

An icon adjacent to the item indicates the type of device and its status, where the color corresponds to the most severe alarm on the device (Blue - OK, Yellow - Minor, Orange - Major, Red - Critical).

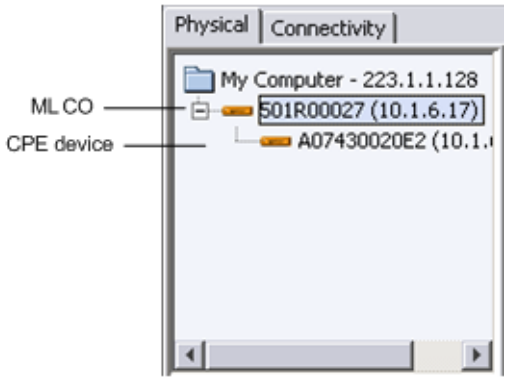


Table 7: Tree element Icon meanings

Tree Element Icon	Meaning
My Computer <IP Address>	Indicates MetaASSIST View running on your computer and shows the IP address of the computer. When the computer is not connected to the LAN (ML NE is monitored via craft), the loopback IP address appears (127.0.0.1). When the IP address of the computer was changed, MetaASSIST View will update the displayed value only when MetaASSIST View is re-started.
	NE connected.
	NE attempting to connect (slanted blue icon).

NOTE: You cannot drag/drop items in the Navigation tree.

MetaASSIST View applies the following features on the assets in this Tree:

- Displays TID (Target Identifier) on successfully logged in NEs for ease of monitoring by logical name;
- Displays IP address when available and indicates full management access.

In most cases, all HSL linked NEs along with the corresponding TID and IP are automatically added during connection. For other cases, see Logging In descriptions.

Network Element Tree

When NE in the Topology tree is selected, the Network Element tree displays selected NE content Navigation Tree. The Navigation Tree includes an expandable/collapsible hierarchy and alphabetical list (user selectable). By clicking a tree element, the appropriate pane appears.

NOTE: The Navigation Tree can be alphabetically sorted only when a session is *not* connected. If you are running a session, you must disconnect to apply alphabetical tree order. To alphabetically order the tree, from the **View** menu option, select **Navigation Tree Order -> Alphabetical**.

Content of the single NE Navigation Tree depends on:

- Logging In User Privilege - some panes require specific (write or admin) permissions and are available only to users with the appropriate access privileges.
- IP address availability - SNMP agent is unavailable for NEs without an IP address.

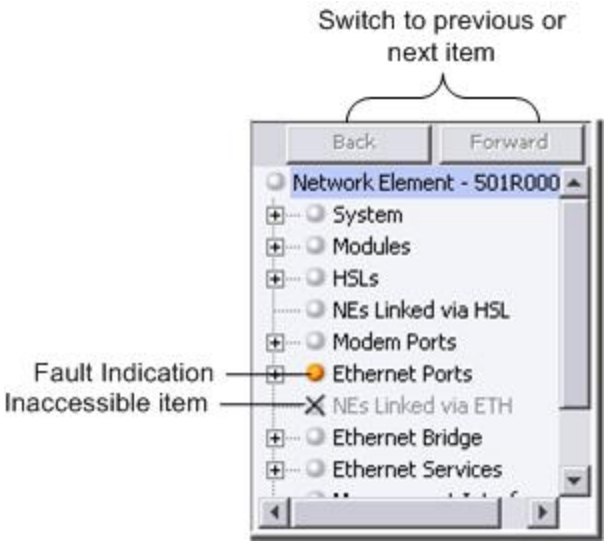


Figure 9: Navigation tree area

The following table describes the icons in the Navigation tree. These also appear in the work area and system alarms table.

Table 8: Icon meanings

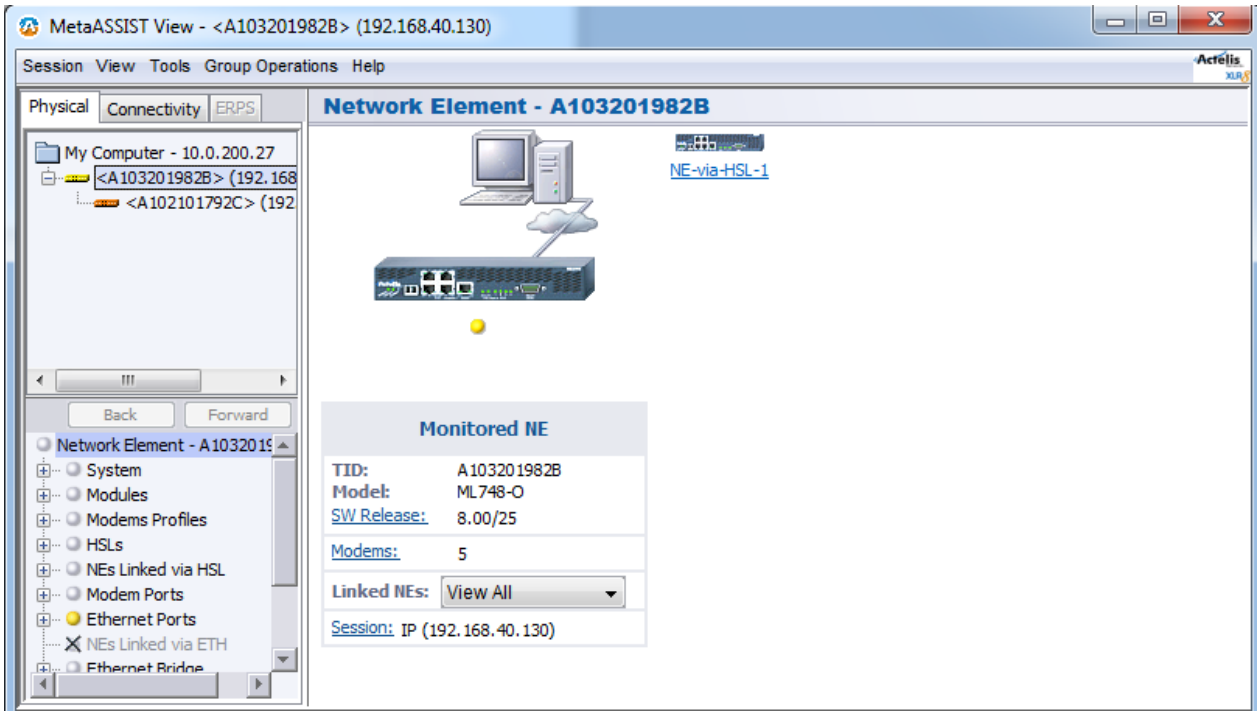
Icon	Meaning
	Gray Icon - for the following cases: ▪ No critical, major or minor alarms; ▪ Entities that have no alarm status (such as Users); ▪ Entities are disabled.
	Red Icon - Critical Alarm
	Orange Icon - Major Alarm
	Yellow Icon - Minor Alarm
	Icon with an x - Inaccessible element
	Tool Icon - Maintenance mode

Network Element Pane

The **Network Element** pane provides a glance view of local Network Element and when applicable, Network Element linked via HSL.

➢ **To access the Network Element pane**

In the Network Element tree, click **Network Element**. The **Network Element** pane opens in the work area.



The Monitored NE is displayed on the left hand side of the Network Element pane along with the following detailed System information: System Name (TID), Model, SW Release, Number of Enabled Modems and IP address. In addition there is a filter, allowing to display linked NEs (All, Enabled, Disabled, Alarmed).

The linked via HSL NE is displayed by a **NE-via-HSL-<ID>** link. In addition, placing the cursor on the NE displays a tool-tip with the following detailed information: System Name (TID), Model, IP address, ETH BW available on the HSL and highest severity Alarm condition (if occurs).

The **NE-via-HSL-<ID>** link behaves as follows:

- Switches to the linked NE **Network Element** pane when HSL up and NE is logged in
- Remains on Local NE and switches to **NEs Linked via HSL** pane when HSL up and NE is not logged in
- Remains on Local NE and switches to **HSL-<ID>** pane when HSL is operationally down or disabled

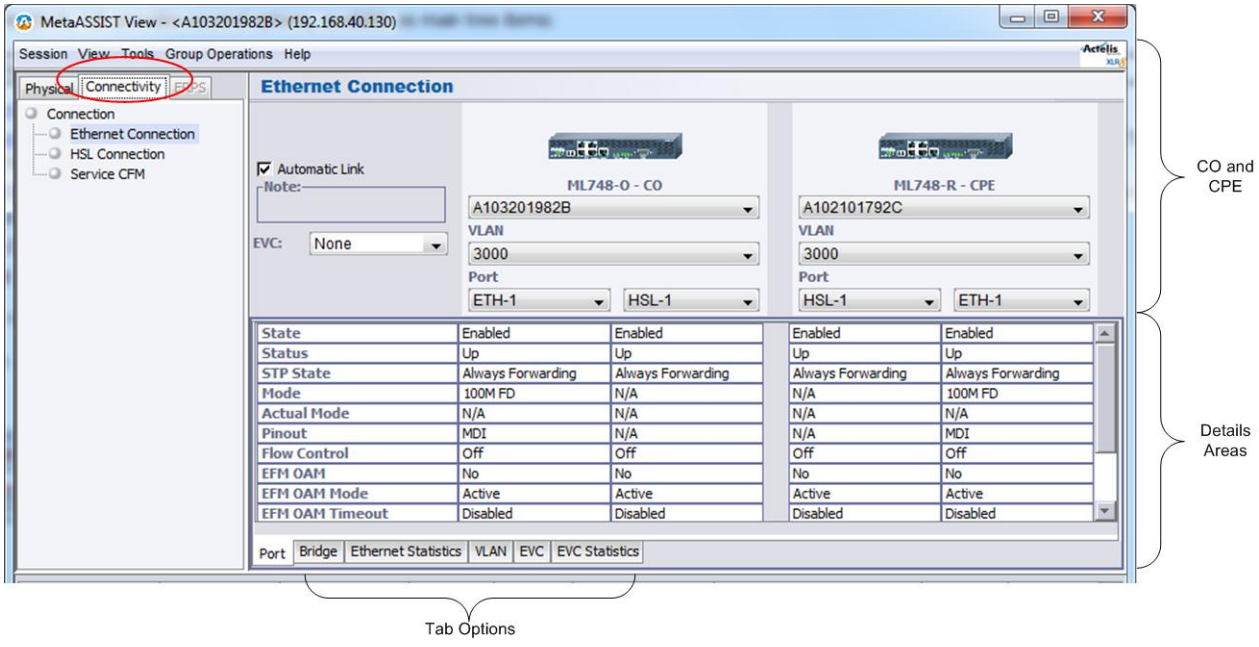
Connectivity Tab

The Connectivity tab provides several options, available as main tree items:

NOTE: The available options may vary depending on your ML700 model.

- Ethernet Connection - used to monitor status and setup of the particular Ethernet Connection (predefined via the Physical tab).
- **HSL Connection** - compares HSL on CO and CPE side (see **HSL Connection Glance View** (on page 13-46)).
- **CFM** - The CFM options are now located in the Physical tab under CFM/Y.1731.

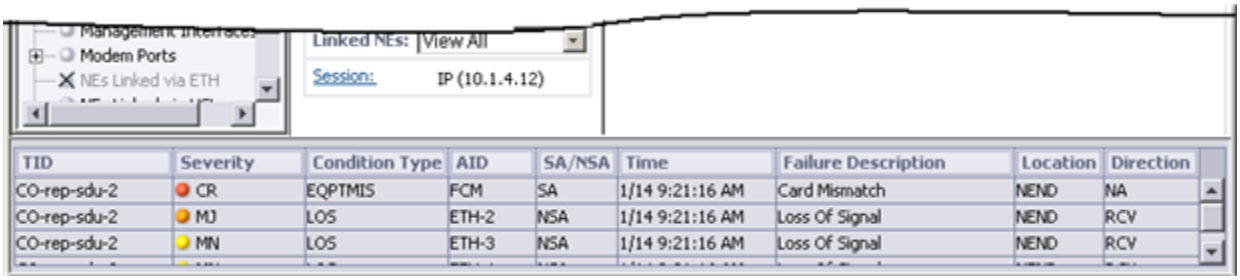
Below is an example of the display invoked when the Ethernet Connection option is selected.



Current Alarms Area

The Alarms Area displays all the current alarms of the Monitored NE alarms. If the NE is CO, alarms of its CPE are also displayed. Alarms are sorted according to severity, starting with the critical alarms, and then by date-and-time.

You can scroll through the table to view additional existing alarms. Clicking on any of the alarms navigates to the appropriate pane.



The Status bar displays the total number of Critical, Major and Minor alarms in the Monitored NE, management (TL1) traffic direction and Monitored NE date-and-time. In addition, when the cursor is placed over the management traffic direction area, a pop-up displaying management traffic statistics appears. It includes the received and sent bytes between the MetaASSIST View application and the Monitored NE.

Refer to **NE Connection Status** (on page 13-3) for a description of the connection status indications.

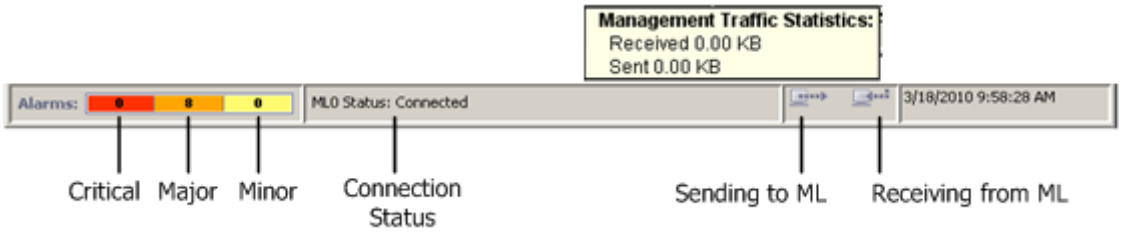


Figure 10: Alarms Area and Status Bar

Multi-lingual Support

All labels in the MetaASSIST View are in English. Any printable 8-bit ASCII-extended characters are valid for all configurable "free string" parameters (i.e. User Name, Password, System, Port ID, etc.).

Typically used ISO 8859-1, also called as ISO Latin1, refines ASCII-extended (8-bit) codes and is sufficient for the most common European languages, including characters such as ß (German), ñ (Spanish), å (Swedish and other Nordic languages) and Ö(Hungarian).

NOTE: MetaASSIST View and MetaASSIST EMS ignore the following: ? (0x3F ASCII code), " (0x22 ASCII code) and /n line feed (0x0A ASCII code) characters.

3 Management Configuration

This chapter describes the connectivity methods and the required configuration procedures.

In This Chapter

NE Management Communication Protocoles and Ports

Each ML NE can be managed via different communication protocols:

- Prompted TL1 via TCP port 3083 (not configurable) - for man-machine interface
- Unprompted TL1 via TCP port 3082 (not configurable) - for machine-machine interface
- Prompted CLI via TCP port 23 (telnet attached) – for man-machine interface
- Discovery Protocol via UDP port 3087 (not configurable) - for ML discovery by MetaASSIST View
- Telnet via TCP port 23 (not configurable) – to provide TL1/CLI connections described above
- SSHv2 via TCP port 22 (not configurable) - for secure TL1/CLI connections described above
- HTTP via TCP port 80 (not configurable) - for file transfer operations
- SNMP via UDP input port 161 (not configurable) and output port 162 (configurable)
- SNTP via UDP port 123 (not configurable) - for date and time auto-synchronization in the LAN
- Radius Client on ML via UDP port 1812 (not configurable) – for auto-authentication by external Radius Server
- Syslog Client on ML via UDP port 514 (not configurable) – for auto-upload of log records to external Syslog Server

Access via each communication protocol can be controlled via Access Control List, see **Managing User Accounts** (on page 12-3).
In addition, **User Account** (on page 12-3) and **SSH features** (on page 12-25) secure TL1 communication protocol

ML Link Visibility via MAV

MAV session connected to an ML NE (CO or CPE) via a CRAFT port, shows indirectly connected CPE or CO NEs (Linked via HSL) only if the following conditions are true:

- CO and CPE are connected by copper pairs.
- The peer NE (either CO or CPE) has “Access from Peer” Enabled (factory setup) – controls IP-less access (via craft port).

  Note: A MAV Craft port session shows CO NE linked via HSL only in P2P topology of ML700 and ML600 models (except for ML688).

MAV session connected to an ML NE (CO or CPE, via ETH-x, COLAN or HSL-x port), shows directly (via ETH-x, COLAN) and indirectly connected (Linked via HSL) NEs if the following conditions are true:

- CO and CPE are connected by at least one copper pair.
- L2 (LAN) and L3 (IP) settings on both ML NE (CO and CPE) are configured correctly. For security reasons, remote (telnet) access to each ML NE can be secured enabling SSH, ACL features on selected NE or by separating IP/LAN network, differently configured on CO and CPE NE.

  Note: If an IP on ML NE is configured (i.e. is different from 0.0.0.0) MetaASSIST View will always try to connect by IP address (also to NEs linked via HSL). If an IP/LAN configuration does not allow connection between this ML and the management host (intentionally or due to configuration mistake) MetaASSIST View will not try to connect by non-IP access.

In mixed configuration (CO NE has IP address and CPE NE does not have IP address), MetaASSIST View will connect to the CPE NE without IP, using non-IP access (also controlled by "Access From Peer").

Note: CPE NE with SW earlier then R5.0a supports basic non-IP access capabilities for monitoring of NE statuses and basic configurations. CPE NE with SW=R5.10 supports full non-IP access capabilities (including file transfer-based features). Note that on any NE with no IP, SNMP communication is disabled.

➢ **It operates as follows:**

To show ML link, MetaASSIST View uses the following ML NE communication abilities:

- Embedded Operational Channel (EOC) - single modem-based connectivity that is always (if modem in synchronized) available from XTU-O modem to access XTU-R modem.
- IP-less Ethernet - based on 802.1ah OAM (Operation Administration and Management) PDU transport connectivity is available between ML devices via HSL ports only. IP-less 802.1ah OAM PDU transport allows full management access, including file transfer.
  Notes:
  - CO NE requires an IP Address to enable file transfer to an IP-less CPE NE.
  - IP-less access from the Peer can be controlled: enabled (factory default) or disabled.
- IP/Ethernet connection - requires configuration of IP Address, Gateway and Subnet Mask configured on the NE. *The MGMT VLAN must be consistently configured on all NEs.*
  Note: The IP/Ethernet access on each NE can be controlled and additionally secured (by ACL or SSH).

Opening a MetaASSIST View Session

➢ **Note the following**

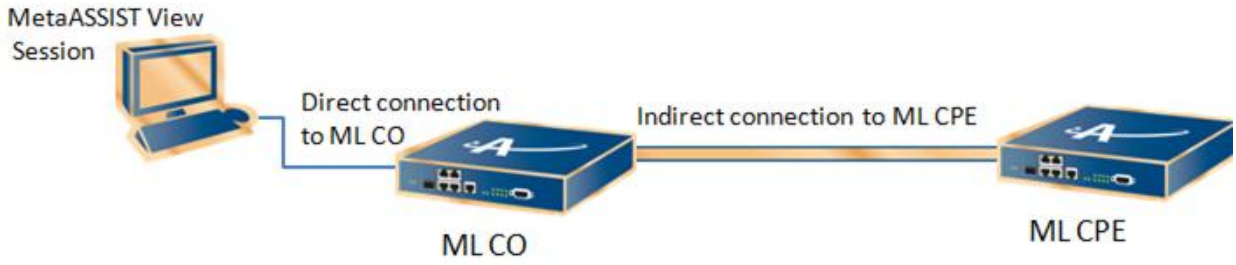
- Sessions can be opened to the ML through various types of connections (local RS232, Ethernet, HSL, etc. - see below), where the session can be direct to the ML or via another unit (indirect).
- Up to 100 Local user/IP-shared accounts are supported - either **RADIUS** (on page 12-15), local DB or a combination of both. The same user account can be re-used from the same or different IP hosts.
- A MetaASSIST View session to the ML is opened using User Name and Password to login to the ML NE. The default User Name and Password are factory set on the ML NE and are modifiable. The indirectly connected MLs are automatically accessed using the same User Name and Password applied to the directly connected ML.
- If configured, a *user defined* **security access warning** (on page 12-2) appears when an ML is accessed.
- Auto-logout (for Write and Admin access privilege) is performed if no user operation was detected for a pre-defined period of time (default on ML NE = 30 minutes). Read-Only users, by default are never logged out (can be reconfigured on ML NE).
- ML units meeting the required criteria are discovered automatically (**auto-discovery** (on page 3-7)).
- ML units that fail to connect are listed in a table and can be analyzed.
- IP/Ethernet connection - The MGMT VLAN must be consistently configured on all NEs. *The IP/Ethernet access on each NE can be controlled and additionally secured (by ACL or SSH).*
- Embedded Operational Channel (EOC) - single DSL mode-based connectivity that is always available for the STU-R NE. EOC is used to detect STU-R NE and to enable remotely configuring IP/VLAN connectivity from STU-C NE (NE with HSL configured in –O mode).

➢ **Types of session connections**

- **Serial RS-232 Craft (on page 2-3)** interface - used mainly for first time set up and can be used to reconfigure IP addresses.
- **Ethernet COLAN (MGMT)** port. By default, this port is *disabled* as a management port and is included in the default MGMT VLAN (VID=100) as untagged member.
- **Ethernet service** port - by default, it is configured for *service traffic* only. Can also be configured for in-band management.
- **HSL** port. Enables indirect access to remote ML systems from the directly connected system. By factory default, all HSL ports are included in default MGMT VLAN (VID=100) as tagged members.

➢ **Types of sessions**

- Direct session - a session terminated by ML NE without another ML NE involved in this connection. Any of the available physical connections (RS232, COLAN, ETH-x) can be used.
- Indirect session - a session terminated by ML NE via another ML NE. Used over HSL-1 Ethernet-like port which cannot be directly terminated by another network device.



TCP/IP Connection to the ML

The Connect dialog provides options for both a local and a remote TCP/IP connection. Local access is described in **Craft Connection to the ML** (on page 2-3). All hosted CPEs are automatically displayed under the accessed CO. The user can determine whether sessions can be opened to the displayed CPEs.

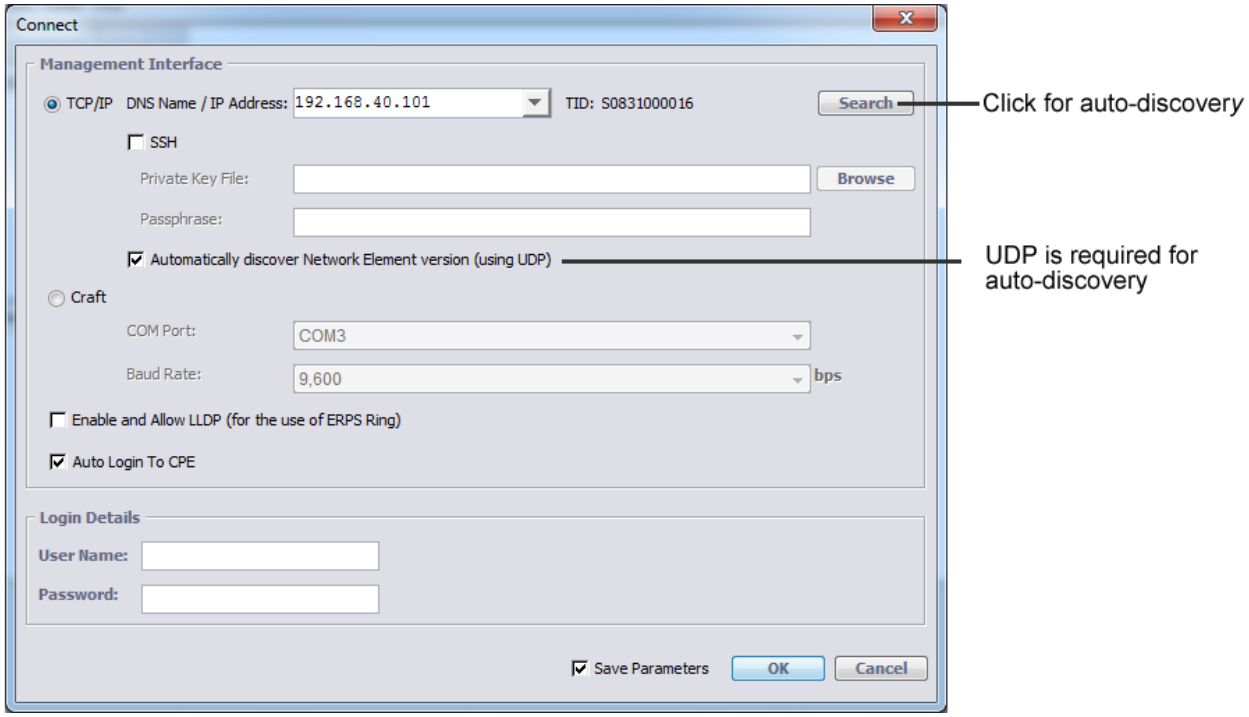
➢ **To open a remote session to the ML**

1. Launch the MetaASSIST application by doing one of the following:

   - Click the **MetaASSIST View** icon on the Desktop, or
   - From the **Start** menu, select **Programs**> **Actelis Networks**>**MetaASSIST View**.

   The MetaASSIST Main window opens and the Connect dialog is automatically invoked.

NOTE: For basic information on navigating the MetaASSIST Main window, refer to The MetaASSIST View Workplace. To resolve unsuccessful connections, see Resolving Management Connection Problems.



2. Under **Management Interface,** enable the **TCP/IP** option.
3. The IP of the desired ML can be determined or input using he following options:
   - Entering the required IP
   - Selecting the IP from the pull-down list of successfully accessed IPs
   - Using **Auto-discovery** (on page 3-7) - verify that UDP is enabled (and UDP traffic is not blocked by a Firewall in your network), and then click the **Search** button. Will discover ML elements in the same management segment (with IP address and connected via HUB or BRIDGE *NOT* via ROUTER).

NOTE: For Management Network in which UDP traffic is blocked by Firewall, uncheck the check-box **Automatically discover Network Element version (using UDP)**. This will allow communication.

4. Determine how sessions will be available to the hosted CPEs displayed under the CO:
   - **Auto Login to CPE** enabled **-** default setting. All the hosted CPEs will be accessible.
   - **Auto Login to CPE** disabled - hosted CPEs will be displayed under the CO but will not be accessible by default. Selected CPEs can be accessed by right-clicking on the CPE of interest and selecting **Auto-connect**.

NOTE: If **Save** Parameters is enabled, the Auto-login settings are saved.

5. **LLDP -** this option is relevant to ERPS. In order to configure ERPS (at a later phase), it is required to enable LLDP.

6. Under **Login Details**:
   - Enter the **User Name**: **admin** (to perform configuration)
   - Enter the corresponding **Password**: **admin**

   NOTE: User Name and Password are case sensitive. Change passwords according to **Password Control** (on page 12-8).
7. To save the configured parameters (Auto-login to CPE, LLDP, etc.) for the next login, checkmark **Save Parameters**.
8. Click **OK**. The MetaASSIST View Main window appears showing the ML CO and ML CPE units elements.

Auto-discovery of ML Systems

MetaASSIST View supports auto-discovery of the ML systems that meet the following criteria:

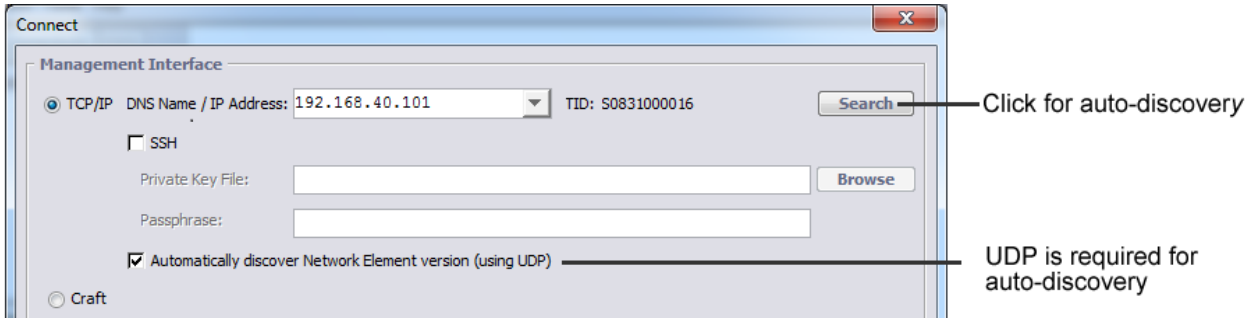
- ML systems that have been assigned an IP address.
- ML devices that are on the same routing segment with a Management host where MAV is installed, i.e. will discover ML devices attached directly, via HUB or BRIDGE devices and will not discover ML devices attached via ROUTER.

NOTE: For auto-discovery to work, the UDP option must be enabled and UDP traffic cannot be blocked by a firewall in the network.

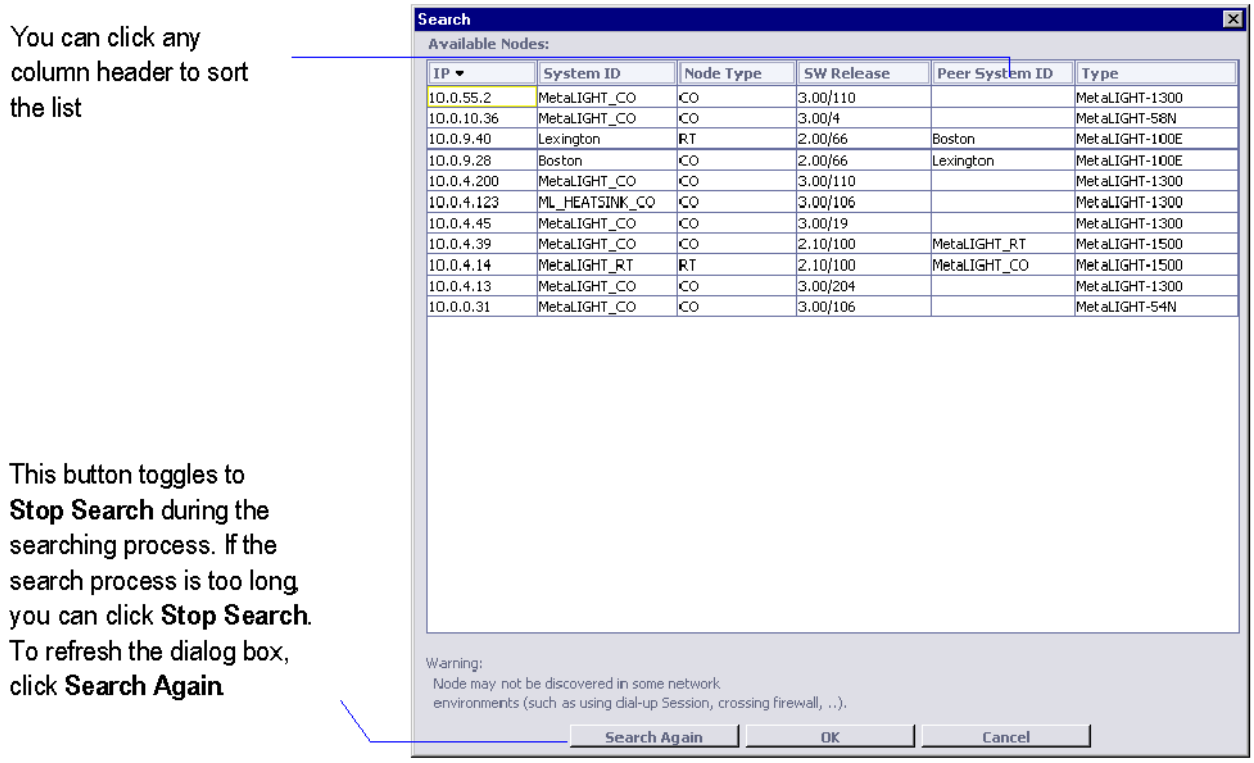
➢ **To discover currently active ML device in the LAN**

Each time the MetaASSIST application is invoked, the Connect dialog appears. In addition to the standard Craft and TCP/IP connectivity options, the dialog provides access to Auto-discovery options.

1. In the **Connect** dialog box, click the **Search** button.



The **Search** dialog appears.



2. In the **Search** dialog box, double-click on an IP address or select it and click **OK**.

NOTE: ML device that cannot be managed by this version of MetaASSIST View are grayed out.

Units that Failed to Connect

Any NE that failed to connect will appear in the Network Navigation tree as a slanted *blue icon* and will be listed in the **ML Failed to Connect or Login** pane. The units are listed in a table according to their corresponding HSLs where for a selected NE CO, the hosted CPE (that failed to connect) is displayed; for a selected NE CPE (if it failed to connect to the CO), then the CO will be displayed.

Options are available for performing common operations such as Restart, SW download, Configuration, etc. that may have caused or resolved the connection problems. An NE may fail to auto-connect due to a wrong IP or VLAN configuration, therefore it is recommended to first check these configurations and change them if needed. After verifying that the IP and VLAN configurations are correct, try to reconnect the NE by clicking the **Login** button.

➢ **To view the device that failed to auto-connect or login and troubleshoot the connection**

1. In the Network Element Tree:
   - Click **Network Elements Linked via HSL** and then **ML failed to auto-connect and/or login** or
   - Click on the corresponding link on the **Network Elements Linked via HSL** pane

The corresponding pane appears in the work area. The pane shows all the ML devices that failed to auto-connect, according to their HSL, along with general information on each device. The operation buttons are described after the figure.

2. Once finished troubleshooting the connection problem, you may attempt to login to the remote NE by selecting the desired **HSL-AID** and click **Login**.

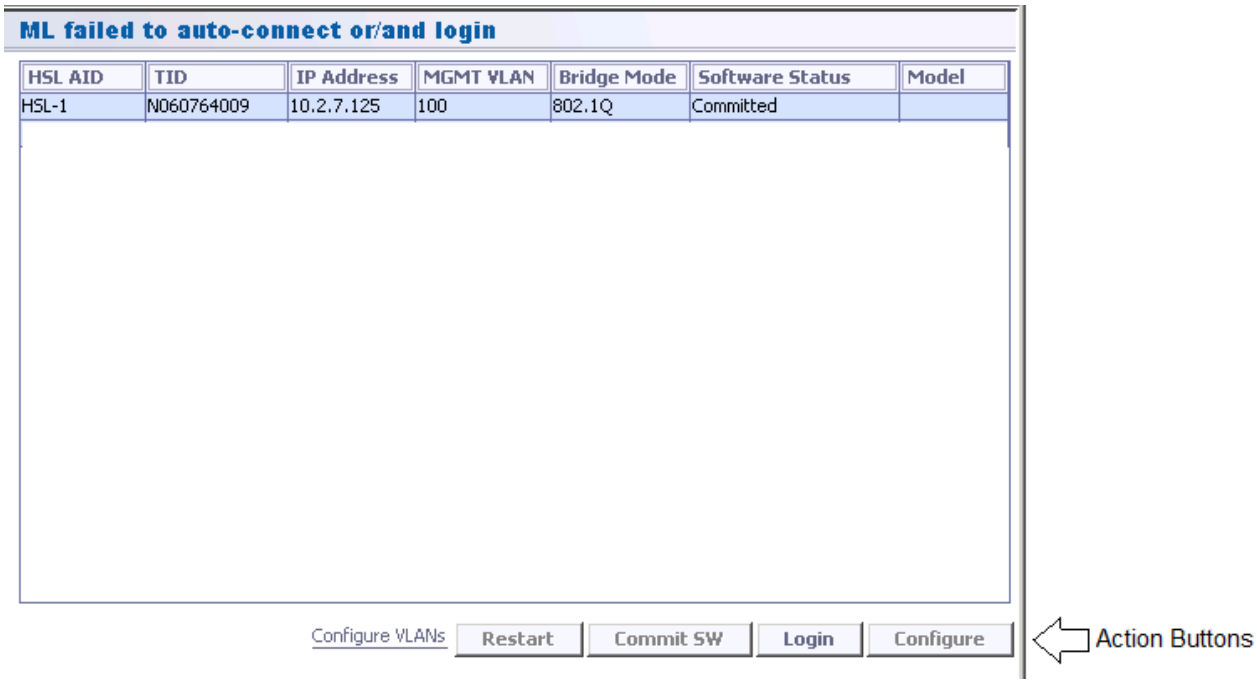


Table 9: Operation buttons

Button	Description
Restart	Restarts the selected device in the pane. Warm (Preserving Setup) or Cold (with Factory Setup) CPE reboot is invoked remotely.
Commit SW	Commit a new SW version (already located on the device). For more details about this procedure, see **Updating the System Software** (on page 14-13).
Login	Initiates a reconnect attempt (it is recommended to use this button after changing the configuration). This may be done on a group of selected NEs.
Configure	Accesses the L2/L3 setting configuration options. Used to change IP, subnet mask, Gateway configuration mismatch or MGMT VLAN configuration mismatch.
Configure VLANs (link)	Accesses the VLAN configurations options of the selected device. For more details about this procedure, see **VLAN Configuration** (on page 8-1).

IP-less Connection to ML (CPE)

IP-less Ethernet connectivity (based on 802.1ah Fast Operation Administration and Management (OAM)) is available between all ML NE models. This type of configuration (NEs without IPs) is suitable for massive deployment of multiple CPE devices and allows comprehensive management of ML hosted CPEs. It allows full management access, including file transfer. IP-less access from the Peer is enabled by default, but can be disabled.

Indirectly connected (linked via HSL) ML NEs can be deployed without an assigned IP Address (IP Address = 0.0.0.0), however some features are not available through the MetaASSIST View or are limited as described in this section.

➢ **Note the following criteria for connecting to a CPE without an allocated IP address:**

- If the CO has an IP address and the CPE does NOT, the CPE will be accessed using non-IP access (also controlled by "Access From Peer").
- An attempt will NOT be made to connect by non-IP access following an unsuccessful configured IP connection attempt.
- An IP-less CPE can only be accessed by one user at a time.
- SSH client and ACL are unsupported on non-IP CPE.
- NE Linked via ETH view is disabled on non-IP CPE.
- CPE NEs support full TL1/MAV capabilities (including file transfer-based features) on non-IP CPEs.
  CPE NEs supports SNMP trap forwarding from non-IP CPE through IP-based CO.

IP/LAN Connectivity on Directly Connected NE

NEs can be connected to the management LAN using an *out-of-band*, dedicated management port COLAN (MGMT) connection, or an *in-band* connection that is implemented through any service port such as ETH or HSL (in relevant MLs).

NOTE: COLAN (MGMT) port is disabled by factory default.

When enabling the COLAN (MGMT), ensure that there are no Ethernet loops between the COLAN (MGMT) and Service ports (ETH or HSL), see **Resolving Non-Alarmed Service Problems** (on page 15-16).

To provide IP/LAN connectivity on a locally connected NE, you will need the Management VLAN, IP address, IP gateway address, and IP subnet mask information from your Network Administrator for each NE installed in the topology.

IP/LAN Connectivity on Indirectly Connected NE

An indirect session can be opened for MLs configured as follows:

- CO and CPE are connected by copper pairs, and configured appropriately: one NE as STU-C NE (HSL configured in –O mode), other NE as STU-R NE (HSL configured in –R mode).
- The peer NE (either CO or CPE) has "Access from Peer" Enabled (factory setup). *When opening a local (craft connection) MetaASSIST View session to an ML700 CPE in a P2P topology, the CO NE linked via HSL is displayed as well.*
- L2 (LAN) and L3 (IP) setting on both ML NE (CO and CPE) are configured correctly. For security reasons, remote (telnet) access to each ML NE can be secured enabling SSH, ACL features on selected NE or by separating IP/LAN network, differently configured on CO and CPE NE.

The IP/LAN on an indirectly connected (via HSL) NE (usually CPE) is configured via the "NE linked via HSL" pane. By default, the system applies all the connectivity parameters (except for the IP Address which should be unique) of the directly connected NE (usually the CO), to the indirectly connected NE (usually the CPE).

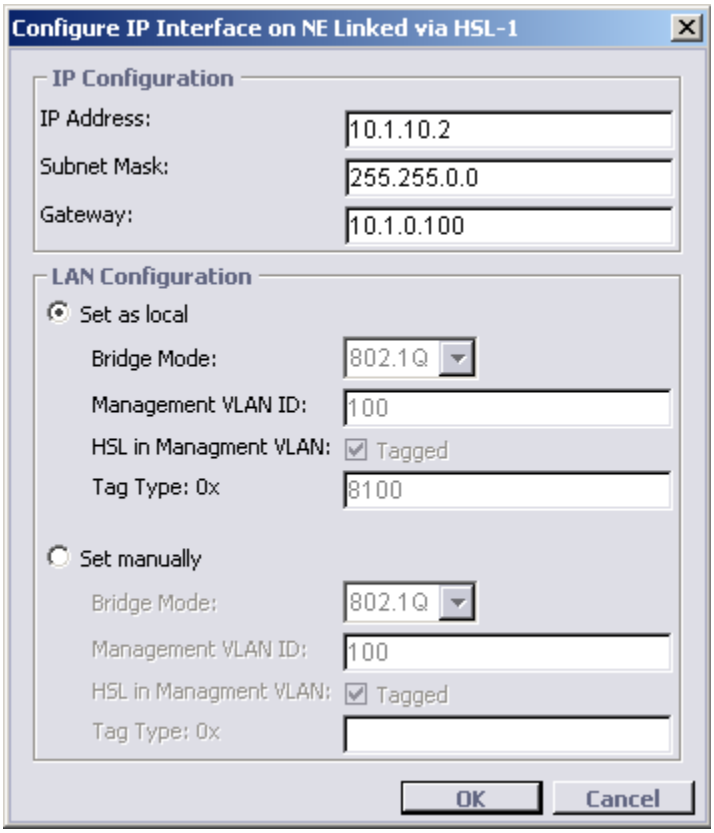
If different IP/LAN parameters are required on the CPE NE, these can be individually modified for each NE. Modifiable parameters include IP gateway address, IP subnet mask, Bridge Mode, Management VID and VLAN membership type.

NOTE: By default, the IP address of each ML NE is set to IP 0.0.0.0. It is required to modify this address to a valid and unique IP address.

➢ To configure LAN/IP on an indirectly connected ML NE

1. Open a session to the CO ML.
2. In the **Network Element** tree, expand **NEs Linked via HSL**. The **NEs Linked via HSL** pane opens.

3. Click **Configure** button. The **Configure NEs Linked via HSL** dialog appears.



4. In the IP Configuration area define the following:
   - IP Address
   - Subnet mask
   - Gateway
5. Set the LAN Configuration parameters using one of the following options:
   - Set as local - Read only - sets the LAN parameters to the same values as those of the host CO.
   - Set manually - initially displays the configuration of the remote NE. The parameters can be modified.
   - Click **OK**.

L2 (MGMT VLAN) Connectivity

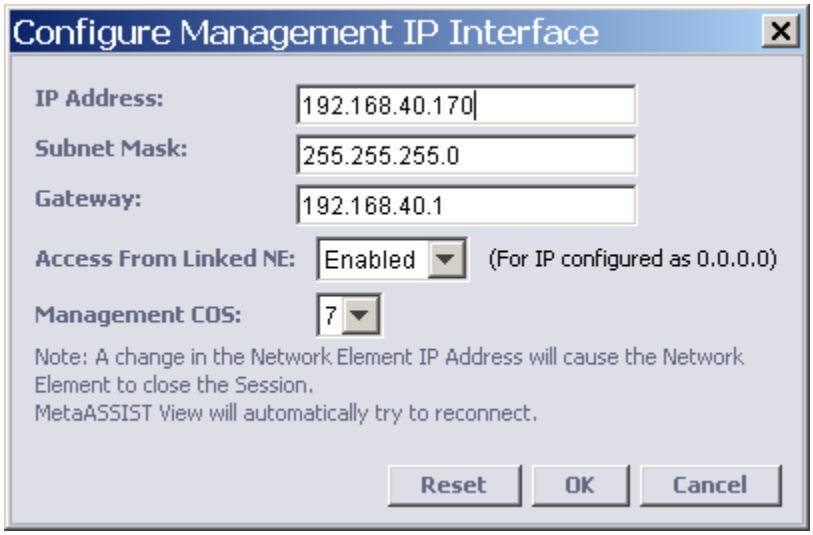
ML700 provides Management LAN access according to 802.1Q bridge mode (VLAN aware) - accessible via COLAN (MGMT) for untagged management traffic.

L3 (IP) Connectivity

ML systems are assigned the default IP address and Gateway of 0.0.0.0 (unusable) and a Subnet Mask of 255.255.0.0 (Class IP Addresses).

➢ **To set IP connectivity parameters on monitored units**

1. In the **Network Element** tree, open **Management Interfaces**. The **Configure Management IP Interfaces** pane opens.
2. In the **IP Interface** area, click the **Configure** button. The **Configure Management IP Interface** dialog appears.



3. Enter the IP management interface parameters as provided by your network administrator.
4. To block remote IP configuration on monitored NE via a linked NE (not relevant to ML530) - set **Access From Linked NE** to Disabled. By Factory Setup this option is enabled on any ML system.
5. COS (Class of Service) of Management VLAN flow is configurable (set to 7) by default. All Management frames created by CPU will be originated with COS bits as configured.
6. To reset all parameters to factory setup values, click **Reset**.
7. Click **OK**.

SNMP Agent and Trap Parameters

Each ML device can be configured to send traps up to four defined trap destinations. The SNMP agent parameters and trap destinations can be defined on an individual element level or for a Group of elements.

By default all traps are enabled for every system. However, irrelevant traps may be filtered out on an ML system levels and configuring destinations to which traps will be sent.

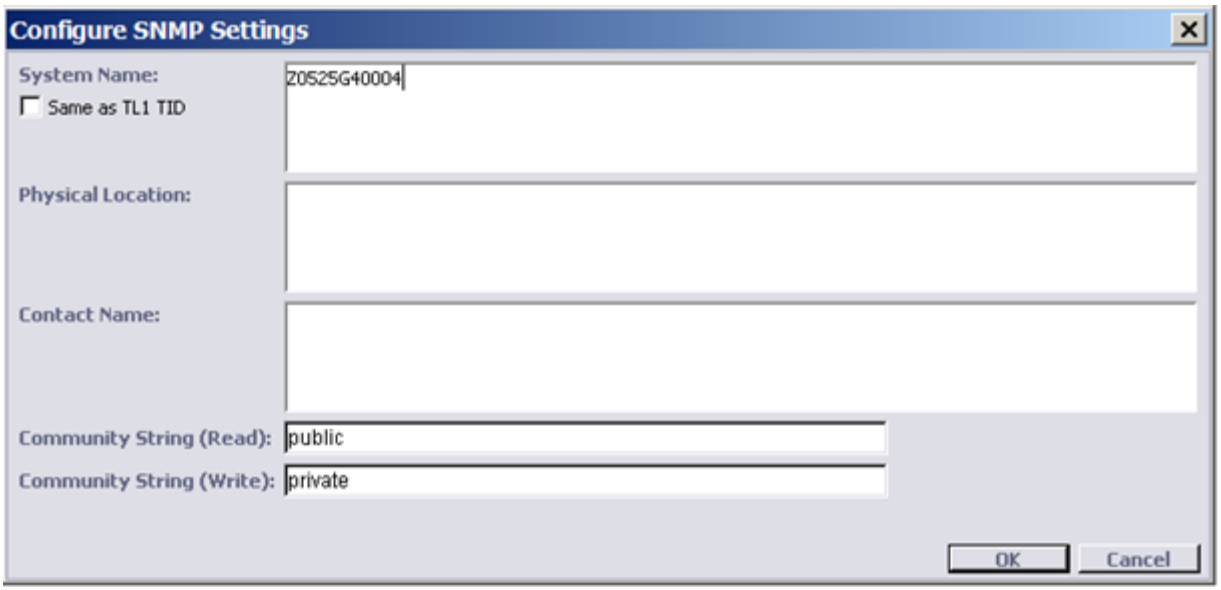
SNMP Agent Configuration

NOTE: SNMP settings can be configured for a single selected element, or simultaneously for a group of selected network elements.

➢ **To define identification parameters and disable irrelevant traps**

1. To invoke the SNMP pane:
   - In the **Network Element** tree, expand the **Management Access** item and select **SNMP.**
   - In the invoked pane, Configuration area, click **Configure**. The **SNMP Settings** pane opens.

NOTE: To invoke the dialog for a selected Group: in the **Network Topology** tree select the Group item, in the Menu bar, select **Group Operations**, **SNMP Configure**. The **SNMP Settings** pane opens.



2. Set the system identification parameters (recommended):
   - **System Name** - The system name is set by default as the unit ID. A recognizable name may be assigned to the system. Range = up to 255 alphanumeric characters.

NOTE: If a name is assigned via TL1 and want the same name to be assigned via SNMP, enable **Same as TL1 TID**.

   - **Physical Location** - Optional - Enter information on the physical location (i.e. address). Range = up to 255 alphanumeric characters.
   - **Contact Name** - Optional - Enter information of the contact person such as name, phone number, etc. Range = up to 255 alphanumeric characters.
3. It is recommended to configure security by changing the default community names. All SNMP implementations universally accept the default name "public." To limit access to the ML unit:
   - Change the Read community name - to limit Get or Read access to the ML unit. Range = up to 32 characters.
   - Change the Write community name - to limit Set or Write access to the ML unit. Range = up to 32 characters.
4. Click **OK**.

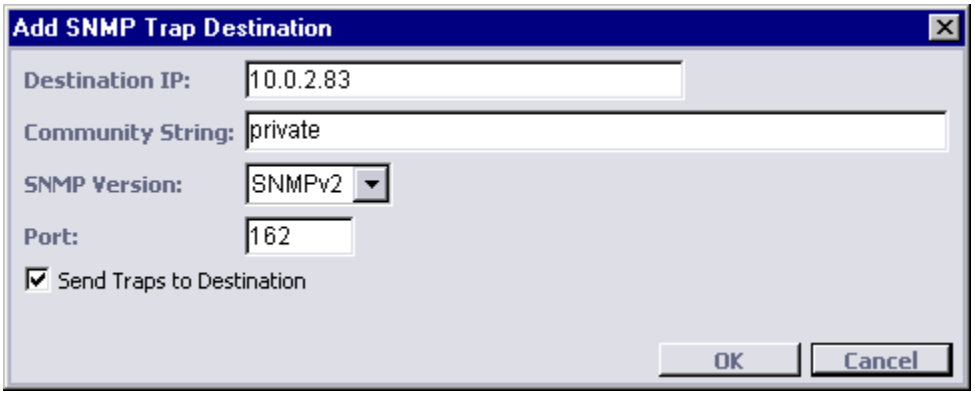
SNMP Trap Destinations

SNMP traps are autonomous SNMP messages sent by the ML device to pre-defined SNMP management system destinations devices upon the occurrence of specific events. Up to four trap destinations can be defined.

NOTE: The destination details must be coordinated with the SNMP management system.

➢ **To configure SNMP Trap Destination:**

1. On the Navigation tree in the Network Element tree, open **Management Access**.
2. Open **SNMP**. The **SNMP Settings** pane opens.
3. Click the **Add** button. The **Add SNMP Trap Destination** dialog appears.



NOTE: For group operations, open the **Add SNMP Trap Destination** dialog box via the menu bar: **Group Operations, SNMP, Add**.

4. In the **Destination IP Address** box, type the IP address of the SNMP management system.
5. In the **Community String** box, type the community string of the SNMP management system. If an incorrect string is typed, the SNMP management system may not receive the SNMP traps.
6. In the **SNMP version** box, select the version of the SNMP used by the management system. The SNMP version defines the structure of the traps that will be sent to the SNMP management system.
7. In the **Port** box, type the SNMP/UDP trap notification port of OSS/NMS host where the ML device traps are to be received. Click **OK**.

SNMP Trap Filtering

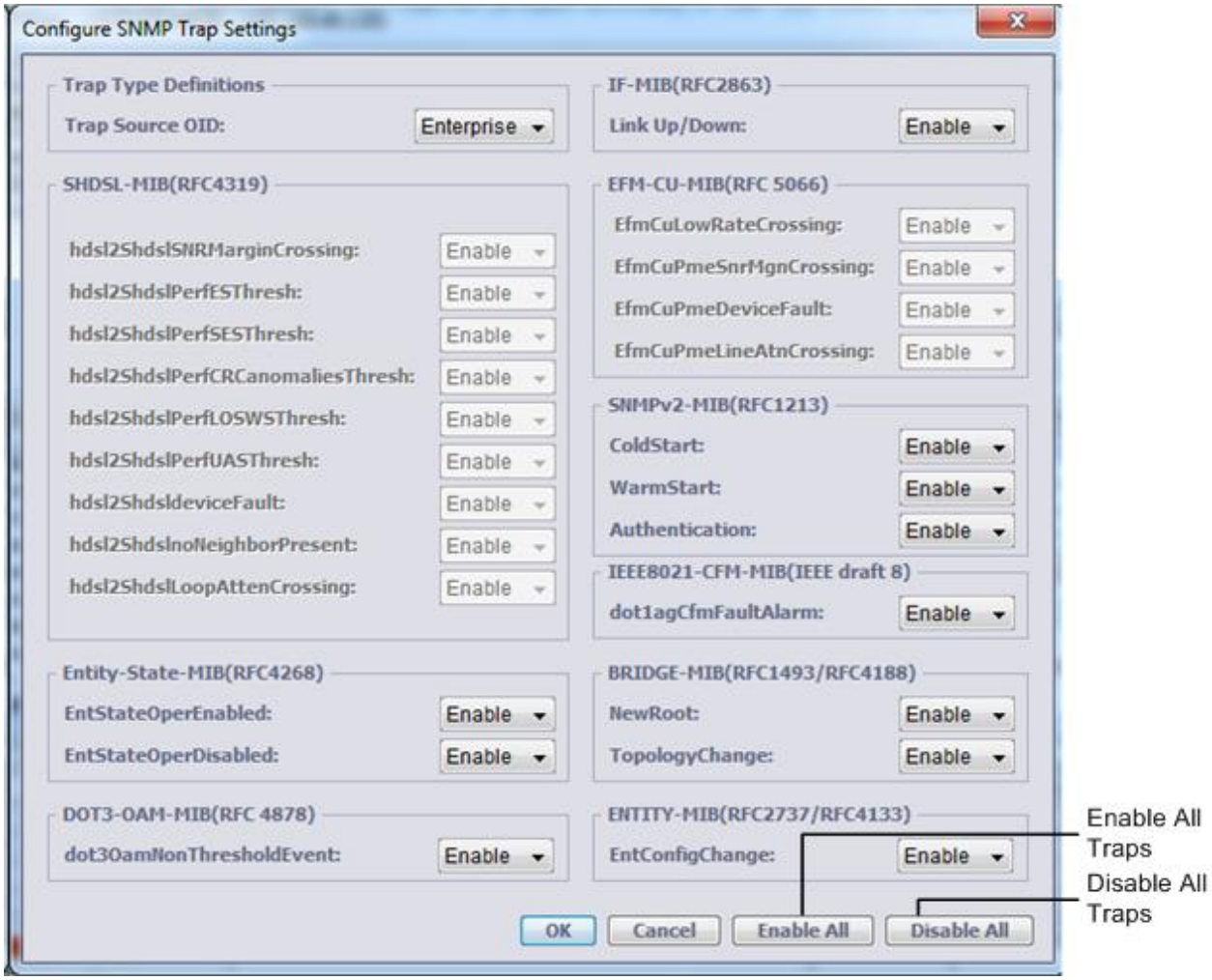
Use this dialog to filter out irrelevant traps. Note that all traps can be simultaneously disabled or enabled (according to your needs) and only allow relevant traps.

Trap Source OID parameter is applicable for Standard MIBs, allowing to mark Traps/Notifications either by ACTELIS ENTERPRISE OID or by OID of the STANDARD MIB where these Traps/Notifications are defined.

NOTE: Irrelevant for ML700 DMT model traps (from SHDSL-MIB and EFM-CU-MIB) are grayed-out as unsupported.

➢ **To filter out SNMP traps for a selected ML system**

1. In the Network Element tree, under Management Access choose SNMP and in the displayed pane, Trap Configuration area, click Configure. The Trap filter dialog appears. The traps are grouped within MIBs where are defined.



2. Under **Trap Type Definitions**, select the **Trap Source OID** as one of the following:
   - MIB - traps displayed according to their MIB source
   - Enterprise - traps displayed according to the ML source
3. To allow Traps/Notifications from Standard MIBs only:
   - Press **Enable All** button
   - Disable **Actelis Alarm MIB** notifications and click **OK**.
4. To allow Traps/Notifications from Actelis proprietary MIB:
   - Press **Disable All** button
   - Enable **Actelis Alarm MIB** notifications and click **OK**.
   - Optionally, enable **Bridge MIBs** and click **OK**.

SNMP Traps from Non-IP CPEs

ML700 CPE that is not assigned an IP (hosted by an IP-based CO NE) sends SNMP notifications using the IP address of the host CO NE.

All configurations of SNMP Agent/Trap Destination provided on non-IP NE are used by the ML to originate the trap, although CO NE IP address is attached when trap frame is sent to the Management plane thought CO NE.

- **To identify original source of a non-IP CPE in SNMP v1 trap, the following fields can be used**

  Agent Address: <CO IP address>, < "don't care" value of UDP SA auto-set by CO> , <CPE SMNP Version>
  Community: <COMSTR configured on CPE>@<CPE-TID%CO-HSL-AID>
  SNMPv1 agent address: 0.0.0.0

- **To identify original source of a non-IP CPE in SNMP v2c trap, the following fields can be used**

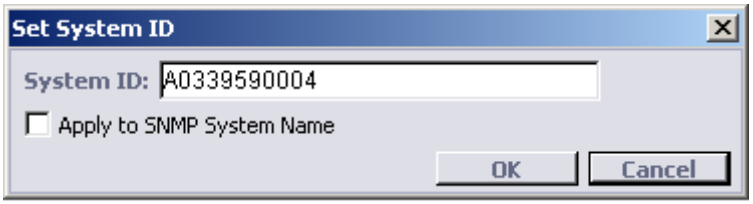
  Agent Address: <CO IP address>, <"don't care" value of UDP SA auto-set by CO> , <CPE SNMP Version>
  Community: <COMSTR configured on CPE>@<CPE-TID%CO-HSL-AID>

System Name Configuration

Each ML system is assigned the Serial Number identification supplied on a sticker on the device. This number is also reported, by factory default, as the System ID (TL1 TID) and System Name (SNMP) (**SNMP Agent Configuration** (on page 3-15)). This serial numerical value can be changed to a logical system name.

➢ To assign a logical system name

1. In the Network Element tree, select **System**. The **System** pane opens in the work area.
2. In the **Configuration** area, click **Set System ID**. The **Set System ID** dialog appears.



3. In the **System ID** field, type the new system name. This will be the TL1 TID. Range: up to 20 alphanumeric characters.
4. To assign the logical name to the system in SNMP, enable **Apply to SNMP System Name**. Unless this box is enabled, the SNMP System Name will be displayed as the serial number.
5. Click **OK**.

Date and Time Setting

ML systems support manual and automatic date and time assignment. Automatic assignment uses Simple Network Time Protocol (SNTP) and requires connectivity to NTP/SNTP server. (Automatic Time of Day (TOD) adjustments according to Daylight Savings Time (DST) rules is also supported.)

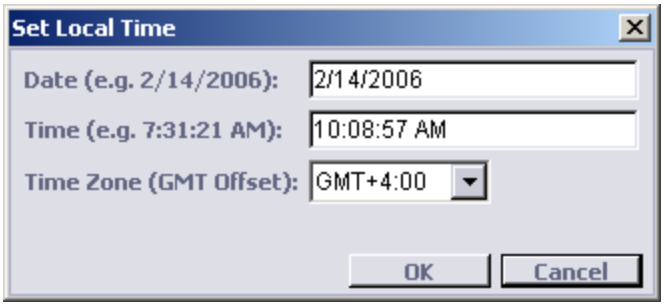
It is recommended to configure Date and Time of the system manually, even when planning to use automatic Date and Time synchronization. *Correct date and time allows reliable system monitoring and is helpful in troubleshooting.*

Configuring Date and Time Manually

This section describes how to configure the ML clock manually. Manual clock configuration is recommended even when planning to use automatic Date and Time synchronization.

➢ To set Date and Time

1. On the Navigation tree in the Network Element tree, expand **System Administration**.
2. Open **Date and Time.** The **Date and Time** pane opens in the work area.
3. In the **SNTP** area, verify **Auto-sync** is Disabled (go to step 7 to configures only the Time Zone).
4. In the **Local Time** area, click **Configure**. The **Set Local Time** dialog appears.



NOTE: For group operations, open the **Set Local Time** dialog box via the menu bar: **Group Operations, Date and Time, Configure**.

5. To set the date: in the **Date** box type the date in accordance to the computer format (for example, 2/14/2006).
6. To set the time: in the **Time** box type the time in accordance to the computer format (for example, 10:08:57 AM).

NOTE: Refer to **Daylight Saving Time (DST) Configuration** (on page 3-23).

7. To set the time zone from the **Time Zone** list box, select the time zone in accordance to the local time zone (for example, GMT +4:00).

NOTE: Time Zone is effective in Auto Sync mode only.

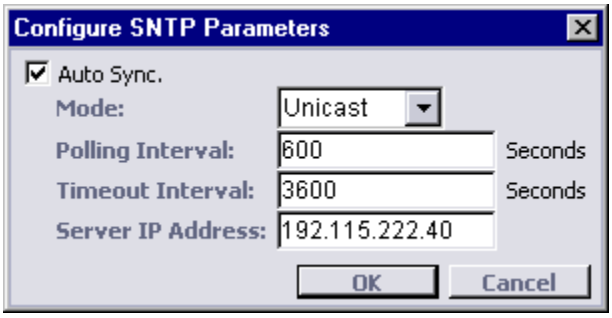
8. Click **OK**.

Automatic Date and Time Adjustment

The ML device supports automatic date and time adjustment using SNTP.

➢ **To configure SNTP parameters:**

1. In the Network Element tree, expand **System Administration**.
2. Open **Date and Time.** The **Date and Time** pane opens in the work area.
3. In the **SNTP** area, click **Configure**. The **Configure SNTP Parameters** dialog appears.



4. To enable automatic synchronization, select the **Auto Sync** check box.
5. From the **Mode** box, select Unicast or Broadcast (determines whether SNTP client listens to broadcasts or queries the server (polling)).

NOTE: Broadcast mode is unsupported in the current SW release although it appears as a selectable option.

6. In Unicast mode only, in the **Polling Interval** box, type in the polling interval in seconds. This is an interval between SNTP client attempts initiated by the ML device. Default interval provided by the ML device is 600 seconds. Value is configurable in range from 60 to 10,800 seconds.
7. In Unicast mode only, in the **Timeout Interval** box, type in the timeout interval in seconds (the interval of time allowed without synchronization). When this interval is expired without successful connection to the server, an alert is sent to the user. Default interval is 3,600 seconds. Value is configurable in range from 60 to 86,400 seconds.

NOTE: Timeout Interval must be greater than the Polling Interval.

8. In Unicast mode only, in the **Server IP Address** box, type in the server IP address (default value on factory setup is 0.0.0.0).
9. Click **OK**.
10. To verify setting the Time Zone, see **Configuring Date and Time Manually** (on page 3-21).

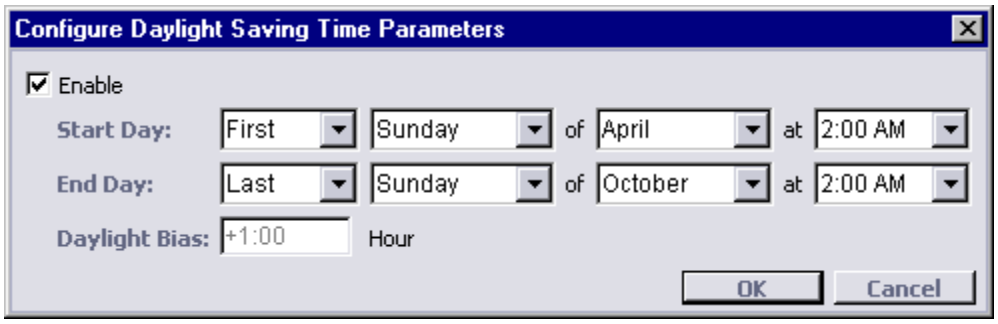
Daylight Saving Time (DST) Configuration

The ML device supports DST correction. This feature is disabled by default. When enabled, the DST correction feature is applied yearly regardless of manual and automatic (via SNTP) TOD adjustment.

NOTE: When DST starts, TOD skips one hour. When setting the TOD within that "missing" hour, the TOD is automatically adjusted forward by the DST bias, e.g. if DST starts at 2:00, then setting the TOD to 2:30 will result in TOD being set to 3:30.
When DST ends, the last hour is repeated twice. When setting the TOD within that "duplicated" hour, the TOD is set to the first instance of that hour, i.e. the hour within the DST.

➢ **To set DST:**

1. On the Navigation tree in the Network Element tree, expand **System Administration**.
2. Open **Date and Time.** The **Date and Time** pane opens in the work area.
3. In the **Daylight Saving Time** area, click **Configure**. The **Configure Daylight Saving Time Parameters** dialog appears.



4. To enable DST, select the **Enable** check box.
5. From the **Start Day** list boxes select the Start Day parameters.
6. From the **End Day** list boxes select the End Day parameters.

NOTE: Start Day month and End Day month must be different.

7. Click **OK**.

NOTE: Daylight Bias of 1 hour is not configurable.

4 Equipment and Port Configuration

This chapter describes how to configure ports, pluggable equipment and alarms.

In This Chapter

System-wide Settings

System level attributes such as alarm behavior, etc. that apply to the ML as a unit, are configured via the System pane.

System Pane

The **System** pane displays the current system level settings and provides access to the configuration, control and resource monitoring options.

NOTE: In models with SFP pluggable module, Auto-configuration feature is available and appears on the **System** pane.

➢ **To access the System pane**

- In the Network Element tree, click **System**. The **System** pane opens in the work area.
- The pane is divided into three areas: Configuration, Alarms and Conditions and Details.

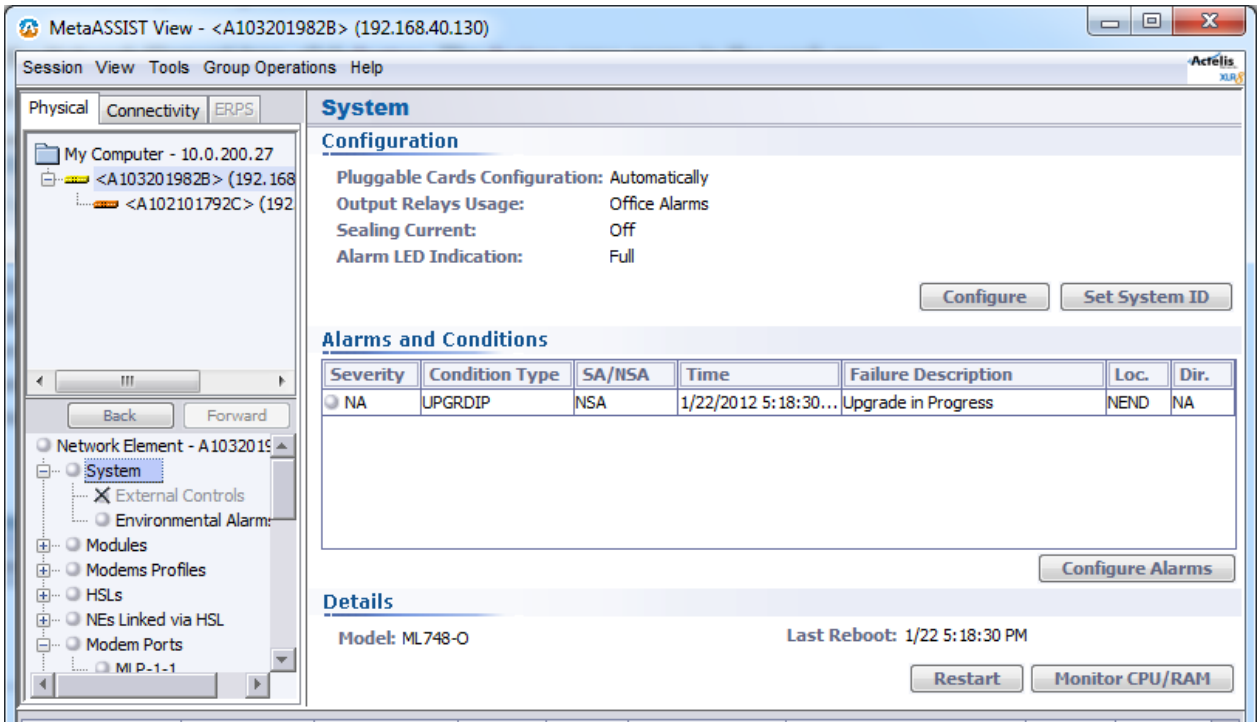


Table 10: System Pane

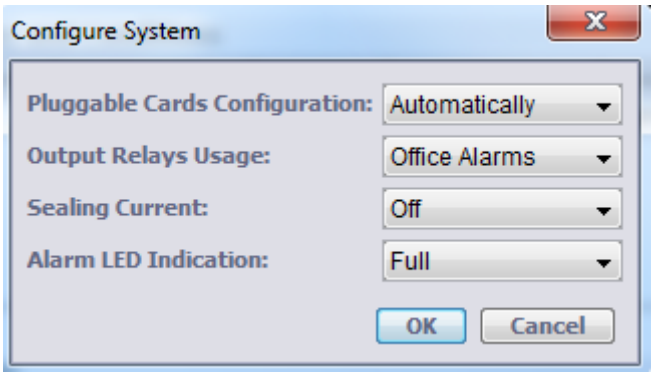
Pane Area	Description
Configuration	Displays and provides access to configurable system attributes. The following buttons are available: • Configure - accesses the System Configurable Attributes. • **Set system ID** (on page 3-20) - used to assign the system a recognizable name.
Alarms and conditions	Used to monitor and set system level alarms (Configure Alarms button)
Details	Used to control unit and monitor resources. The following buttons are available: • Restart - restarts the unit • Monitor CPU/RAM - shows percentage of CPU and RAM usage.

System Configurable Attributes

The **Configure System** dialog provides options for setting general parameters that affect the operation of the modems, output relays, cards, module configuration and other system level operations.

➢ **To configure the System equipment resource parameters**

1. In the Network Element tree, select **System.** The System pane opens in the work area.
2. In the **Configuration** section, click **Configure**. The Configure System dialog appears.



3. Set the **Pluggable Cards Configuration** method - determines if external cards/modules (SFP) are enabled automatically (default). The external card/module is *always* identified. However, in order for it to be monitored, the appropriate option has to be *enabled* as well.
   - Automatically - enables the installed SFP for monitoring.
   - Manual - the identified external module is not enabled automatically. In order to be monitored, enable the SFP according to SFP Module Manual Control.
4. Set the **Output Relays** (on page 4-5) according to the installation: External Controls or Office Alarms.

5. Enable or disable the **Sealing Current** according to the system wide network definitions. The Sealing Current is small electric current introduced by each modem in the High Speed Link to "seal" the copper line from corrosion in humid environments. The Sealing Current setting is applied to all working modems of the enabled HSL.

   The Sealing Current default setting (ON/OFF) depend on the ML model; however, except for drop-and-continue configurations (that can only be implemented on some ML models), to enable the Sealing Current, the option should be ON *only on the ML CO (and disabled on the CPE)*. Enabling the Sealing Current on both sides may either prevent the current (same polarity) or double the current (swapped tip/ring).

6. Alarm LED Indication - defines the behavior responses of the Alarm LED on the unit's front panel.
   - **Full -** all problems invoke a LED alarm indication
   - **Partial** - only critical problems that require HW or SW replacement invoke a LED alarm indication: HWFLT alarm indicated by STATUS LED and PROGFLT alarm indicated by ALARM LED.

     All other Alarms (less critical or port alarms) are indicated by the port LED (available per ETH, HSL and MLP ports). In addition, alarms suppressed due to Partial alarm LED configuration are not reported via GPO as well.

7. Click **OK**.

Alarms and Indications Control

- ML system supports general purpose output (GPO) and general purpose input (GPI) alarms.
- The GPO can be used to provide ML alarm notification. This option is configured by default (Office Alarms option) through Output Relays.
- The GPO can also be used to provide external controls such as air-conditioner activation, via ML systems. The option is configured through Output Relays.
- ML system provides General Purpose Inputs (GPI) that can be used to report external equipment alarms such as open door or water flood in outdoor cabinet. This option is implemented through the Environmental Alarms configuration.

General Purpose Output (GPO) Configuration

The Alarm Terminal Block located on the unit rear panel (for details, see unit Rear Panel Description) supports a General Purpose Output (GPO) in addition to the two environmental alarm inputs.

The ML device allows you to configure the operational mode of the General Purpose Outputs (GPO) relay contacts as office alarms or external controls.

The GPO relay contact can be set to one of the following:

- Office alarm indications (Critical/Major)
- External control such as sprinkler, lights, air-conditioning etc.

The default setting is office alarm, which can be connected to external alarm device(s).

Office Alarm Control

A single Normally *Open* (NO) GPO relay is provided in the ML system for Office Alarm indication. A sound emitting device can be connected to the Office Alarm relay to provide audible alarm functionality.

When the unit is configured for Office Alarms and connected to an external audible device then a Major or Critical alarm raised on the ML device will also activate the Audible office alarm.

Office Alarm will *Close* due to:

- Unit initialization
- Critical or Major failure

NOTE: Alarms suppressed due to Partial alarm LED configuration are not reported via GPO.

Selecting External Controls

You can perform the following on GPO represented by CC-{1}:

- Select Operated/Release
- Select Control Type (Air conditioner, Fan, General, Sprinkler, etc.)

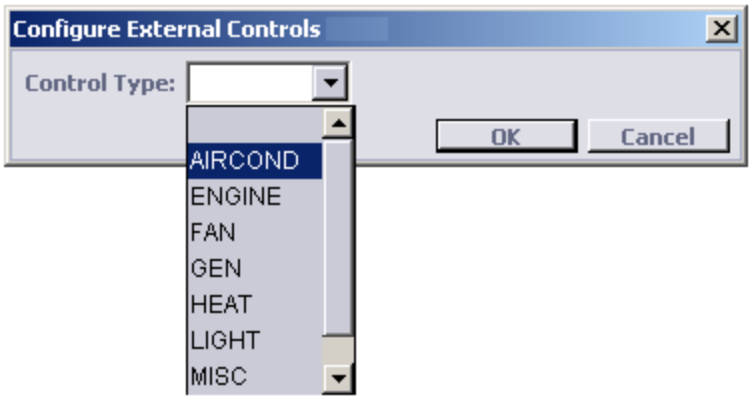
➢ **To set Output Relays to External Controls:**

1. In the Network Element tree, open **System**. The **System** pane opens in the work area.
2. In the **Configuration** section, click **Configure**. The **Configure System** (on page 4-3) dialog appears.
3. From the **Output Relays** list box, select **External Controls**.
4. Click **OK**.

Configuring External Controls

➢ **To configure external controls**

1. In the Network Element tree, open **System**.
2. Open **External Controls**. The **External Controls** pane opens in the work area.
3. Select a row in the table and click **Configure**. The **Configure External Controls** dialog appears.



4. From the **Control Type** list box, select a control type (AIRCOND, ENGINE, FAN, GEN, HEAT, LIGHT, MISC or SPKLR).
5. Click **OK**.

Operating External Controls

➢ **To operate external controls**

1. In the Network Element tree, open **System**.
2. Open **External Controls**. The **External Controls** pane opens in the work area.
3. Select a row in the table and click **Operate**. The relay contact closes and "yes" appears in the **Operated** column.
4. To release the contacts, click **Release**. The Operated column is cleared and the relay contact opens.
5. Click **OK**.

Environmental Alarm (GPI) Configuration

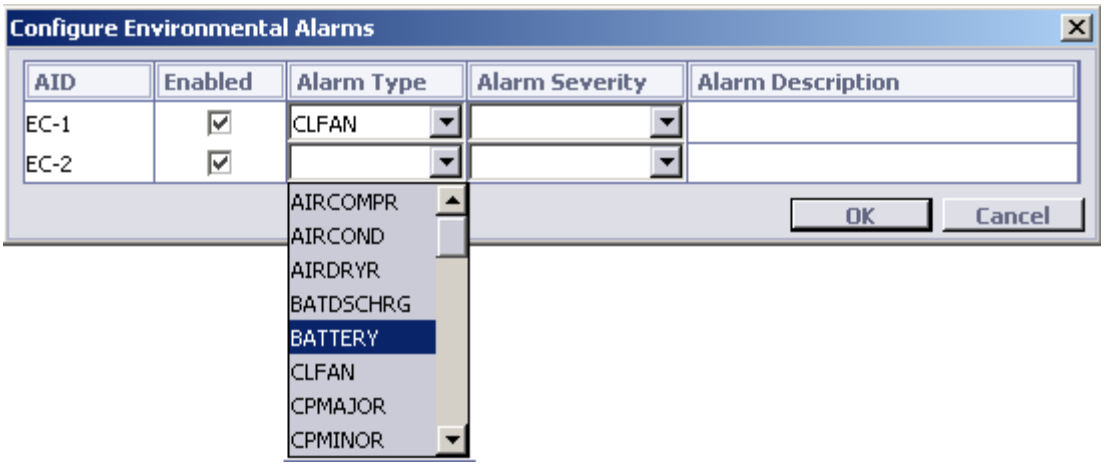
The Alarm Terminal Block located on the unit rear panel supports two environmental alarm inputs (in addition to the office alarms output). These may be connected to various detectors such as, smoke detector, door open detector, etc.

The ML device allows you to configure two environmental alarms via General Purpose Inputs (GPI)). You can configure each GPI (Environmental Control: EC-{1-2}) by associating Alarm Type, Alarm Severity and Alarm Description. GPI reports as follows:

- Reported by EC-{1-2} AID as environmental alarm in TL1 alarm format;
- Indicated by the Alarm LED according to the configured severity;
- Reported via GPO available on ML device (when connected and configured for External Alarm purposes).

➢ **To configure Environmental Alarms:**

1. In the Network Element tree, open **System**.
2. Open **Environmental Alarms**. The **Environmental Alarms** pane opens in the work area.
3. Click **Configure**. The **Configure Environmental Alarms** dialog appears.



4. To enable an alarm:
   - In the appropriate row, select the **Enabled** check box.
   - From the **Alarm Type** list box, select the alarm type that fits the connected detector. (See **Environmental Alarm Condition Types** (on page 1) for details).
   - From the **Alarm Severity** list box, select the required alarm severity.
   - In the **Alarm Description** box, type a short description of the alarm.
   - Click **OK**.

SFP Pluggable Modules

This section is relevant for ML units that support pluggable SFP modules (can be ordered from Actelis).

Supported SFP modules must comply with SFP MSA standard agreement and must be inter-operable with 100Full-duplex, 1000Full-duplex or 100/1000Full-duplex multi-rate SFP socket ports provided on the ML. Actelis provides support for a wide range of optical and copper SFP modules for pure Ethernet, CWDM, T3/E3 over Ethernet (PWE), MiTOP-E3/T3, Ethernet over T3/E3 (GFP or HDLC), etc. (see **SFP Modules** (on page 2).)

The ML unit is set by default to auto-provision SFP modules, allowing automatic configuration on power-up and upon card insertion. Auto-Provisioning can be disabled, enabling manual provisioning.

Note the following:

- If unknown SFP card or module is inserted, the UNKNOWN alarm is generated and auto-provisioning is not performed.
- **MiTOP-E3/T3 SFP** (on page 4-10) modules support "TDM over PSN" technology and require comprehensive configuration of PWE data path. For such modules, ML NE allows to configure management connection attributes (IP, GW, Net Mask and VLAN).

SFP View Provisioning Options

The SFP View provides access to SFP analysis and activation options. In the MetaASSIST View, the SFP card is labeled according to its location on the front panel. In the example below of the ML650S that supports two SFP port, SFP-1-1 is the right-most SFP port (Port-5), SFP-1-2 is the left SFP port (port-6 in the example).

The monitoring and configuration options for each SFP card is provided via a dedicated pane available from the Network Element tree.

➢ To display the SFP Pane

In the **Network Element** tree, select one of the following (depending on your system:

- For ML230/2300 - select **Cards and Modules, SDU-x, SFP-x**
- For all other units (ML500, ML600, ML700, etc.) - select **Modules, SFP-x**

- The relevant, dedicated SFP pane appears.

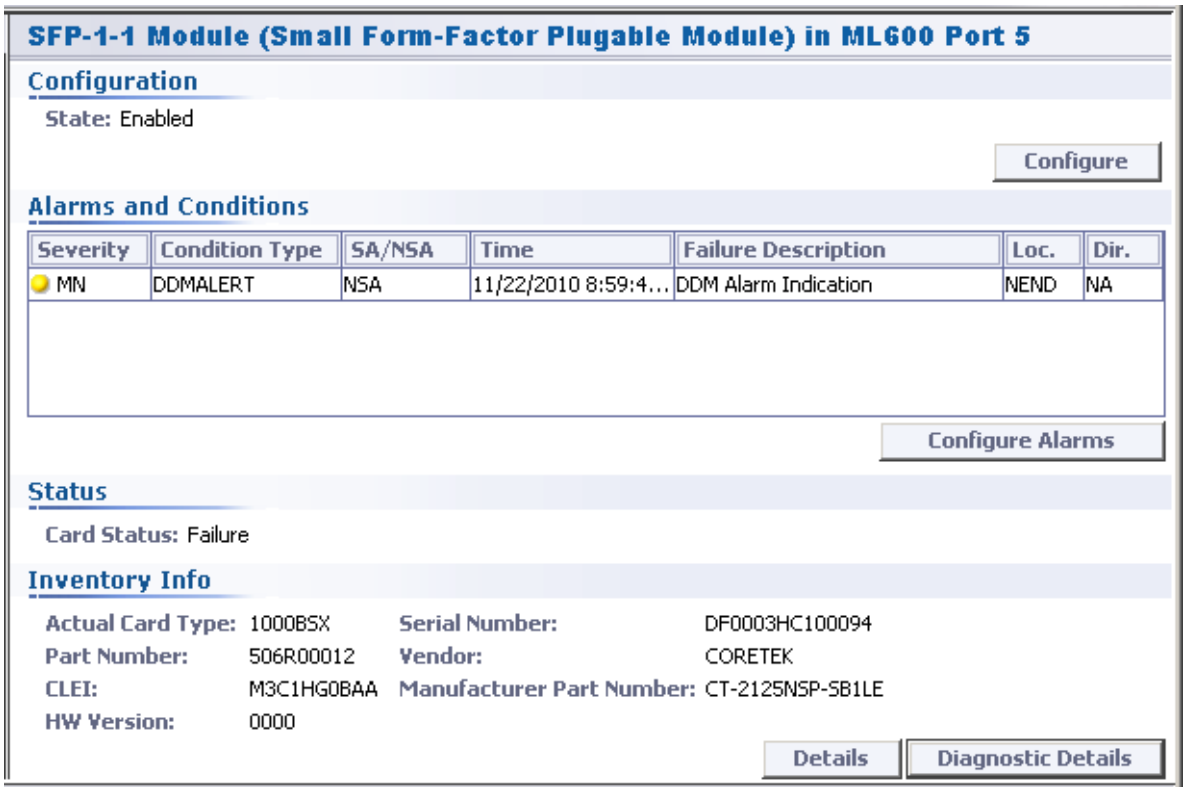


Table 11: SFP Pane Areas

Table Area	Description
Configuration	Displays status and provides access to module enable option (**Configure** button). The option is relevant only for manual provisioning. (If the **System Configurable Attributes**, **Pluggable Cards Configuration** parameter is set to Automatic, the SFP module is auto-provisioned; if the parameter is set to Manual, provision the SFP module by clicking the **Configure** button and check-marking the **Enable** option).
Alarms and Conditions	Shows any SFP alarms with the relevant information. The **Configure Alarms** button provides access to the SFP alarm management pane - used to disable alarms and modify their severity.
Status	Operation status
Inventory Info	Shows hardware and software information on the SFP module, in addition to two buttons that access more detailed information: • **Details** button - displays the SFP manufacturer details such as rate, wave length, reach, etc. • **Diagnostic Details** - This button provides access to the DDM (digital diagnostic memory) data of SFPs supporting DDM with Alarm report option. The invoked pane shows the current values, thresholds of alarms values and alarms (in raised).ML integrates a single DDMALERT alarm raised over all possible (10) threshold cross events which may be reported by SFP. *Note that SFP alarm thresholds are provided by the manufacturer and cannot be modified via the ML.*

MiTOP, MiRIC and MiRICi SFP Management Access

ML supports RAD's MiTOP-E3/T3, MiRIC and MiRIC SFP modules. MiTOP-E3/T3 is a finger-sized, small form pluggable module that enables transport of "TDM over PSN" technology and requires comprehensive configuration of PWE data path. The MiTOP device can be configured in one of two ways:

1. Full configuration using a **Dongle SFP Configuration Adaptor** (**DSFP-CA**) unit
2. Inserting MiTOP SFP to ML unit SFP socket and setting the *IP address* and *VLAN* parameters via a local MetaASSIST View connection followed by a full attribute configuration via Web access session (can be opened via the MetaASSIST View) (see **MiTOP Configuration via MetaASSIST View** (on page 4-11)).

This section describes the IP Address configuration (without a Dongle) via MetaASSIST View and provides a summary of the recommended MiTOP SFP and ML configuration parameters for Actelis applications, along with a detailed example.

Note the following:

- Remote management connection attributes can only be configured on MiTOP-E3/T3 SFP module(s) for units *plugged into the appropriate ML SFP socket* (port should support 1000Full-duplex mode). These attributes cannot be configured in advance and are not stored in the ML for retrieval if the module is removed.
- If a (plugged in) MiTOP-E3/T3 SFP module is not configured properly (i.e. insufficient PWE path, duplicated IP, or other incompatible setting), you can use the **RESTART** button to reset the SFP module to factory setting (then SFP must be reconfigured from the beginning) or reset the SFP module with current setting to refresh the PWE path.

MiTOP Configuration References

- For Actelis recommended MiTOP or MiRIC settings, refer to the MiTOP Configuration tables MiTOP Configuration Table or Appendix J - MiRIC Configurations Table
- For detailed explanation on how to configure MiTOP/MiRIC SFP, refer to RAD's UM (included in ML CD)
- For T3/E3 link monitoring and troubleshooting, refer to RAD's UM.

ML Service Configuration for MiTOP Support (Relevant for SDU-400 Only) - apply the following configurations to the service carrying the E3/T3 traffic:

- Set the service Shaper to **Enabled**
- Set service rules attributes as follows:
  - **CBS**: 60,000 kbps for T3; 45,000 kbps for E3.

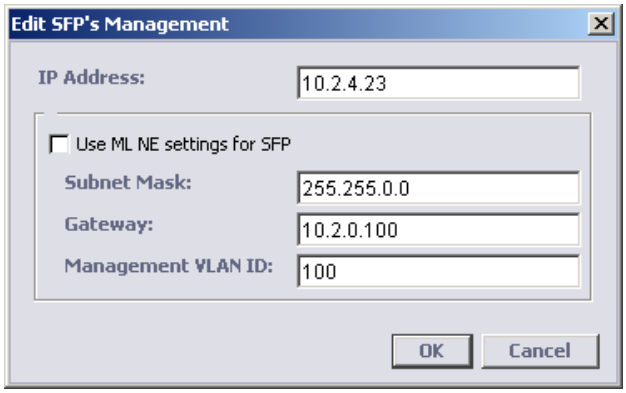
    NOTE: In case the payload size is lower than the MiTOP default value of 256 bytes (not recommended), CBS value may need to be increased.
  - **EBS**: 100,000
  - **EIR**=100
  - **EBS**=1632

MiTOP Configuration via MetaASSIST View

This section details the two-step MiTOP SFP configuration via the MetaASSIST View.

➢ Step 1: Configuring the MiTOP SFP Management Parameters

1. Access the MiTOP SFP Pane (under **Modules** in the **Network Element Tree).**
2. In the displayed pane, click the **Edit SFP's Mgmt** button.
3. SFP management can be provided in a different or in the same as ML devices Management plane. To use the same Management plane, checkmark the **Use ML NE setting to SFP** checkbox.



4. To complete setting on the ML (for in-band access to SFP) open the VLAN pane of the ML NE and specify an ETH-x port, where the SFP port is plugged in a Management VLAN ID as specified in the above SFP dialog.
5. After configuring IP/LAN management access on the SFP, and the VLAN is set accordingly on the ML NE ETH-x port, use the WEB browser to complete the rest of the configuration, as specified below.

➢ Step 2: Opening a WEB session to the MiTOP SFP module, to configure additional SFP parameters

1. On the **Network Element** tree, click **Modules**, **SFP-1-x** (where x is the relevant port to which MiTOP SFP device is connected). The MiTOP SFP screen opens.
2. Click the **Browse** button to open the default PC web-browser that is connected directly to the SFP IP (assigned in the previous step).
3. Login to the SFP system using one of the following:
   - User Name "**su"** and Password "**1234"** or,
   - User Name **admin** and Password **admin**
4. For in-band (from wire) management, configure the SFP module for TAGGED frames in the MGMT VLAN (to separate the configuration and service data on the SFP) and apply COS=7 to MGMT traffic – to prioritize management above service.

NOTE: For connection to the SFP plugged into the *CPE NE*, configure the SFP in the same Management plane as ML devices.

5. Assign the SFP the same VLAN as the MGMT VLAN on the ML NE. To continue SFP PWE Service configuration, refer to MiTOP-E3/T3 User Manual or to brief checklist table provided in MiTOP Configuration Table.

MiTOP Configuration Example

➢ MiTOP Configuration Example

1. Install a MiTOP device in ML SFP socket.
2. Configure Management access to the MiTOP device (either via MAV or via Dongle SFP Configuration Adaptor):
   - Add Tagged port of SFP to MGMT VLAN of the ML;
   - Define IP address, IP mask and default gateway IP address of the MiTOP (via MAV it is on SFP module pane). For example:
     - MiTOP-1: 10.1.50.1, 255.255.0.0, 10.1.0.100
     - MiTOP-2: 10.1.50.2,255.255.0.0, 10.1.0.100
3. Access MiTOP-1 via Browser (10.1.50.1):
   - User: su
   - Password 1234
4. Enter MiTOP Physical Port Configuration (Configuration > Physical Ports):
   - Set E3 or T3
   - Enter E3/T3
   - Set Tx Clock Source: CO - LBT (on CPE - Adaptive)
   - Set needed Line code and Line type
   - Save parameters

Attention! **Save** must be performed after changing of each parameter, however a **Save** button is not available in each page. In such pages, click the **Previous Menu** and save your changes.

5. In Configuration (Applications/Multiservice over PSN) of MiTOP-1, access PW and General Parameters, define the following and then **Save**:
   - Set Source IP (for MiTOP-1 - 10.1.50.1)
   - PSN Type UDP/IP or MEF
6. In Configuration (Applications/Multiservice over PSN) of MiTOP-1, access Peer, define the following, **Save** and then *check that a Peer MAC address appeared:*
   - Peer Name 2 (in MiTOP-2 it will be Peer Name 1)
   - Peer IP address - 10.1.50.2 - address of MiTOP-2
   - Optionally set MAC (usually discovered automatically by ARP)

Attention! If you need to edit any parameter, you must fill *all* parameters in a table, because clicking the **Save** copies values from the table.

7. In Configuration (Applications/Multiservice over PSN) of MiTOP-1
   - PSN parameters - for work with Tagged VLANs, set VLAN tagging Enable and then VID and its priority (the same will be in ETH port of ML). Return and Save.
   - Service Parameters - set Payload size and Jitter buffer (change default value of 500uSec to 2000uSec). Return and Save
   - Set Connection Status Enable and Save
8. In Monitoring you can see: Alarms (in Status), E3/T3 and Ethernet statistics, Connection status and statistics.

Modem Line Ports (MLP)

ML systems modem line ports (MLP) provide synchronous full-duplex DSL transmission over a single twisted pair. A number of MLPs (up to 2, 4 or 8 - model dependent) are bonded together to form an HSL (High Speed Link).

The MLP definitions are usually performed during the installation procedure as part of the preliminary configuration. Additional parameters may be defined as well.

MLPs may be added to an HSL regardless of the calibration state of the HSL and it is not *required* to recalibrate the HSL each time MLPs are added or removed. However, for optimal performance, it is recommended to calibrate the HSL after changes.

MetaASSIST View provides several panes with various MLP monitoring and analysis options.

MLP Workspace

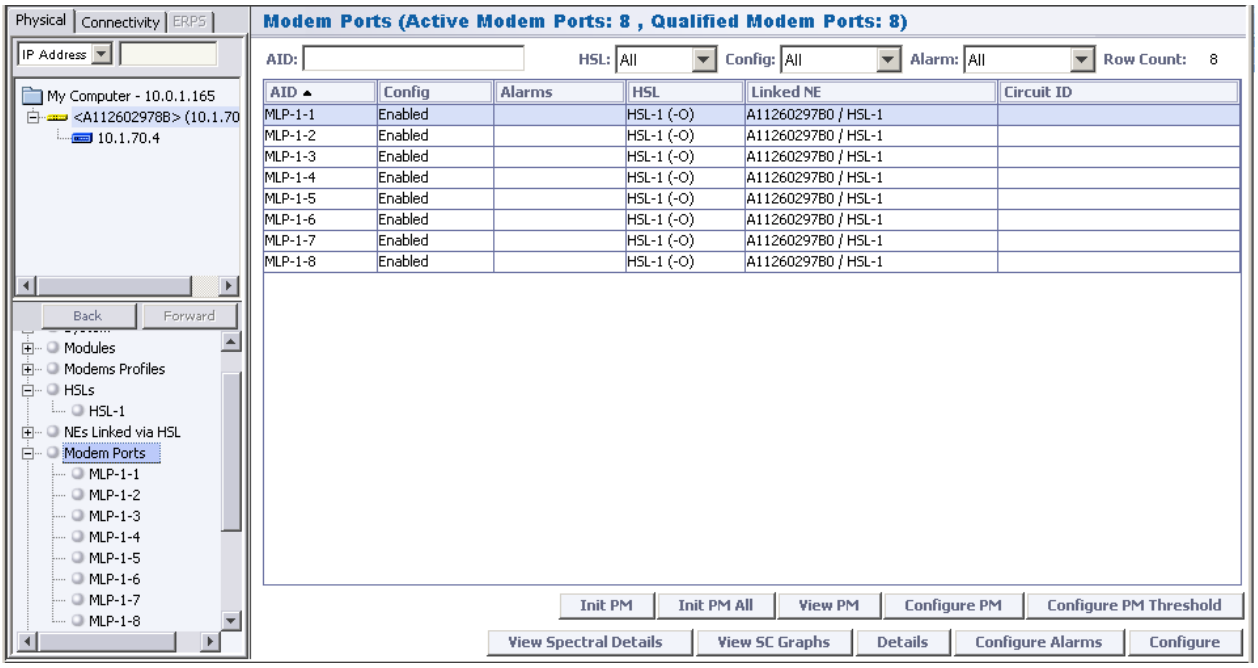
Several views are available for MLP configuration, monitoring and analysis. Each view has a dedicated set of monitoring and configuration buttons, where *some* of the options are common to the different views (the left pane in each view shows how the view is accessed):

- MLP Glance View - lists all the MLPs and their attributes in tabular format. In addition, the pane allows performing GROUP operations by selecting a number of MLPs on which the desired configuration or control operations will be performed. The column heading fields are described in **Modem Ports in HSL (MLP Details)** (on page 13-45).

  The following buttons are available:

  - Init / View / View All/ Configure / Configure Threshold **Performance Monitoring (PM)** (on page 13-12)
  - **View Spectral Details** (on page 13-51) - provides detailed spectral information.
  - **Details** (on page 13-45) - shows detailed information on the selected MLPs
  - **Configure Alarms** (on page 13-10) - alarm configuration for the selected MLPs

- Configure - displays the MLP configuration dialog.



- MLP Specific Pane- details and attributes of the individual MLP view. In addition to the Alarms display and configuration options that are standard in this type of display, the pane contains the following areas:
  - Configuration - shows the current parameter definitions and provides access to the MLP configuration (**Configure** button) and analysis options.
  - Details - provides MLP control and analysis options. The View Line Inventory button displays hardware and software versions as well as various identification information. The remaining buttons are described following the image.

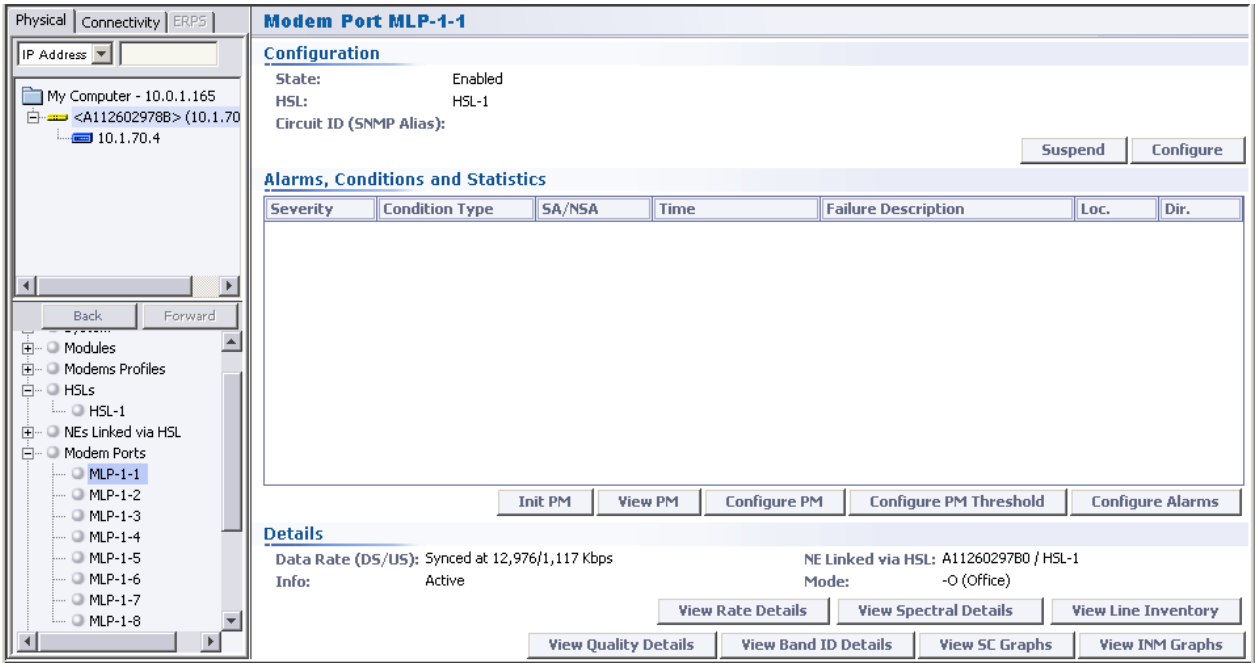


Table 12: MLP Troubleshooting and Analysis buttons

Click this View Button	To view the following information for the selected DMT pair
Rate Details (on page 13-50)	Allocated, available and attainable data rates.
Spectral Details (on page 13-51)	Status (Tx mode, EWL length, etc.), Spectral details (US0 Mask, US PSD, etc.) and US/DS signal power (dBm) measurements
Line Inventory	Available only on the ML700 CO. HW, SW, identification and status information on the CPE side of this copper pair.
Quality Details (on page 13-52)	SLA and actual measurements (noise margin, INP, interleaving, etc.)
Band ID	US and DS rates, attenuation and SNR
SC Graphs (on page 13-54)	Sub-carrier graph analysis options according various user selected parameters.
INM Graphs (on page 13-53)	Provides histograms of the Impulse Noise.

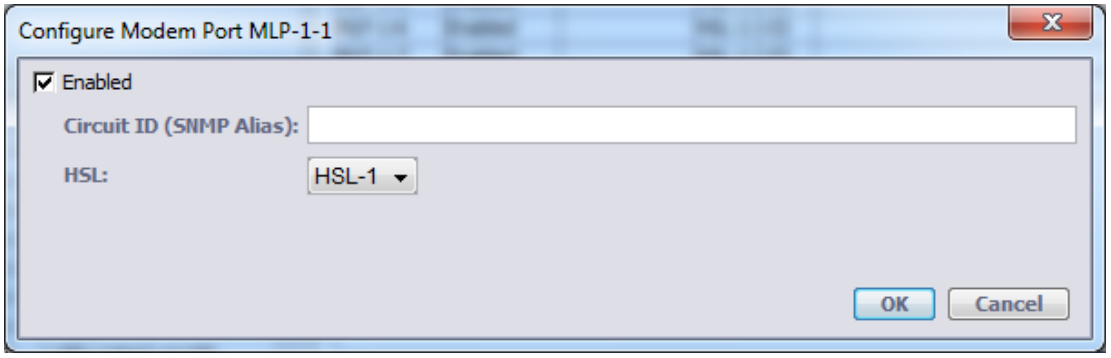
MLP Configuration

This dialog is used to enable or disable modems and to configure modem parameters.

➢ **To configure modems**

1. In the **Network Element** tree, select **Modem Ports**. The **Modem Ports** pane opens showing the list of MLPs.
2. Select the modem(s) to be enabled or configured and click the **Configure** button. The **Configure Modem Port** dialog appears.

NOTE: To select more than one MLP at a time, click on the wanted MLPs while holding the SHIFT button.



3. To disable modems not in use, clear the **Enabled** checkbox. The definitions will be retained and reapplied when the MLP is enabled. *Note that activated calibration will remain pending as long as not all enabled modems are synchronized.*
4. Click **OK**.

High Speed Link (HSL)

ML HSL is a logical port consisting of bonded, multiple MLPs that are allocated to that HSL. The HSL links an ML700 CO and an ML CPE unit. The HSL is then calibrated according to predefined **calibration profile templates** (on page 6-1).

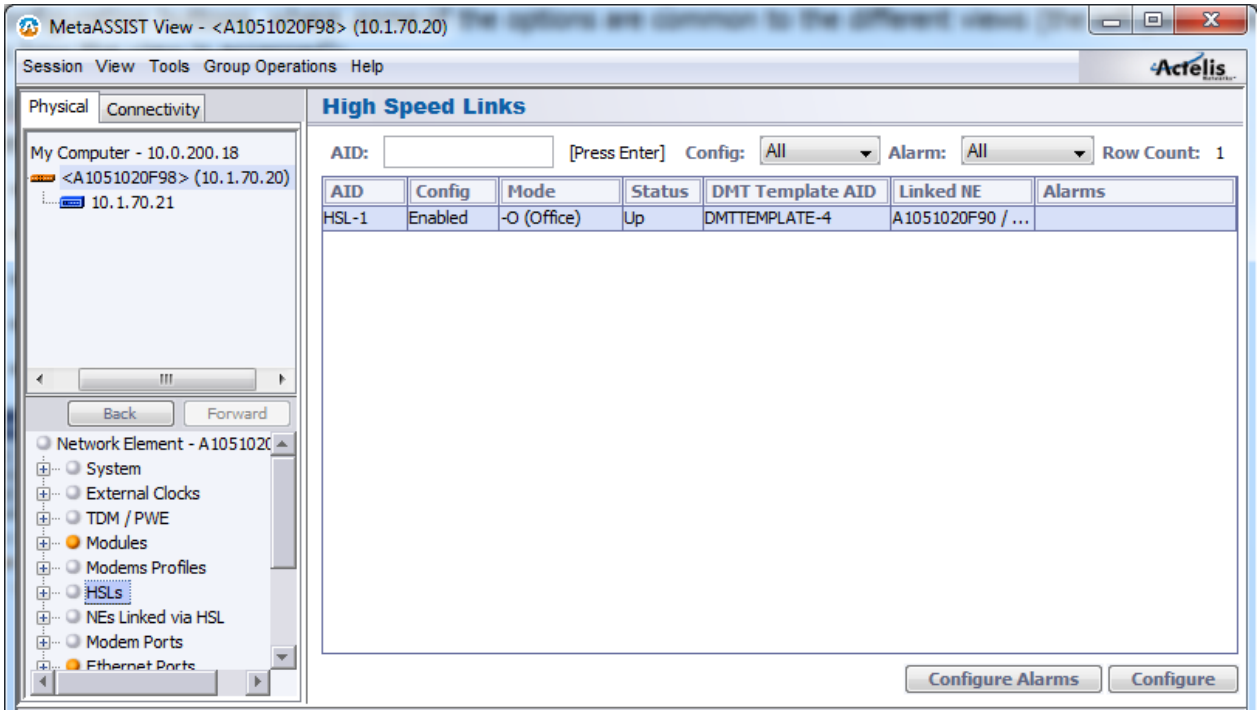
➢ **HSL activation flow is as follows:**

- Configure the HSL
- Delete unused MLPs
- Calibrate the HSL - according to predefined **profile templates** (on page 6-1) (modify the templates if required)
- Configure Ethernet attributes on the HSL

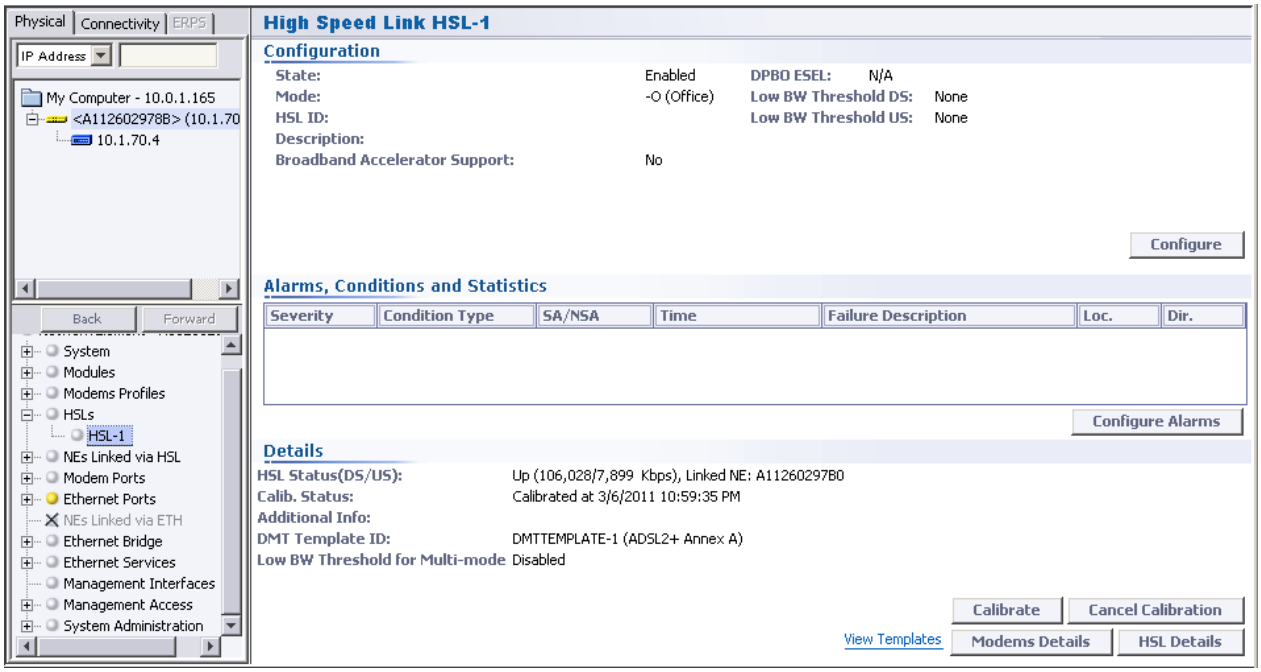
HSL Workspace

Several views are available for HSL configuration, monitoring and analysis. Each view has a dedicated set of monitoring and configuration buttons, where *some* of the options are common to the different views (the left pane in each view shows how the view is accessed):

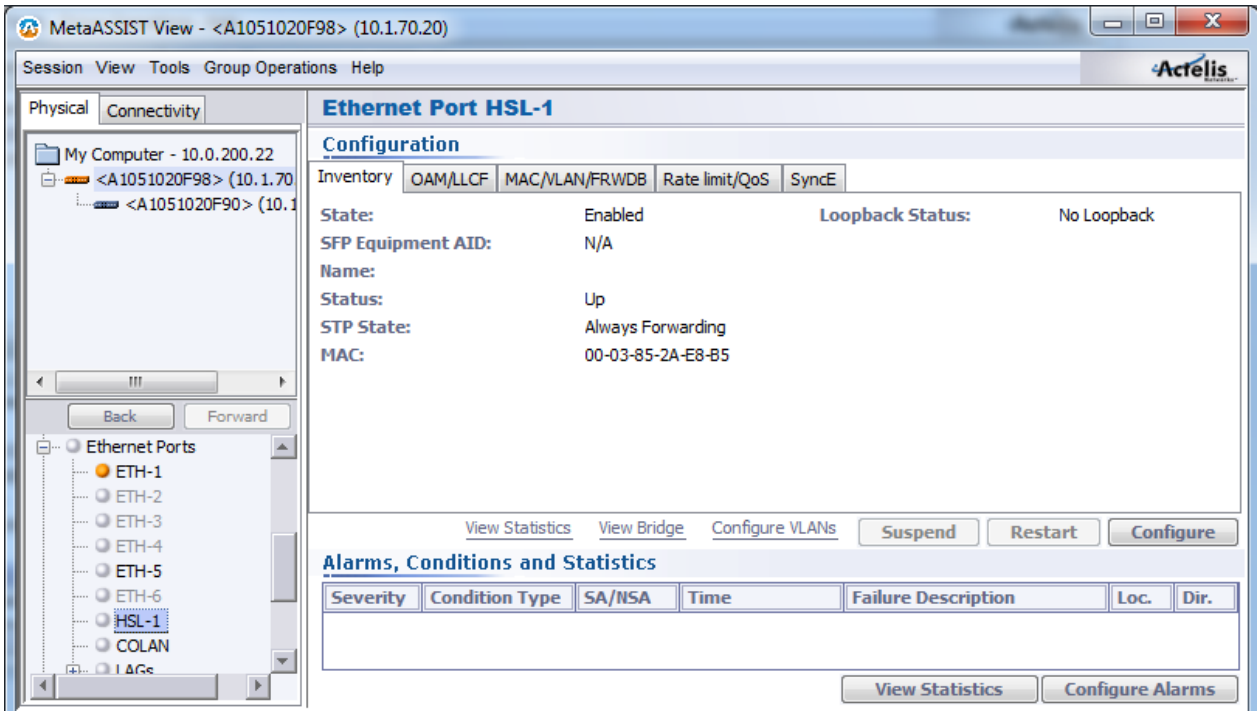
- HSL Glance View - summarizes the HSL attributes in tabular format. In addition, the following buttons are available:
  - Configure - HSL configuration dialog
  - **Configure Alarms** (on page 13-10) - alarm configuration for the selected HSL



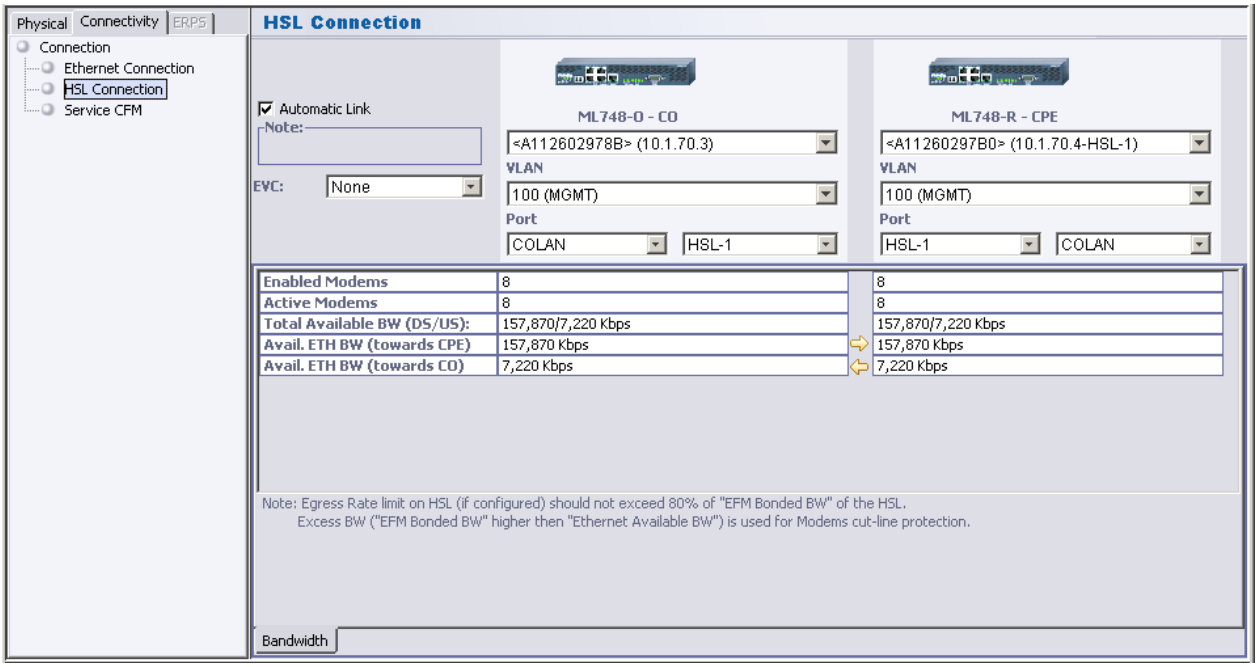
- HSL specific pane - provides additional information on HSL configuration settings and access to alarm configuration and HSL calibration options. The pane contains the following areas:
  - Configuration - shows the current configuration and provides access to the HSL configuration options (**Configure** button)
  - Alarms, Conditions and Statistics - shows any current alarms along with fault sourcing information and provides access to the alarm configuration options via the **Configure Alarms** button.
  - Details - provides HSL control and analysis options. The following buttons and links are available:
    - Calibration buttons - used to calibrate the HSL link and cancel the calibration
    - **View Templates** (on page 6-3) - link to DMT template management pane.
    - **Modem Details** (on page 13-45) - tabular list of modems allocated to HSL and their details
    - HSL Details - detailed information on specific HSL



- Ethernet Port HSL View - shows the Ethernet attributes of the HSL port and provides access to the Ethernet related configuration options. For details, see **Ethernet Port Workspace** (on page 4-26).



- **HSL Connection pane** (on page 13-46) (under **Connectivity Tab)** - shows details on both sides of the connection. It can be used to compare parameters of the CO versus the CPE HSL/MLP, debug mismatches, and more.



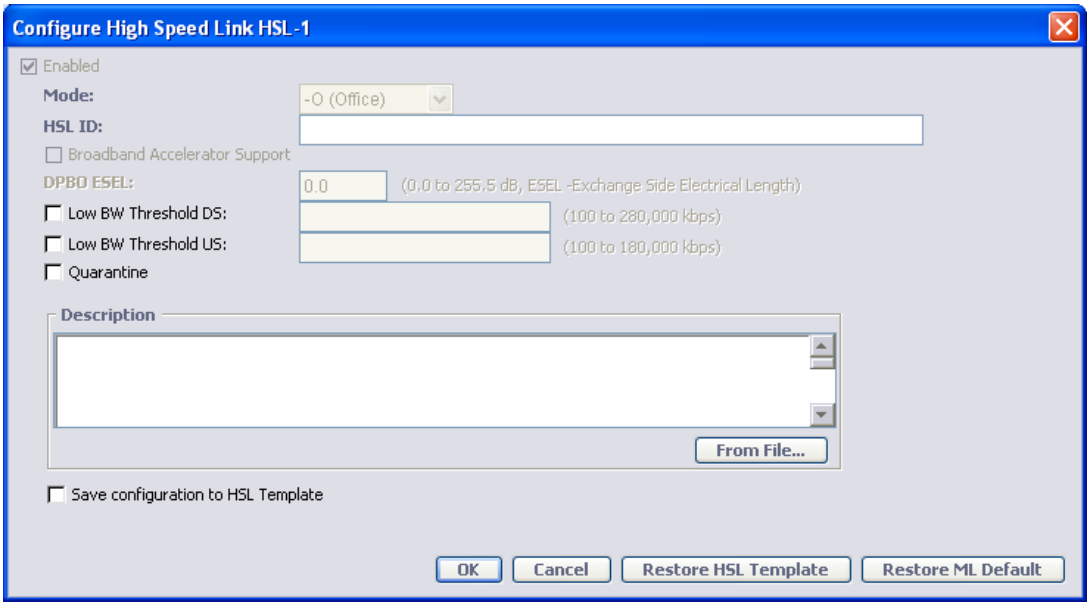
HSL Configuration

No configuration is required for the ML700 HSL operation. However, you may optionally configure the Low Bandwidth threshold (for upstream and downstream) and some identification parameters. These serve to further optimize the link operation and determine how the calibration procedure is performed.

NOTE: The HSL parameters can be saved to or retrieved from a (previously saved) configuration template file and only the relevant parameters (i.e. Mode and Topology options) can be modified.

➢ To configure the HSL

1. In the **Network Element** tree, select the **HSLs** item and at the *bottom* of the displayed pane, click the **Configure** button**.** The following pane appears



2. In the **HSL ID** field, enter an identifiable name for the HSL link (up to 64 characters. i.e. Martin Industrial Zone Building A). The ID configured here will also be used in SNMP as HSL interface alias name.
3. Check the “Broadband Accelerator support” in case of link with BBA units (BBA do not support VDSL2, in case that the BBA support is enabled the DBPO is not editable (used only for VDSL2).
4. Only for VDSL2 installed at street cabinet:
   - Set the DPBO Exchange Side Electrical Length (ESEL)

NOTE: When editing HSL, some parameters may be grayed-out because HSL operational status (In Service) does not allow changing them. To edit such parameters, cancel HSL calibration in advance.

5. To set a minimum bandwidth threshold, under which an alarm will be invoked and which may be used in case of multi-mode calibration:

   Checkmark **LOWBW Threshold DS** and **LOWBW Threshold US** and enter the low BW threshold for this link within the displayed range. *This does not initiate the BW restoration procedure, it only generates an alarm.*

6. Set Quarantine feature – when feature is enabled on HSL, its modem(s) may be automatically removed (temporarily) from HSL (they remain synchronized but are not used to send data traffic). Quarantine is applied on a modem experiencing errors for few continuous seconds. Modem is restored to normal operation automatically after one minute free of errors.
7. In the **Description** field, you may either manually enter a detailed description or information (up to 1300 characters) on the HSL, or you may import a *.txt file by clicking the **From File** button.

   NOTE: this description also appears in the HSL Topology view.

8. To Restore HSL default configuration from the Template, click the **Restore HSL Template** button. The HSL template is saved locally on the computer, and can be imported or Exported from/to Another PC.

   To enter the current configuration into the configuration template checkmark the **Save configuration to HSL template** button.

   NOTE: The HSL Configuration file also stores the HSL calibration parameters. Usage of this file is also accessed through the HSL calibration pane.

9. Click **OK**.

HSL Calibration

To achieve optimal throughput, the HSL should be calibrated, enabling the modems to operate at the optimal rate under the existing environmental conditions, system deployment technology and SLA requirements. The calibration procedure implements a predefined template comprised of allocated Modem Profiles.

Prior to HSL calibration communication between the CO and CPE units is not available (neither EOC nor Ethernet Traffic).

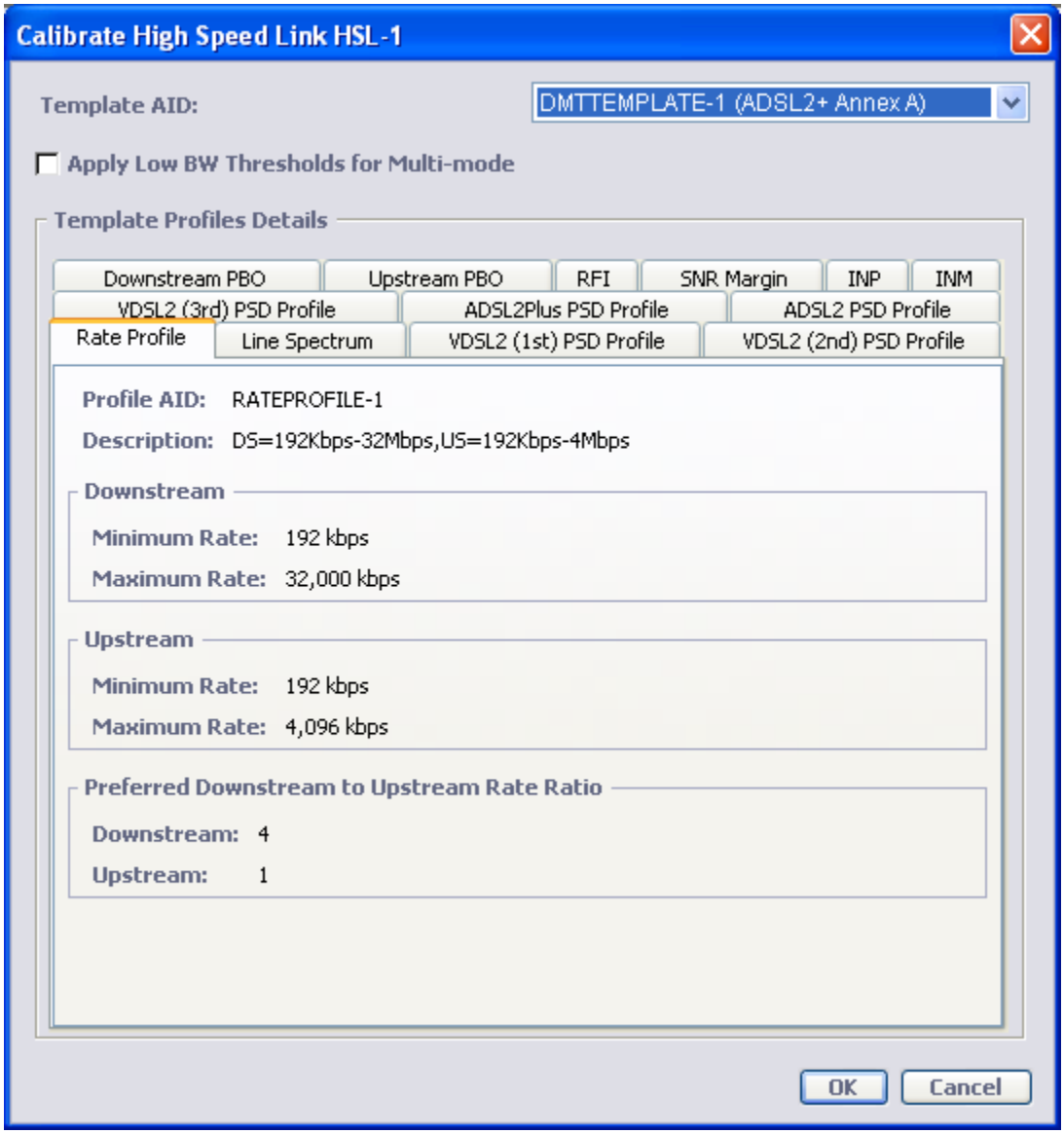
Table 13: About the Calibration

Regarding Modem Profile templates:	It is recommended to choose from the available Modem Profile templates You may customize or define your own Modem Profiles according to the instructions in the chapter '**Modem Profiles** (on page 6-1)'.
Regarding the Calibration process:	The parameters defined in the Actelis enhanced calibration process use only the modems that provide the optimal performance. *HSL calibration invoked on ML700-O will begin when any one of the assigned to the HSL modems becomes available.* Modems which are limiting the HSL performance will be automatically removed (disqualified due to Bad Ratio) from the HSL if at least one of the following conditions is true: • There must stay not less than two of modems assigned in the HSL in order to have modem redundancy and higher link resiliency (i.e. ML system will never switch to a single modem HSL even if this modem's rate is higher than a sum of rates on the rest of HSL modems). • The suspected modem limits the overall HSL bandwidth due to the EFM rate ratio of 1:4 (meaning improved HSL BW is achievable without this modem on the HSL)
	NOTE: In case of modem auto-removal during calibration, a QUALFLT alarm (with QUAL value BADRATIO) will be generated on the relevant MLP. In case of modem auto-removal during modem show-time adjustment, a BADRATIO alarm will be generated on the relevant MLP. In case of modem auto-removal due to quarantine, QUARANTINE alarm will be generated on the relevant MLP.
Prior to calibrating the system, obtain the following information:	• Modem's Minimal and Maximal Data Rate • Required Modem Quality (e.g. SNR margin) • Required transmission technology and profile (e.g. VDSL2 Profile B8-7), multiple transmission technologies may be provided. • See **Modem Profiles** (on page 6-1) section for additional information
Keep in mind the following criteria when specifying calibration parameters:	Calibration parameters should be specified in accordance with the Service Level Agreement (SLA). Required SNR margin should be in accordance with customer's DSL installation guidelines.

NOTE: The Achievable Calibration Target bandwidth depends on copper condition, topology, length, wire gauge, etc.

➢ To calibrate the HSL

1. In the **Network Element** tree, click **HSL**. The corresponding pane is invoked.
2. Before calibrating the HSL:
   - Verify that In the **HSL pane**, **Details** area, view the **Calib. Status** parameter to determine the last operation applied on the HSL.
   - Verify that the required profiles (Rate, SNR, etc.) and Template are updated.
3. In the Details area, click Calibrate. The Calibration dialog is invoked.



4. Select the **Template AID**. This is a predefined template comprising of a number of predefined profiles displayed in the corresponding tabs. The tabs are the same for all templates; however, the parameter values of each tab correspond to the template.
5. Check the "Apply Low BW Thresholds for Multi-mode calibration" in case that there are Low BW thresholds and system is set to Multi-mode (on page 6-14)
6. To review profile details, choose the *specific* profile that is required for the HSL calibration by clicking its tab: for example, a Rate Profile, Line Spectrum or VDSL2 PSD Profile (note that three profiles of this type are available).

   The tab will be highlighted and displayed (Rate Profile in the example above).

   NOTE: If any parameter requires updating, update the specific profile first (see **Modem Profiles Management Model** (on page 6-1)) and only then update the template (if required).
7. Click **OK.**

Ethernet Port

The Ethernet Ports Configuration options are used to configure the Ethernet attributes on various types of ports in the unit: Ethernet service ports, Colan port, SFP port and HSL ports.

The Ethernet configuration dialogs are invoked for each specific port and are similar in appearance. However, not all attributes are relevant for all types of ports. For example, some of the Physical Interface options which are accessible on Ethernet service ports dialogs are not relevant (and so not accessible) on the HSL Ethernet configuration dialog.

The ML allows simultaneous configuration of the same attributes to a number of ports, by selecting all requested ports through the Ethernet Ports Table pane.

Note the following:

- Some Ethernet ports correspond to installed SFP ports (where relevant) - according to their location.
- COLAN port - The COLAN (MGMT) Port by factory setup, is dedicated for out-of-band Management but can be used also as a service port. Ensure that there are no Ethernet loops between the COLAN (MGMT), ETH and HSL ports (use STP if required). To dedicate the COLAN (MGMT) Ethernet port for service purposes, see Traffic VLAN Procedure. In addition, port priority and pinout must be changed according to your setup. To dedicate the COLAN (MGMT) Ethernet port for management purposes, see **Management VLAN Procedure** (on page 8-3).

Ethernet Port Workspace

Several views are available for Ethernet ports configuration, monitoring and analysis. Each view has a dedicated set of monitoring and configuration buttons, where *some* of the options are common to the different views (the left pane in each view shows how the view is accessed).

- Ethernet Glance View - lists all the Ethernet ports and their attributes in tabular format. In addition, the pane allows performing GROUP operations by selecting a number of Ethernet ports on which the desired configuration or control operations will be performed.

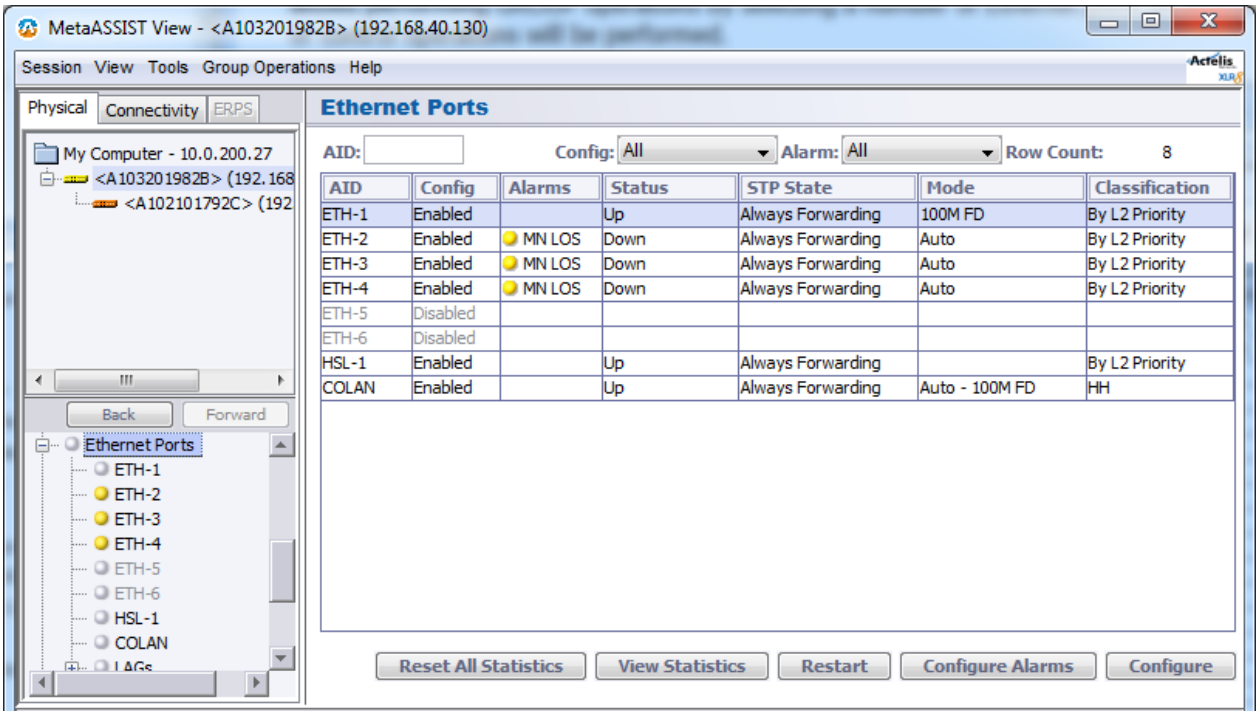


Table 14: ML700 Workspace

Button	Description
Reset all Statistics	Resets the **statics** and **trigger** values for ALL ports (individual port statistics can be reset through their dedicated View Statistics pane)
View Statistics (on page 13-26)	Displays a detailed performance monitoring pane showing statistics on traffic (Tx and Rx frames, dropped frames, etc.)
Restart	Resets the port. This may cause a momentary disruption in the service associated with that port
Configure Alarms	Alarm configuration for the selected port
Configure	Displays the Ethernet port configuration dialog

- Ethernet Specific Pane - shows details, configuration settings and status of the selected Ethernet. The items are grouped in respective tabs, where the tab parameters may vary according to the type of Ethernet port (service, HSL, etc.).

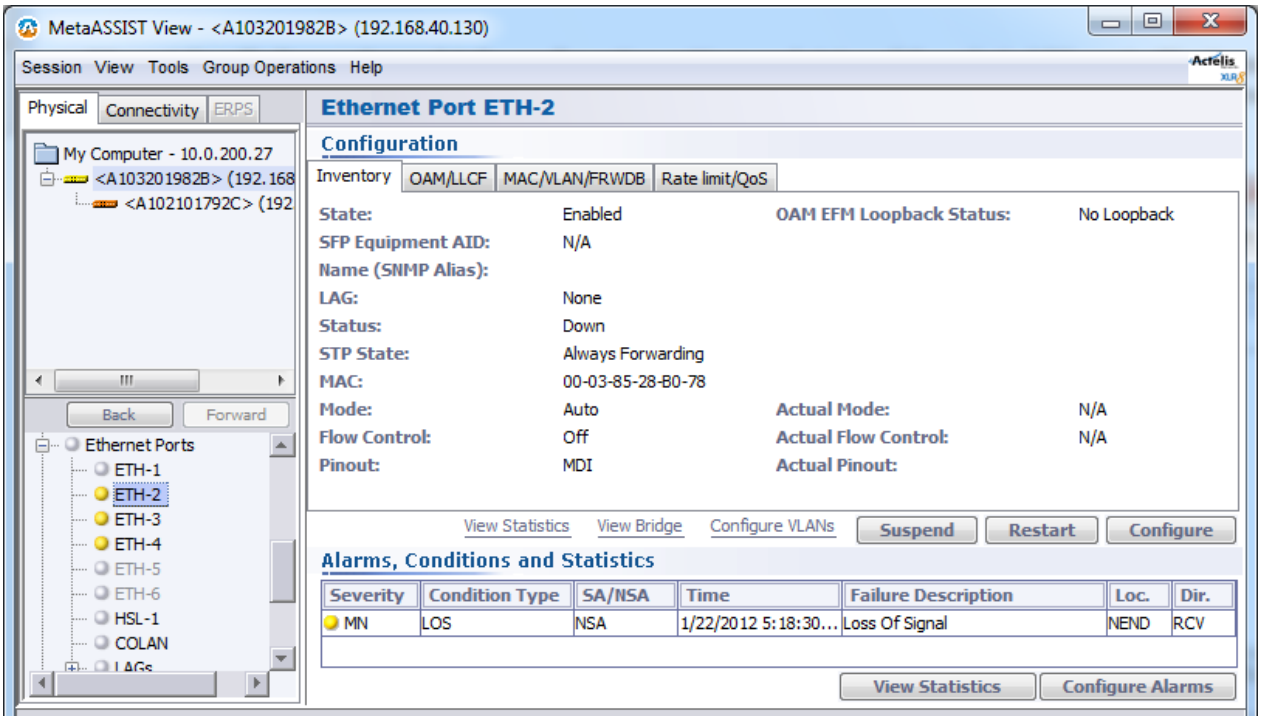


Table 15: Configuration area tabs

Tab	Description
Inventory	Summarizes the main Ethernet configuration settings and provides status information.
OAM/LLCF	Provides two types of information: EFM OAM settings and status, LLCF status and access to Operate Loopback options. EFM OAM standard allows troubleshooting of point-to-point Link Layer connectivity between two attached NEs. ML devices support EFM OAM on all Ethernet (ETH-x) and Ethernet-like ports.
MAC/VLAN/FRWDB	Shows the bridge mode (e.g. 802.1Q) and PVID if relevant.
Rate Limit / QoS	Shows the Ingress and Egress rate limits and speeds for the port, as well as other QoS parameters such as Classification, Scheduler, etc.

Table 16: Ethernet Pane links and buttons

Button/Link	Description
View Statistics	Shows connection analysis information
View Bridge	Access to Ethernet Bridge Pane
Configure LANs	Access to VLAN configuration pane
Suspend/Restart	Used to temporarily disable the port (required for various operations such as Loopback) and to Restart the port
Configure	Access to the Ethernet configuration dialog
View Statistics	Access to frame Tx, Frame Rx and Collision statistics for the port
Configure Alarms	Alarm configuration options for the port (disable irrelevant alarms or change the severity levels)

Ethernet Port Configuration

NOTE: Traffic may be briefly disrupted when Ethernet port configuration changes are applied.

On each Ethernet and Ethernet like port, you may configure various types of parameters, where not all features are supported on all port types and for all models.

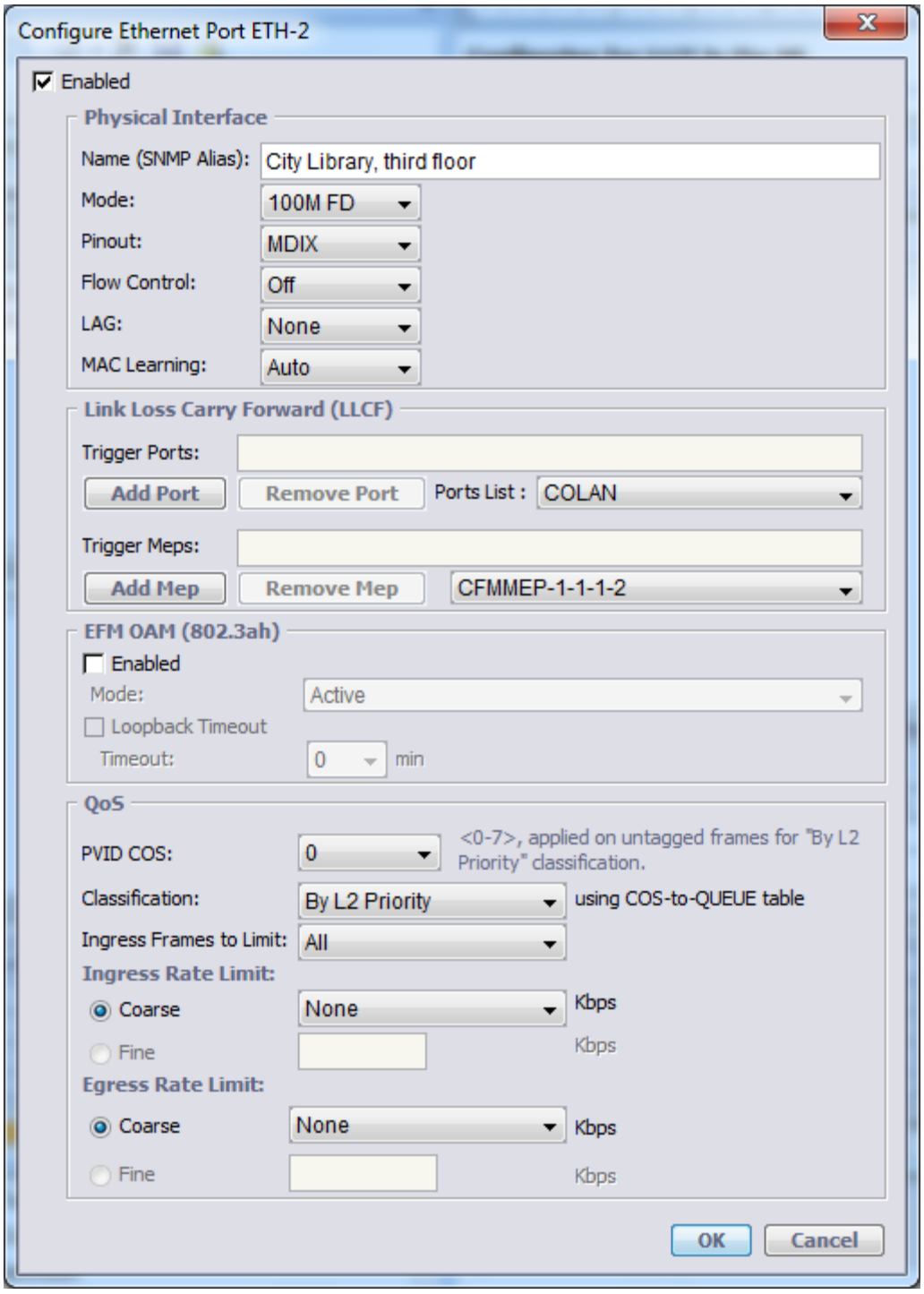
This section will provide a general description of the Ethernet configuration procedure for all ports, where the differences between port types and models will be indicated where relevant. Each group of parameters will be explained in detail in the relevant section.

➢ To access the Ethernet Port Configuration dialog

1. In the **Network Element** tree, click **Ethernet Ports** and choose the desired Ethernet port or choose the port(s) from the Glance View. The corresponding Ethernet port pane appears.

   ETH-5/6 port configuration requires SFP-1 pluggable module configuration in advance. If **Modules Configuration** is set as **Automatically**, then SFP-1 and ETH-5/6 are both auto-provisioned. If **Modules Configuration** is set as **Manually**, then ETH-5/6 should be manually configured.

2. In the **Configuration** area, click the **Configure** button. The Configure Ethernet Port dialog box appears. The example below shows the service Ethernet port dialog. However, other dialogs are similar in appearance, where irrelevant options are disabled.



3. Set the **Physical interface (IEEE 802.3 Ethernet media)** (on page 4-30) parameter group.
4. Set the **Link Loss Carrier Forward (LLCF) by Port(s) or/and MEP(s) triggers** (on page 4-35) parameter group.

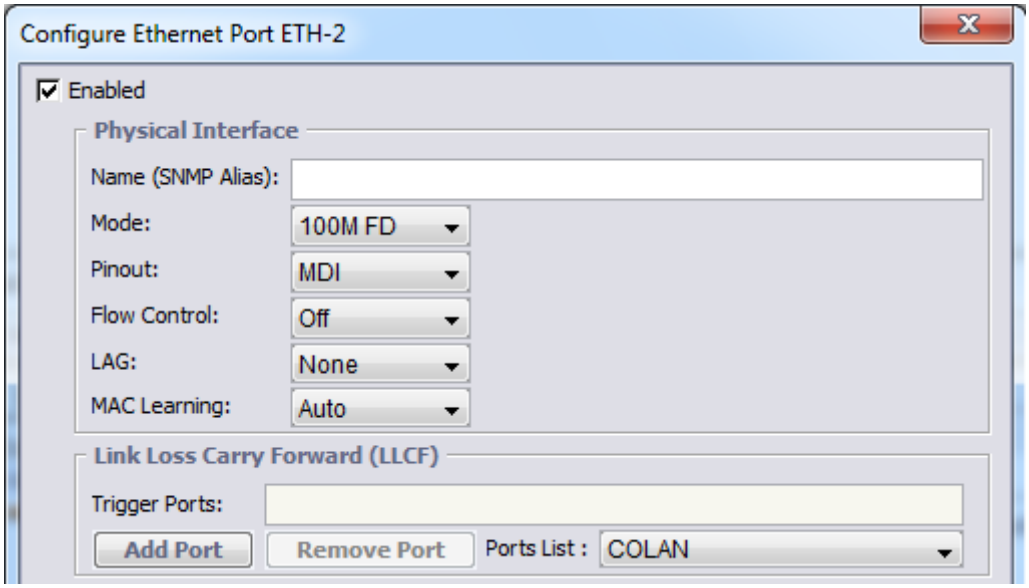
5. Set the 802.3ah EFM OAM parameters - EFM OAM standard allows troubleshooting of point-to-point Link Layer connectivity between two attached NEs. ML devices support EFM OAM on all Ethernet (ETH-x) and Ethernet-like ports. In addition to standard parameters, ML devices allow to set Loopback Timeout:
   - Enabling EFM OAM - EFM OAM is disabled by default. When **Enabled**, ML devices support only Active mode (originate discovery message toward attached device) and report status of discovered. For more information see 802.3ah Ethernet OAM.
   - **Loopback timeout** - a timer for remote EFM OAM Loopback. If remote EFM OAM Loopback is applied toward ML port and is not released, this loopback will be forcedly reset for normal Ethernet traffic after timer is expired.
6. Set the QoS Parameter group according to the relevant sections:
   - **Classification Method** (on page 7-3) (and PVID CoS for Classification Method set to L2 Priority)
   - Optional - (Ingress or Egress) **Rate Limit** (on page 7-5).
7. Click **OK** to save.

ETH Port Physical Interface Configuration

This section describes the Physical Interface sub-set of the Ethernet port configuration parameters. Refer to Configuring Ethernet Ports for an overview.

➢ **To configure the Ethernet port 802.3ah Physical Media parameters**

1. Access the Ethernet Port Configuration dialog (partial dialog showing the parameters covered in this section is displayed below).



2. To enable the interface, select checkbox **Enable**. Ports ETH-{1-4} can be configured in advance (without need to plug Ethernet cable first).

   Prior to enable ports ETH-5 and ETH-6, SFP-1-1 and SFP-1-2 modules should be either plugged (and then auto-configured) or just configured manually, keeping the option of pre-provisioning.

3. In the **SNMP Alias** field, enter an identifiable name for the Ethernet link. Range = up to 32 characters. This description is NOT sent along with SNMP messages such as log information. The same name will appear via TL1 communication and via SNMP communication, as "ifAlias" OID in IfXTable MIB.

4. Setting port communication Mode. This parameter is not relevant to HSL ports.

   The port communication mode is by default defined as **Auto-negotiation**, where the speed and duplex mode are automatically recognized. In some cases, such as assigning the port to a LAG or for 100BaseFX (fiber) ports, it is required to select the speed and duplex mode. For example, 100M HD refers to 100Mbps Half Duplex mode (in case of manual setting, set the **Pinout** MDI option as well).

   NOTE: upon insertion of SFP module to the system (and if Auto-configuration is allowed per system), ETH-5,6 port is automatically configured with: MODE=AUTO, Flow Control=OFF

5. If Auto-negotiation is NOT selected, decide on Pinout for ETH-{1-4} 10/100BaseT ports. If auto-negotiation enabled and link is Up, the MDI mode is automatically detected (Auto-MDIX)). MDI (Medium Dependent Interface) defines cable connector (pinout) between the signal transceivers and the link. Select as follows:

   - MDI - Straight connection. Used when connecting to an MDI-X device such as a switch.
   - MDI-X - Crossed connection. Used when connecting to an MDI device such as a PC NIC. Default for Ethernet COLAN port.

   If Auto-negotiation is NOT selected, Set the port **Flow Control** (not relevant to HSL ports). Select as follows:

   - OFF – no Flow Control mechanism is applied.
   - ON – Flow Control mechanism starts work in both TX and RX directions of the port.

   Flow Control is used to pause ingress traffic (regardless of frame priority) when the egress port is congested.

   - Flow control on RX direction obeys instructions from the opposite port, to slow down its own port transmit rate.
   - Flow control on TX direction instructs the opposite port to slow down its transmit rate.
   - Flow Control can be established as a part of Auto-negotiation or can be set manually.

   NOTE: In manual setting it is important that both ports are configured in the same way and in the same MODE, as the Flow control applied in HALF-DUPLEX and in FULL-DUPLEX modes are incompatible.

6. **LAG** assignment: If the port is to be assigned to a LAG, select the LAG to which the port will be allocated. Note that all ports assigned to the same LAG must have the same definitions. See **Static Link Aggregation (LAG) Configuration** (on page 4-39) on assigning LAGs.
7. **MAC Learning** - defines MAC address learning operation mode on the interface:
   - Auto - MAC learning is ON. Default setting on all ports.
   - Off - disables MAC address learning on the port. If MAC learning is disabled, traffic is forwarded to all non-RX ports (broadcasted) participating in the VLAN with RX-port.
   - Limit - number of MAC addresses limited according to setting on Bridge Level Configuration (Ethernet Bridge Configuration) **MAC Limit Size** value.
   - Filter - use Allowed MAC SA mechanism (see **MAC Filtering** (on page 5-9)).
8. Define additional parameters on the dialog according to the relevant sub-sections or click **OK** to save.

LLCF on ML Devices

LLCF (Link Loss Carrier Forward) is used to detect reduced bandwidth or complete loss of traffic passed through two ML NEs (CO and CPE) and to report the occurrence or clearance of such an event towards the Customer (downstream) or WAN (upstream) devices attached to ML NEs via Ethernet ports. ML700 supports both **Port Triggered** and **MEP Triggered** LLCF, where *MEP triggered LLCF* is supported *only on Ethernet Service* ports.

The LLCF options are configured via the Ethernet Port Configuration dialogs. This section provides information on LLCF operation in ML700 and describes how to configure the LLCF functionality.

LLCF operates as follows:

- LLCF *occurrence* on an Ethernet port signifies that the ML NE port halts a link signal transmit, emulating LOS on the connected ML devices.
- LLCF *clearance* on an Ethernet port signifies that the ML NE port renegotiates and starts transmit toward connected ML devices.
- LLCF is *raised immediately* upon local Trigger Port failure and *within ~100 msec* of upon Trigger port failure on attached device (when LLCF is propagated twice).
- LLCF on HSL port is cleared *only* when Ethernet traffic is restored on the HSL (when synchronization of all bonded in HSL modems is complete).

ML700 supports LLCF in both Downstream and **Upstream** (on page 4-35). For additional configuration criteria, refer to When Configuring LLCF in ML Devices.

Downstream LLCF

For DOWNSTREAM link monitoring (useful in P2MP or P2P topologies):

- **CO NE** - should be configured to monitor local ports as LLCF triggers, where upon port failure, the CO NE reports the CPE NE through HSL by an LLCF message.
- **CPE NE** - should be configured to monitor local HSL port as an LLCF trigger – this allows monitoring local HSL port physical failure as well as CO NE port failures, which are propagated via HSL by messages (CO failures will be sent to CPE NE only if HSL on CO NE is configured appropriately).
- If another CPE is configured as an LLCF trigger port, it shall detect LOS on its Ethernet port and notify the CO NE. The CO NE provides "Intra-switch" between the CPEs and sends LLCF to the target CPE.

NOTE: CO NE HSL can be optionally configured to monitor available HSL BW and report LLCF notification upon configurable threshold crosses down.

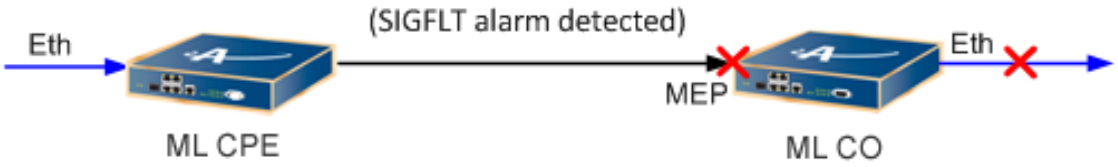
The following figures illustrate end-to-end *downstream* LLCF notification for four types of failures: HSL down, low bandwidth on the HSL, CO Ethernet port down and CPE port down.

HSL down is identified by the CPE and CPE Ethernet port is disconnected.
CPE configuration: Ethernet Port Configuration dialog – **Trigger List** to include HSL

Downstream LLCF - Reduced HSL BW

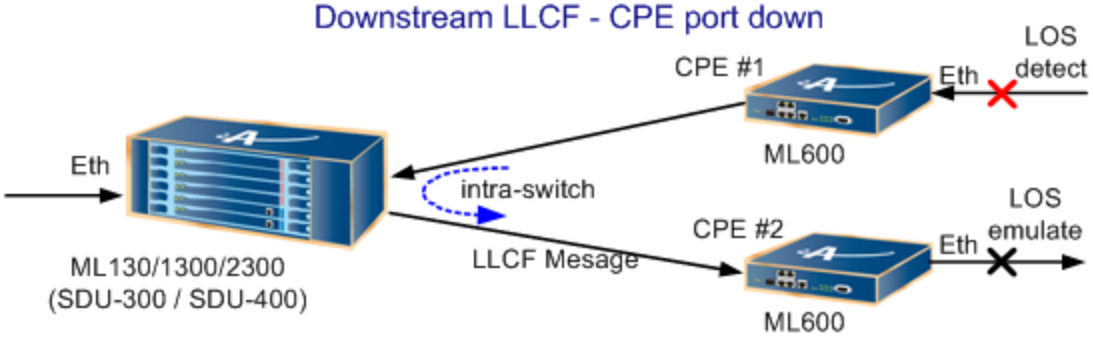
HSL BW below LLCF Threshold (configurable) is identified by the CPE and CPE Ethernet port is disconnected.
CO configuration: HSL Configuration dialog – **LLCF Threshold** value is set,
CPE configuration: Ethernet Port Configuration dialog – **Trigger List** to include HSL

Downstream LLCF – CO Eth Down



SIGFLT (Signaling Fault) on Maintenance End Point (MEP) on Y.1731 is identified by the CPE and CPE Ethernet port LOS is emulated.
CPE configuration: Set Y.1731, create MEG and MEP on Trigger port, and configure LLCF MEP Trigger on Target port

Downstream LLCF - CPE port down



CPE Eth. port down is identified by the CPE #1 and LLCF is forwarded to CPE #2 via CO NE ("intra-switch").
CPE #1 Configuration: Ethernet port configured as trigger port.
CO Configuration: HSL from CPE #1 is configured as LLCF trigger of HSL towards CPE #2.
CPE #2 Configuration: HSL in LLCF trigger list, emulates LOS upon receiving LLCF from CO NE.

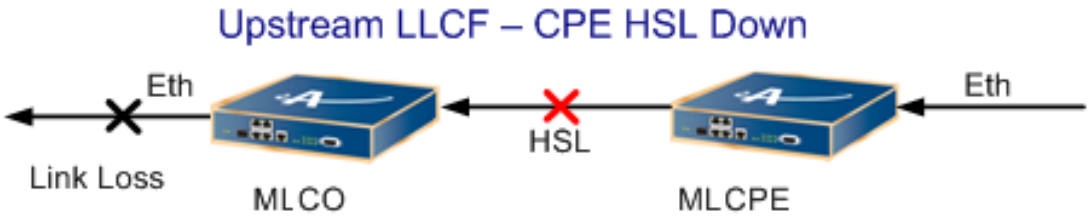
Upstream LLCF in ML700

For UPSTREAM link monitoring (useful in P2P topologies):

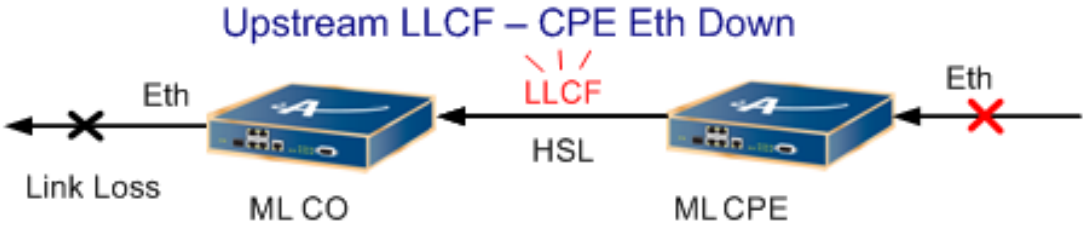
- **CO NE ETH port(s)** - should be configured to monitor local HSL port as an LLCF trigger - this allows to monitor HSL port physical failure.
- Additionally, if **CPE NE** is configured appropriately, CO NE ETH port(s) will be capable of monitoring CPE NE ETH port(s) failure. To enable this option, the CPE NE HSL port should be configured to monitor local ETH ports as LLCF triggers.

NOTE: Reduced HSL BW occurrence cannot be propagated in the Upstream as an LLCF event (even if it is configured on CO NE HSL). LLCF BW threshold occurrence is always propagated toward the CPE NE HSL.

The following two figures show examples of Upstream LLCF: loss of HSL and loss of CPE Ethernet port.



Link Loss on CPE Ethernet port is identified by the CPE HSL and the CO Ethernet port. CO Ethernet port emulates link loss towards the next device in the (up) link.
CO configuration: Ethernet Port Configuration dialog – **Trigger List** to include HSL



Link Loss on CPE Ethernet port is identified by the CPE HSL and the CO Ethernet port. CO Ethernet port emulates link loss towards the next device in the (up) link.
CO configuration: Ethernet Port Configuration dialog – **Trigger List** to include HSL.
CPE configuration: HSL Ethernet (attributes) Port Configuration dialog – **Trigger List** to include CPE Ethernet port.

Configuring for LLCF in the ML

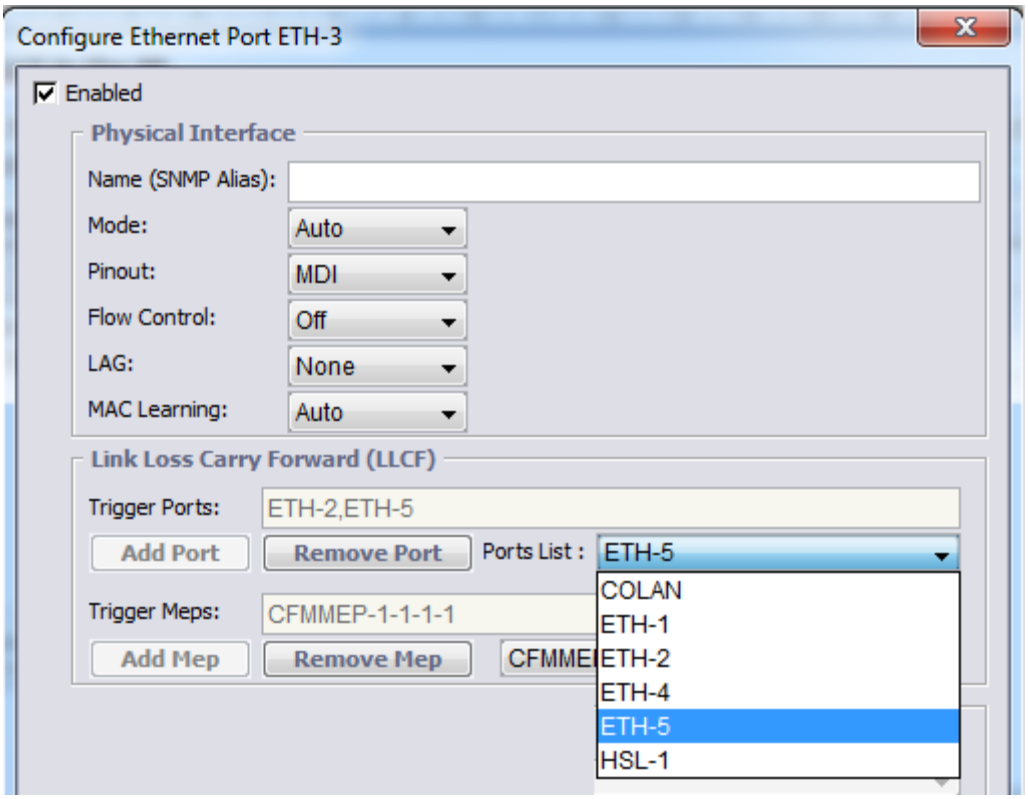
This procedure describes how to define the local target LLCF triggers. The Ethernet Configuration dialog provides options for defining two types of triggers:

- Port triggers - relevant for HSL and Ethernet ports
- MEP triggers - relevant only for Ethernet ports

For more information on LLCF, refer to **LLCF in ML700 Devices** (on page 4-32).

➢ To define the Local Target LLCF Triggers

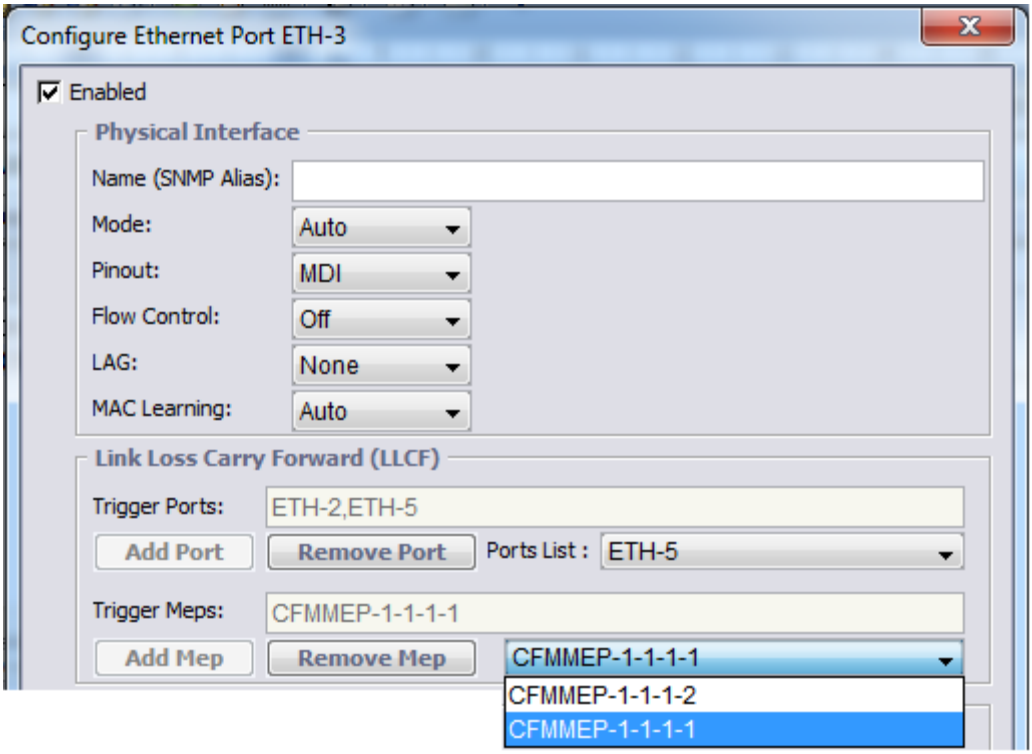
1. In the **Network Element** tree, select **Ethernet Ports** and choose the Ethernet HSL port that will be enabled for LLCF.
2. Click the **Configure.** The configuration dialog appears.



3. To define Trigger Ports:
   - In the **Ports List**, select each of the ports that will trigger the LLCF response if they are disconnected, the frequency is below the defined threshold or the extended limits.
   - Click **Add Port** after each selection. The port will be added to the list. (To remove a port, select the port and click **Remove Port**).
4. To define Trigger MEPs (this option is NOT relevant to HSL as a target port).

NOTE: The list of available MEPs consists of predefined MEPs (according to **802.1ag MEP Definitions** (on page 11-8)).

5. In the **CFM MEP List**, select each of the available (predefined) MEPs that will trigger the LLCF response if Signaling Failure alarm (see **MEP Alarm Troubleshooting** (on page 11)) is raised on the MEP they are disconnected, the frequency is below the defined threshold or the extended limits.



6. Click **Add MEP** after each selection. The port will be added to the list. (To remove a port, select the port and click **Remove MEP**).

LLCF Considerations

When configuring LLCF, note the following:

- A port which is specified as LLCF trigger on another port, cannot use this other port as an LLCF trigger for itself.
- Blocking configuration between ports of single NE is validated and rejected, although validation between two NEs in link is not provided. The user should avoid concurrent UPSTREAM and DOWNSTREAM LLCF configuration, otherwise Ethernet port, once failed on either WAN or Customer side, will permanently hunt traffic transmit on both sides beyond ML link.
- A LAG cannot be added (as an item) to the list of monitored ports; however, individual ports allocated to a LAG can be monitored.
- Multiple Ports can be set as LLCF trigger on all ML devices. If multiple LLCF triggers are listed, the LLCF target port will forward the event (by message or disconnect) only if all enabled ports listed as trigger will fail. If any one of the failed ports in the LLCF Trigger List is up again, the LLCF target port will forward the event (by message or recovery).

- If an LLCF port cannot be immediately protected (i.e. is in ALL APS group which is still active, or PROTFBLK time does not allow performing APS) – an LLCF (toward the HSL) will be sent.
- Either HSL or ETH ports can be specified as LLCF target or LLCF trigger.
- In cases both Port LLCF trigger and MEP LLCF trigger are available and may be configured simultaneously , LLCF will be applied when all (AND condition between LLCF Trigger Ports) listed ports have a failure condition OR at least one (OR condition between LLCF Trigger MEPs) listed MEP have a failure condition.

Static Link Aggregation (LAG)

ML systems support Ethernet trunking that provides a high-speed, full-duplex bandwidth link by converging Ethernet ports (HSL ports cannot be converged) into one logical channel. This allows load sharing of traffic among the links in the channel as well as redundancy in the event that one or more links in the channel fail.

The bandwidth of two or more compatibly configured ports can be combined into a single logical link (the maximum number of ports depends on the ML and SDU card models). All the ports to be allocated to a LAG must be the same speed and configured to full-duplex mode. The load-balance policy (frame distribution) can be based on a MAC address (Layer 2) or an IP address (Layer 3).

Static Link Aggregation (LAG) is especially effective for optimizing bandwidth for cascaded ML CO systems. It provides the following advantages:

- Logical aggregation
- Multiplies available bandwidth
- Group configuration for a number of interfaces
- Load balancing - where load balancing is optimized for 2 and 4 ports in LAG. Load between 3 and 5 LAG members may not be balanced equally
- Can be used to reduce the number of direct connections to the networks
- Fault tolerance - traffic of a failed Ethernet port is re-routed

The LAG Port Workspace

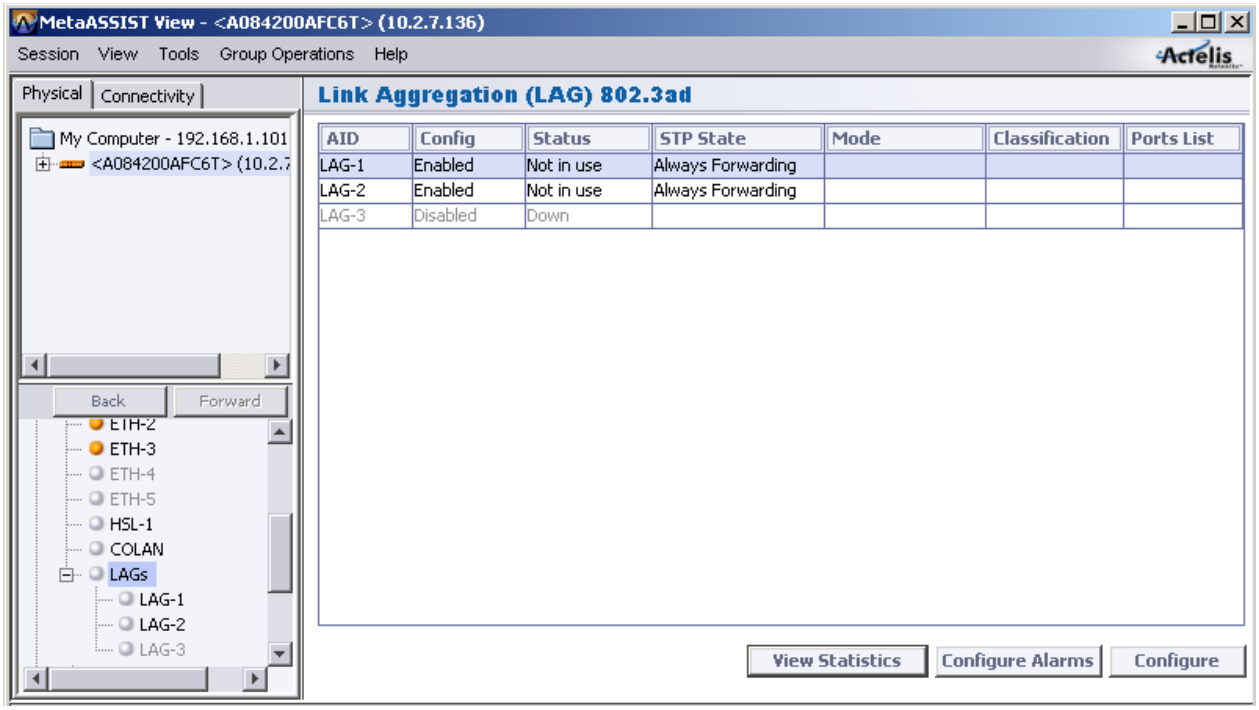
Several views are available for LAG ports configuration, monitoring and analysis. Each view has a dedicated set of monitoring and configuration buttons, where *some* of the options are common to the different views (the left pane in each view shows how the view is accessed).

- LAG Ports Glance View - lists all the LAG ports and their attributes in tabular format. In addition, the pane allows performing GROUP operations by selecting a number of LAGs on which the desired configuration or control operations will be performed.

  The following buttons are available:

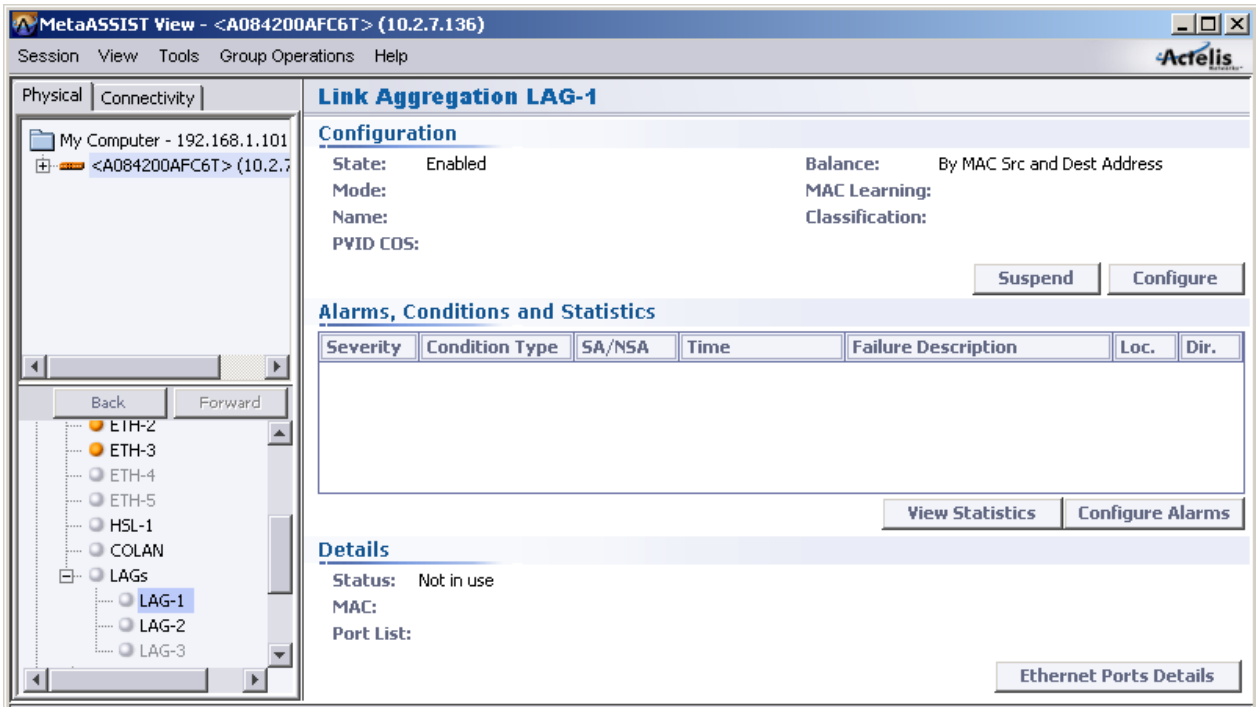
  - **Configure** (on page 4-42) - displays the LAG port configuration dialog.
  - Statistics - used to view Tx and Rx statistics of selected LAG

- Configure Alarms - alarm configuration for the selected port



- LAG Specific Pane- details and attributes of the individual LAG view. In addition to the Alarms display and configuration options that are standard in this type of display, and options described in the Glance View above, the pane contains the following areas:
  - Configuration - shows the current parameter definitions and provides access to the LAG port configuration (**Configure** button) options. the **Suspend** button is used to stop the LAG port operation.

- Ethernet Port Details - a report on alarms, Ingress Rate Limit, Flow Control, etc., for the port.



Overview of the LAG Configuration Procedure

➢ **To configure LAGs**

1. Determine the number (1, 2 or 3) of LAGs you will need and the speed you will require on each LAG.
2. Review the Configuration Considerations below.
3. **Enabling and Configuring each LAG** (on page 4-42).
4. Configure each of the Ethernet ports assigned to a LAG according to given criteria, and assign each port to the relevant LAG.

➢ **LAG Configuration Considerations**

- STP is always disabled on the LAG (and participating ports); therefore the LAG cannot be auto-disabled by STP decision, and continuously provides forwarding. It is strongly recommended to avoid configurations where ML ETH-x ports or other LAG have a duplicate connection with the LAG.
- It may take up to 50 msec (and cause some traffic disruption) to recognize operational failure of a port (LAG member) and switch over to another port (LAG member).
- Ingress/Egress Rate limiting is supported per port (in the LAG).
- A LAG takes on the VLAN definitions of the first port assigned to the LAG.

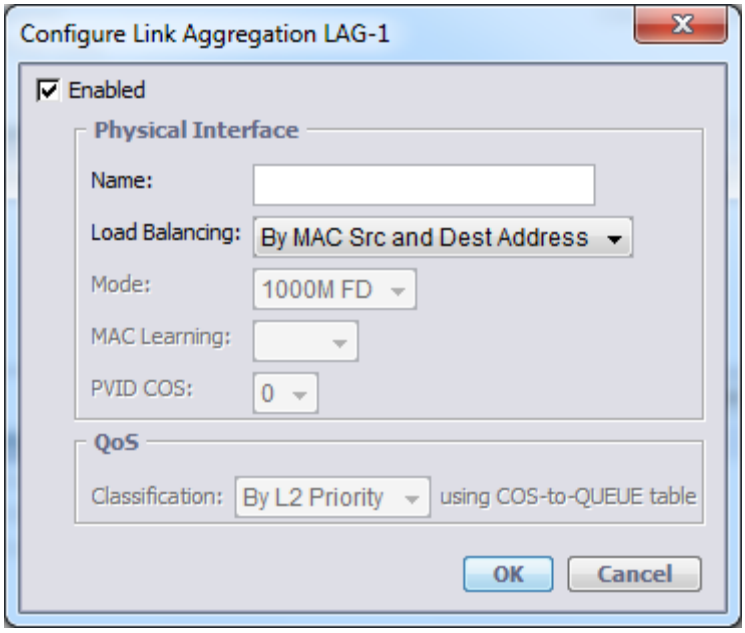
Enabling and Configuring LAGs

LAG links are configured by enabling the available LAG and defining its parameters. Ethernet ports are then added to the LAG. The following parameters are automatically defined by the first port that is allocated to the LAG: Mode and LLCF.

NOTE: See Configuring Ethernet Ports for a description of these parameters.

➢ **To configure LAG links**

1. In the **Network Element** tree, click **Ethernet Ports**, and under **LAGs** click the relevant LAG.
2. In the **Link Aggregation** pane, **Configure** area, click **Configure**. The LAG Configuration dialog appears.



3. Activate the LAG by selecting the **Enable** box. The available LAG configuration parameters will become activated.

   The following parameters are automatically defined by the first port that is allocated: **Mode** - the speed supported by the LAG, and **LLCF** - Link Loss Carry Forward. .
4. The ML operates according to the Load Balancing Policy - **MAC Source and Destination**. In this policy, packets are matched with given MAC source and destination addresses.
5. Allocate Ethernet ports to the LAG.

Allocating Ethernet Ports to LAGs

In order to configure LAGs:

- ETH ports can be bundled in the same LAG only if they have the same: Mode, Classification and RED.
- STP must be disabled on all ports. All ports except for the first that is added, must have none VLAN membership.
- Therefore: for each port disable STP and except for first port, disable VLANs.

➢ **To assign Ethernet ports to a LAG**

NOTE: HSL Ethernet ports cannot be assigned to a LAG.

1. Referring to Ethernet Service, HSL and COLAN Ports Configuration, access the Ethernet Configuration dialog of each port that will be allocated to a LAG and configure the following parameters:
   - Under **Physical Interface,** set **Mode** to **10FD, 100FD or 1000FD.**
   - Select full-duplex modes only and assign the same speed for all Ethernet port allocated to a specific LAG.
   - Select the **LAG** to which this Ethernet port will be allocated. (Only enabled LAGs will be displayed).
2. For (traffic or management) VLAN configuration for a LAG:
   - Configure ONE of the ports of the LAG according to **VLANs** (on page 8-1).
   - The VLAN configuration of the rest of the ports to be allocated to a LAG must be empty.

5 Ethernet Bridge, STP/RSTP

This chapter describes some bridge level configuration procedures and STP/RSTP. Note that the Ethernet Bridge pane shows the defined system level (Bridge) characteristics and provides access to configuration options.

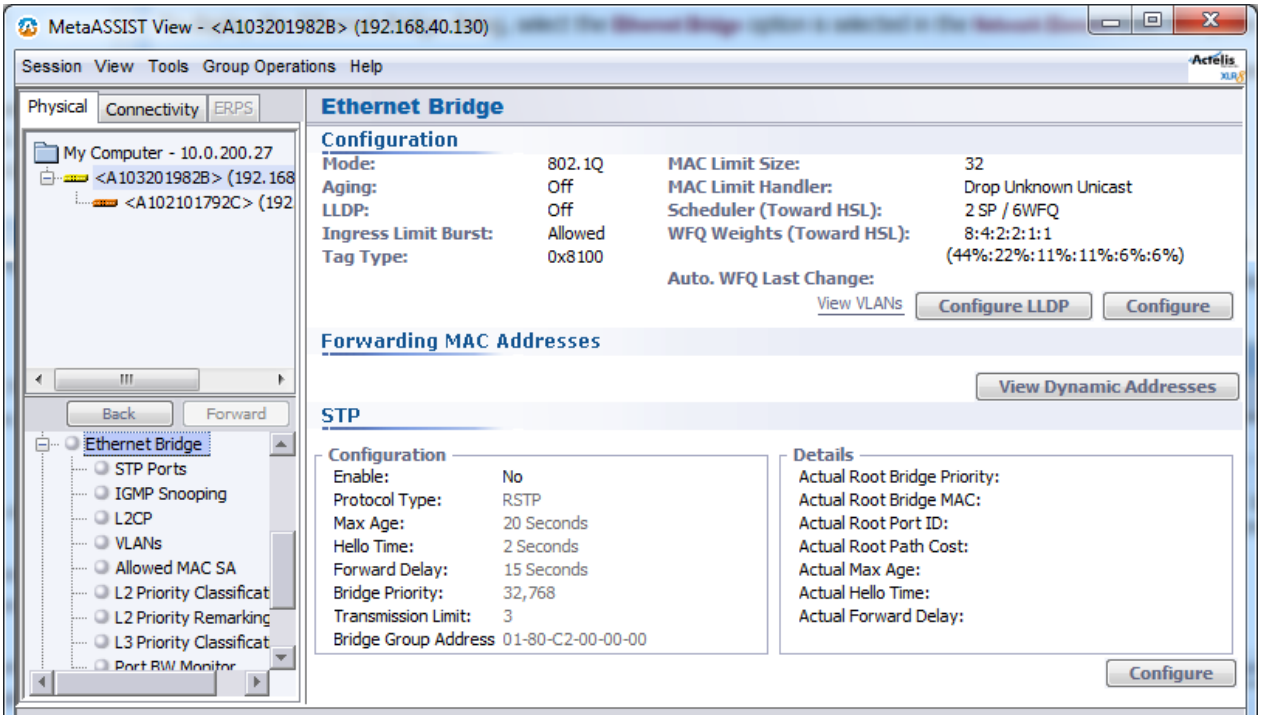
In This Chapter

Ethernet Bridge Pane

The Ethernet Bridge view displays the bridge level settings and provides access to the configuration options.

To display the Ethernet Bridge dialog, select the **Ethernet Bridge** option is selected in the **Network Element** tree. The pane includes the following areas:

- Configuration - shows the bridge level configuration settings and provides access to various configuration options through the corresponding buttons and link:
  - **Configure** button - access to Bridge configuration dialog
  - **Configure LLDP** (on page 5-7) button - LLDP configuration options
  - **View VLANs** (on page 8-7) link - provides access to VLAN management pane
- **Forwarding MAC Address** (on page 13-34) - the **View Dynamic Addresses** button invokes a display of the forwarding MAC addresses
- **STP** (on page 5-20) - shows the current STP parameters settings (Configuration area) versus the actual values (Details), and provides access to the configuration options (via the **Configure** button)



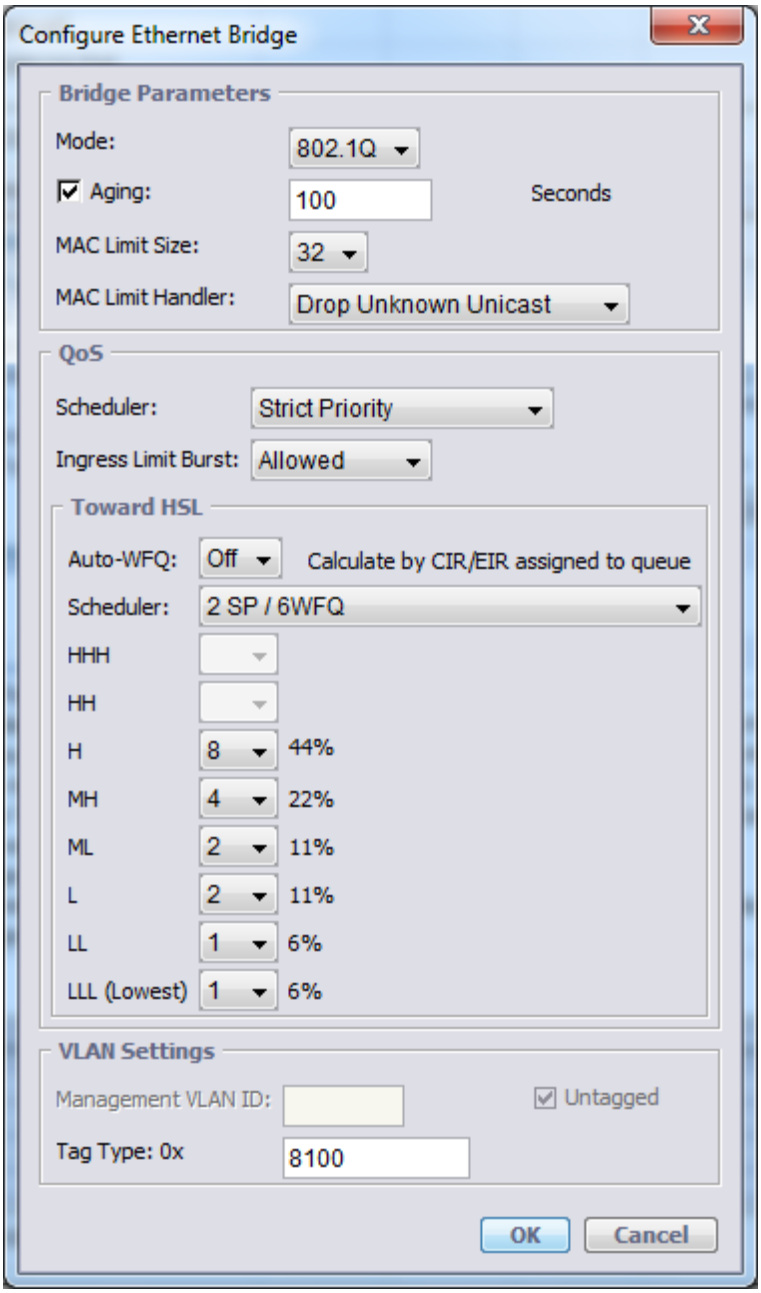
Ethernet Bridge

The Bridge Configuration dialog allows configuring system parameters relevant for the specific ML model. Not all fields are relevant to all models. Model specific information is provided in the field descriptions. This section details parameters specific to the Bridge mode. Some of the other parameters relevant to QoS or VLAN settings are briefly described and reference is provided to the relevant sections.

ML products implement transparent method of bridging as defined in IEEE 802.1. As such, when powered on, they automatically learn the location of the workstations by analyzing the source address of incoming frames from all attached networks. For example, if a frame is identified as arriving on port 1 from Host A, the bridge learns that Host A can be reached through the segment connected to port 1. Through this (learning) process, transparent bridges build a table that determines a Host's Accessibility. The table is used as the basis for traffic forwarding and its size is maintained at a minimum, by an aging mechanism that is used to delete MAC addresses that are no longer relevant (exceeded aging time value) from the database. This section describes the ML switching parameters (such as aging and learning), as well as QoS parameters such as Scheduling, encapsulation, etc.

➢ To configure the Ethernet bridge

1. In the **Network Element** tree, select **Ethernet Bridge** and in displayed pane, click the **Configure** button. The Configure Ethernet Bridge dialog appears.



2. In the **Bridge Parameters Mode** area:
   - 802.1Q - VLAN-aware (default). The forwarding table (used to learn source of frames) is independently learned by each VLAN.
   - 802.1D (not relevant for some models) - VLAN-unaware - the (not relevant for ML640/ML650/ML700). Forwarding table is shared by all the interfaces. If this option is enabled, the **Management VLAN ID** parameter (under VLAN setting) is available as well.

     Bridge-wide modes should be set equally on all Actelis systems installed in the particular deployment.
3. Also in the **Bridge Parameters** area, set the following parameters:

- Tune the **Aging** parameter - time duration over which newly learned addresses in the Forwarding database are valid.

  Range 10 to 3600 sec. (Default = 300 sec.).

  You may *disable* Aging by clearing the checkbox. However, s*ince in ML device Bridge Learning is always enabled for all ports, disabling Aging would eventually stop learning new addresses.* When this happens, all subsequent packet's source addresses cannot be learned. Packets designated to unknown addresses are broadcast to all possible ports (all the ports that are members of the appropriate VLAN).

- **MAC Limit Size** - MAC Learning limit. This value selected limits the NE Learning capabilities cumulatively on all Ethernet ports that are configured (see Ethernet Port Configuration) to Limit MAC Learning. While no ports are configured to Limit MAC Learning, MAC Limit Size value does not affect the system. Range: 2 to 32 (MAC addresses). (see Ethernet Port Configuration).

  MAC learning limit is available in Q-bridge mode only. The number of VLANs available for configuration is limited to 255 (in range from 1 to 4095) when MAC learning limit is enabled (configured on at least 1 Ethernet port).

- **MAC Limit Handler** - determines the behavior of ports whose **MAC Learning** is defined as **Limit** in the Ethernet Ports Configuration. The options are:
  - Forward Unknown Unicast (default) - Unknown MAC SA frames in ingress direction (from wire) are forwarded and broadcasted to all other VLAN member ports. Unknown MAC DA frames in egress direction (towards wire) will be dropped.
  - Drop Unknown Unicast - All Unknown MAC SA frames in ingress direction (from wire) and Unknown MAC DA frames in egress direction (towards wire) are dropped.

4. Configure the **QoS Scheduler and Queue Congestion parameters:** (on page 7-12)
5. Set the VLAN parameters:
   - In 802.1D mode, the Management **VLAN ID box** is configurable via this dialog box. For in-band management you need to specify management traffic type (VLAN-tagged or untagged) and for tagged traffic to set the Management VLAN ID.

     If STP is disabled, do not connect more than one ETH port and COLAN (MGMT) port to the same adjacent switch. See **Resolving Non-Alarmed Service Problems** (on page 15-16).

   - **Tag Type** is by default set to 0x8100 (HEX format) and can be changed (Q-Bridge mode only) according to the devices in the network. The Tag Type can be modified under the following conditions:

- No Ports with Untagged Membership (in either TRFC VLAN or MGMT VLAN) are defined.
- No MGMT VLAN with more than one Tagged Membership port is defined.
- No Ports with concurrent configuration in MGMT VLAN (with any membership type) and as a Tagged Member in TRFC VLAN, while the TRFC VLAN includes also another port(s) with non-STACKED Membership (TAGGED or UNTAGGED).

6. Click **OK**.

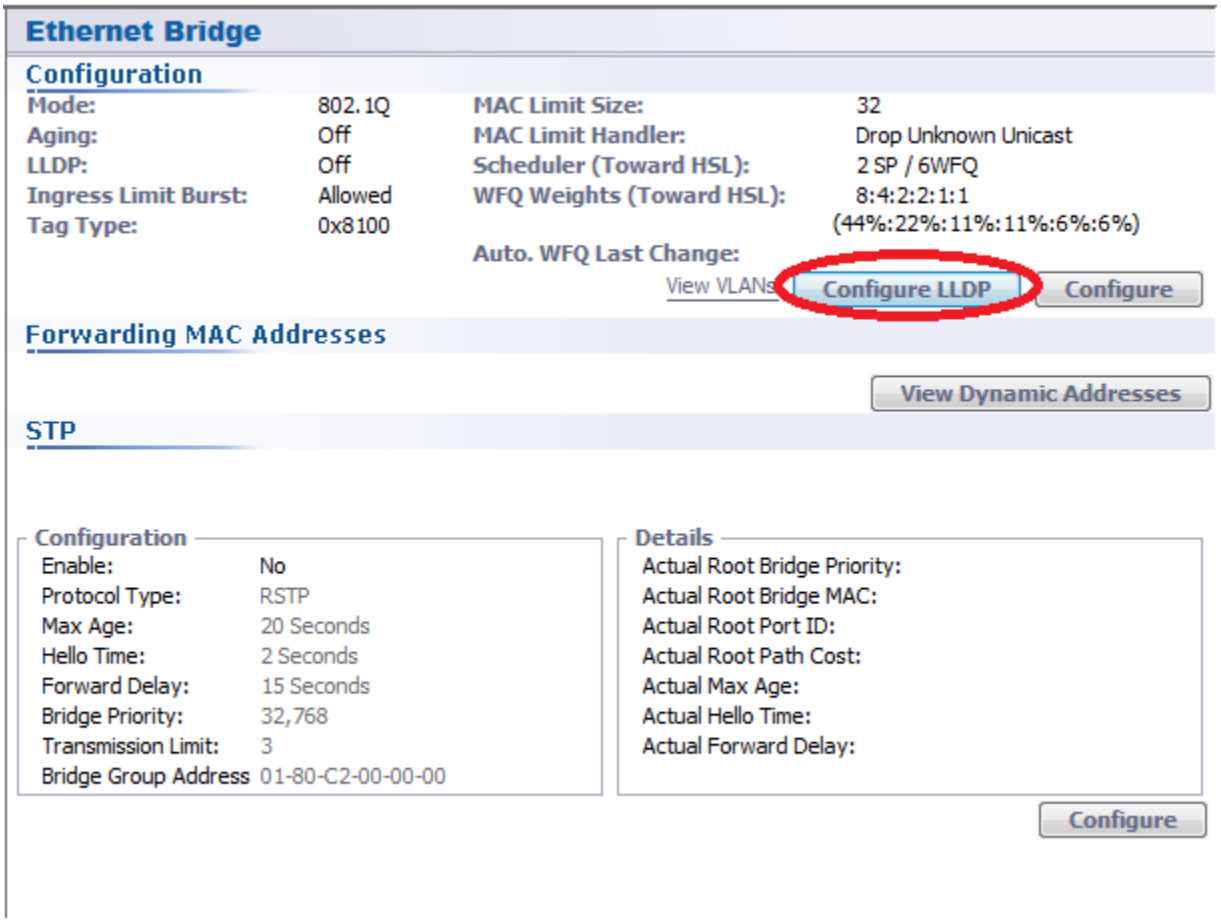
LLDP Configuration

IEEE 802.1ab defined Link Layer Discovery Protocol (LLDP) allows L2 (Ethernet) discovery of attached to ETH-x/COLAN ports of ML devices using the **NEs Linked via Ethernet** (on page 13-39) option in the Network Element Tree. This feature is parallel to the "**NEs linked via HSL**" feature (also in the NE Tree), which provides L1 (EOC) discovery of (CPE NE) devices attached to the HSL ports.

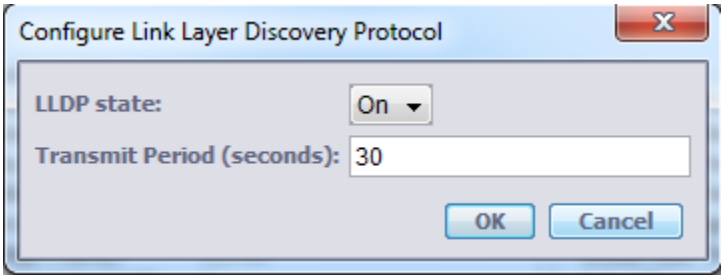
LLDP is disabled by factory default. Enabling LLDP on an ML NE will cause the ML device to start sending identification towards attached devices. If the attached devices don't support LLDP, the discovery table of ML NE will remain empty.

➢ To enable discovering NEs Linked via Ethernet

1. In the Network Element tree, select **Ethernet Bridge**. The Ethernet Bridge pane opens.



2. In the Configuration area, click the **Configure LLDP** button. The Configure LLDP dialog appears.



3. Set the parameters as follows and then click **OK**.
   - Set **LLDP State** to **ON**.
   - Configure the Transmit Time Period - this is the interval of time between two sequential LLDP messages to be sent. Default = 30

MAC Filtering

All ML700 models support Static MAC Filtering on a port level. This controls the service traffic through the ML NE. On these ports, frames from a wire (ingressing) will be forwarded only if their MAC SA value matches one of the specified MAC filters (ML level). (Unauthorized MAC addresses will cause an **INTRUDER** alarm on the port and will lock the port for learning until the port or unit is restarted.)

➢ **To configure MAC filtering**

1. **Set MAC Filters** – specify explicit MAC or range of MAC addresses allowed for forwarding through ML NE, see **Setting MAC Filters** (on page 5-9).
2. **Adjust Bridge** - adjust the bridge configuration to the expected MAC filtering behavior, see **Adjust Bridge Settings to MAC Filters** (on page 5-11).
3. **Configure ETH port** - set the required ML700 ETH port(s) to be secured via the Filtered Access mechanism, see **Setting Ports to Use MAC Filters** (on page 5-11).

Setting MAC Filters

Specify the Unicast MAC to be allowed. Each traffic frame will be inspected for matching between each configured MAC and MAC Source address (if Drop unknown unicast handler is set per Bridge) or MAC Destination address (if Forward Unknown Unicast handler is set per Bridge).

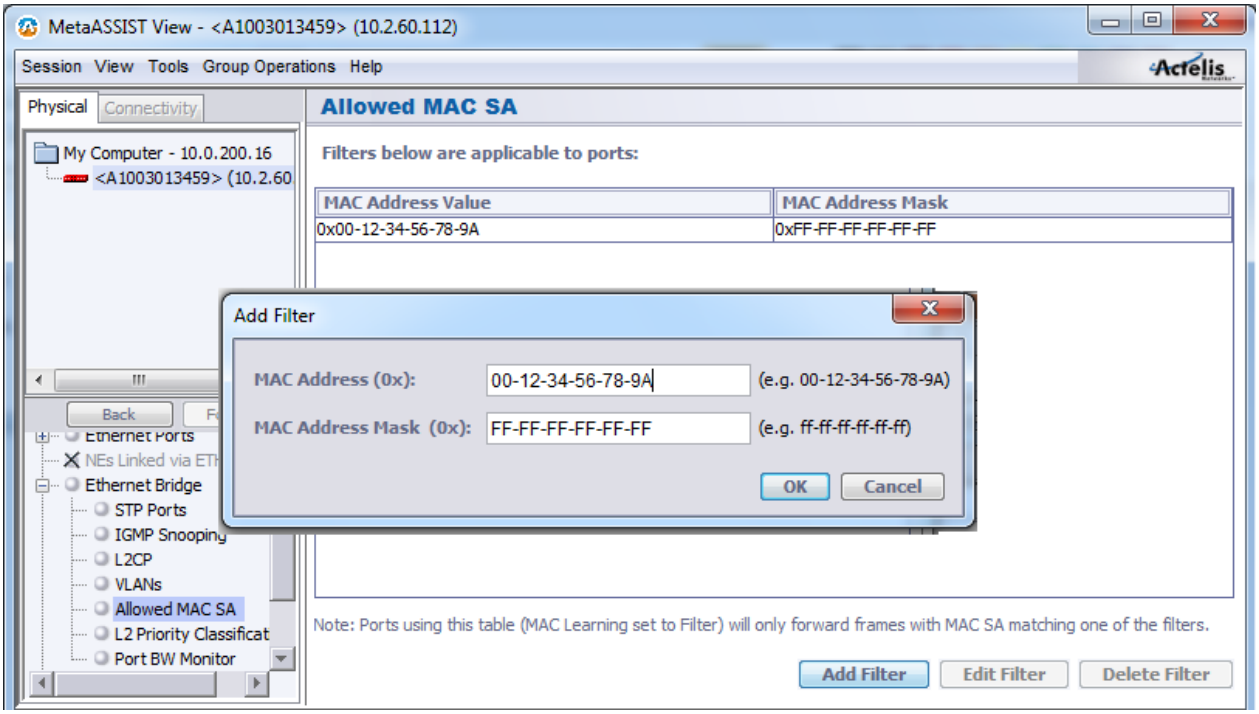
Up to 10 explicit MAC addresses can be specified in the table. MAC for blocking should not be specified.

The Mask is used to cover more than 10 MAC addresses. Mask can be used to cover only ranges that start from *even* number and comprise of sequential numbers that are multiples of two. If Value and Mask specified will result a MAC address of multicast (0x*1-**-**-**-**-**) or broadcast (0xFF-FF-FF-FF-FF-FF) type, then the MAC will not be considered as allowed and will be blocked (when all configuration will be completed).

➢ **To set the MAC Filters**

1. From the **Network Element** tree, under **Ethernet Bridge** choose **Allowed MAC SA**. The **Allowed MAC SA** dialog appears.

2. Click the **Add Filter** button.



3. In the invoked dialog, enter the MAC Address and the Mask (in Hexadecimal).
4. Click **OK**. The MAC address is added to the table of white addresses (allowed list).

NOTE: To edit or delete any of the MAC addresses in the table, select the relevant row in the table, and click **Edit Filter** or **Delete Filter** correspondingly. The last record cannot be deleted if there is at least one ETH port configured to use MAC filtering.

Adjust Bridge Settings to MAC Filters

It is recommended to configure Bridge as follows (refer to **bridge level parameters** (on page 5-3) for details).

Set MAC Limit Size to the maximal value (32) or less (min is one), taking into consideration customer LAN expected size (by PCs attached). This parameter defines the limit of learned MAC Addresses (per system), and is shared between all ETH-x ports configured with LEARNING value of Filter or Limit .

Set AGING to OFF to allow already learned valid traffic to be forwarded even after unauthorized access detection (when learning was blocked).
NOTE: If customer LAN MACs are not static, it is recommended to keep AGING enabled.

Set MAC Limit Handler behavior to Drop unknown unicast in order to avoid any unauthorized traffic from being sent to the network.

NOTE: This handler may cause periodic traffic disruption on the port traffic (every half-time of Aging period), so it is recommended to use this handler type with **Aging Off**. Default handler is set to "Forward Unknown Unicast", which will block traffic only when is returned back (any session assumes two-way communication) to the site. In other words, the default handler does not allow to complete sessions to non-allowed MAC addresses on CPE site, although does not protect a network from multicast/broadcast flood from non-allowed MAC address on CPE site.

Setting Ports to Use MAC Filters

Set ETH-x port(s) **MAC LEARNING** value to **Filter**.

It is recommended to set HSL-1 port (accessed through the **Ethernet Ports** --> **HSL-1** --> **Configure** button) **MAC LEARNING** value to **OFF** in order to allocate space for (up to 32) MAC learned addresses from Customer site only, and not from the whole network.

Resetting the Intruder Alarm

Unauthorized MAC addresses will cause an **INTRUDER** alarm on the port and will lock the port for learning until the port or unit is restarted. This will cause all new unknown unicast frames to be dropped on ingress or on egress (when answered), depending on the bridge settings. Earlier learned valid unicast frames will not be forwarded normally.

After **INTRUDER** alarm is raised, to restore the port normal operation, either restart the NE or perform the following steps:

1. Reset the port by either:
   - plugging/unplugging the cable *or*
   - performing any of the following remote operations: **Reset Port**, **Suspend/Resume Port**, **Delete/Enter Port**
2. To ensure MAC Filtering mechanism restart, Forwarding DB should be cleaned up:

   On **Ethernet Bridge** pane click **View Dynamic Addresses**, then click the **Delete All** button on the Dynamic Forwarding MAC Addresses pane.

NOTE: When MAC filtering is used, the units are limited to a configurable number of MAC addresses (1-32 addresses, default 32) being forwarded through the ML NE (even if no unauthorized attempts have occurred).

IGMP Snooping

IGMP snooping enables the ML device to forward multicast traffic intelligently, only to actively listening ports in the designated VLAN group instead of flooding all ports in the VLAN. It is used for applications such as video streaming to provide services only to the relevant ports. IGMP snooping on all ML products by default optimize only IP multicast traffic which is a subject of IGMP control conversations.
ML products do not police (drop) IP multicast traffic which is silently (without IGMP control traffic) forwarded, unless these IP multicast addresses are pre-configured on ML device.

NOTE: V1/V2 IGMP snooping is supported. IGMP V3 is transparently forwarded (not snooped).

IGMP Snooping Configuration Approach

➢ **IGMP Snooping configuration approach:**

- The **IGMP pane** (on page 5-14) provides access to IGMP configuration and monitoring options.
- Snooping is configured and controlled on two levels: system level (disabled by default) via the **IGMP Snooping Configuration** (on page 5-15) dialog and per Traffic VLAN (enabled by default for all VLANs). IGMP Snooping is only applied on VLANs on which it is enabled; on other VLANs, IP multicast traffic passes transparently.
- Up to 512 dynamically learned Multicast IP addresses can be optimized by IGMP snooping, the rest will pass transparently.
- In addition to the dynamic IP addresses, up to 32 Multicast IP addresses can be specified as static records. Traffic of the Multicast IP addresses specified in a static record, will be blocked initially (until any host subscription will be found through IGMP control traffic snooping).
- Both dynamic and static type addresses can be monitored via the **IP Multicast Monitoring** (on page 5-18) pane.

Note the following:

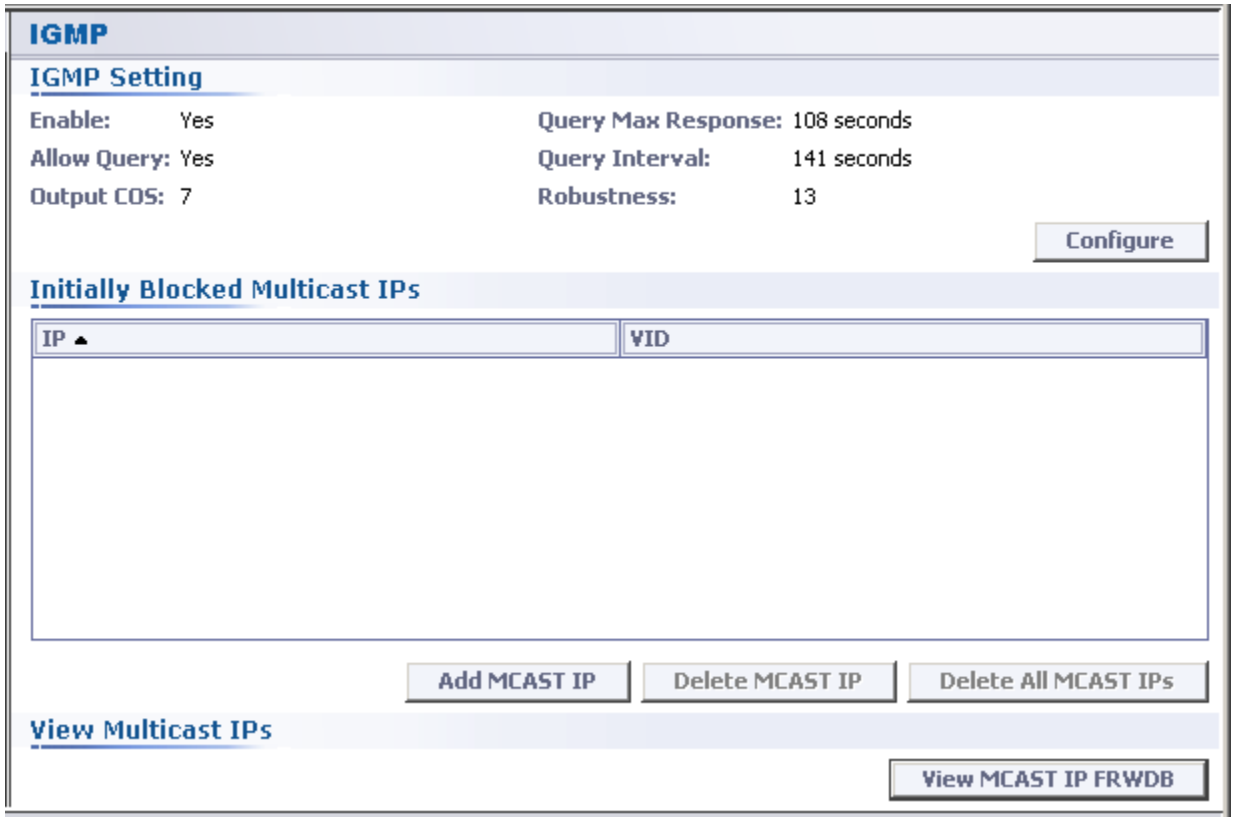
- 32-bit IP is translated to 28-bit MAC (4 bits are lost) - inherent behavior of IGMP .
- ML unit will handle dynamically learned as static records (initially block the traffic), if both IP are translated to the same MAC.
- ML unit forwards to the SUM of all registered ports (static or dynamic) for IP which is translated to the same MAC

IGMP Pane

The IGMP pane provides access to IGMP Snooping configuration and monitoring options.

➢ **To navigate the IGMP pane**

- Access the IGMP Snooping pane as follows:
  - In the **Network Element** tree, under **Ethernet Bridge** select **IGMP**. The **IGMP** pane appears.



- The pane provides the following options:
  - IGMP setting - displays the current settings and provides access to setting configuration options (**Configure** button).
  - Initially Blocked Multicast IPs - used for blocking specific IP sources of stream video until they are relevant so they do not load the network.
  - View Multicast IPs - enables monitoring selected IPs

IGMP Bridge Level Configuration

This dialog is used to enable and configure IGMP Snooping on the system level. (It is then applied to VLANs on which the option is enabled). ML devices perform ONLY snooping and cannot be used as IGMP server (Querier); however, ML devices can be configured with IGMP Querier parameters used for fast convergence (after ML reboot, port failure, STP topology changes).

Note that ML will send a query with IP SA= 0.0.0.0 (as an IGMP proxy). To configure ML with fast convergence option, enable Allow Query and set Out COS used by Query messages originated from ML.

NOTE: All IGMP except for Allow Query and Out COS (that are used for fast convergence of IGMP snooping), should match on all IGMP queries available in the network.

➢ **To Configure the IGMP Snooping Bridge Level Parameters**

NOTE: Be sure to enable IGMP snooping in the VLAN Configuration dialog.

In the **IGMP Pane** (on page 5-14), **IGMP Settings** area, click the **Configure** button. The following dialog appears.

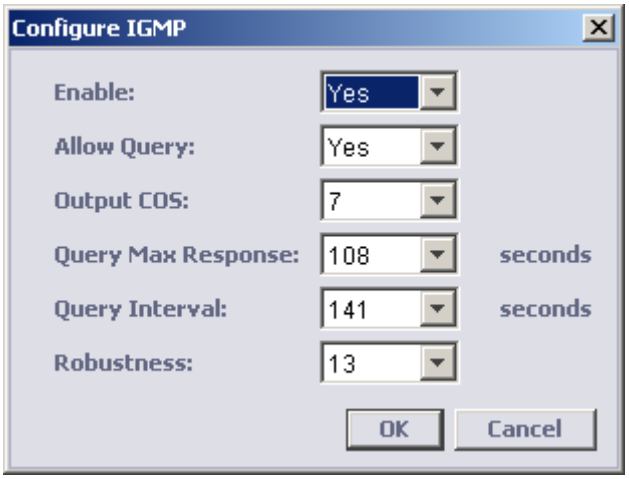


Table 17: IGMP Parameters

Value	Description
Enable	Yes - Snoop IGMP function is operational on the relevant VLANs. No - all multicast traffic is forwarded to all ports in VLAN boundaries, regardless of VLAN setting to snoop IGMP. Clears all dynamically learned multicast forwarding addresses and keep static multicast IPs configured.
Allow Query	Used to configure ML with fast convergence option. To set the fast convergence option, enable Allow Query and set Output COS used by Query messages originated from ML. ML devices will send query with IP SA= 0.0.0.0 (as an IGMP proxy).

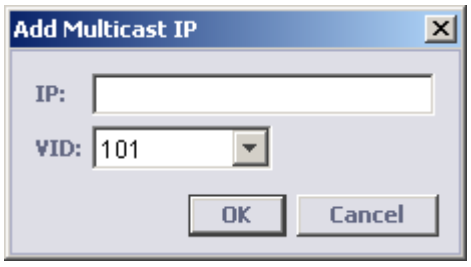
Output COS	OUTPUT COS bit remarking, applied on IGMP traffic, if tunneled through CPU. If mirrored and copied to CPU (SDU-400), parameter is configurable but not applicable. Regeneration, classification, remarking will be applied as for regular traffic (according to rules configured). Default value is 5. Valid values: {0-7}.
Query MAX Response	Query Response Interval inserted into the periodic General Queries. Default: 100 (10 seconds). Valid Range: {0 – 255} By varying the Query Max Response Interval, an administrator can tune the burstiness of IGMP messages on the subnet; larger values make the traffic less bursty, as host responses are distributed over greater intervals. The number of seconds represented by the Query Max Response Interval must be less than the Query Interval. In passive mode used as timeout for FSM.
Query Interval	The Query Interval is the interval between General Queries sent by the Querier. Default: 125 seconds. Valid range {2 – 255} By varying the Query Interval, an administrator may tune the number of IGMP messages on the subnet; larger values cause IGMP Queries to be sent less often. In passive mode, used as timeout for FSM.
Robustness	The Robustness Variable allows tuning for the expected packet loss on a subnet. If a subnet is expected to be lossy, the Robustness Variable may be increased. IGMP is robust to (Robustness Variable-1) packet losses. Range = 2 – 255, default = 2

Static Multicast IP Configuration

IGMP snooping on all ML products by default optimize only IP multicast traffic which is a subject of IGMP control conversations.
ML products do not police (drop) IP multicast traffic which is silently (without IGMP control traffic) forwarded, unless these IP multicast addresses are preconfigured as STATIC on ML device.
Configured Multicast IP addresses are persistent and is not affected by IGMP configuration changes (enabled/disabled per Bridge or VLAN levels).

➢ **To manually add a static IGMP Snooping IP**

1. In the **IGMP Pane**, click the **Add Multicast IP Forward** button. The following dialog appears.



2. In the **VID** list, choose the relevant VLAN (supporting IGMP) and then enter the **IP.**
   Valid range: 224.0.0.3 to 239.255.255.255.
   The IP will be manually added to the list.

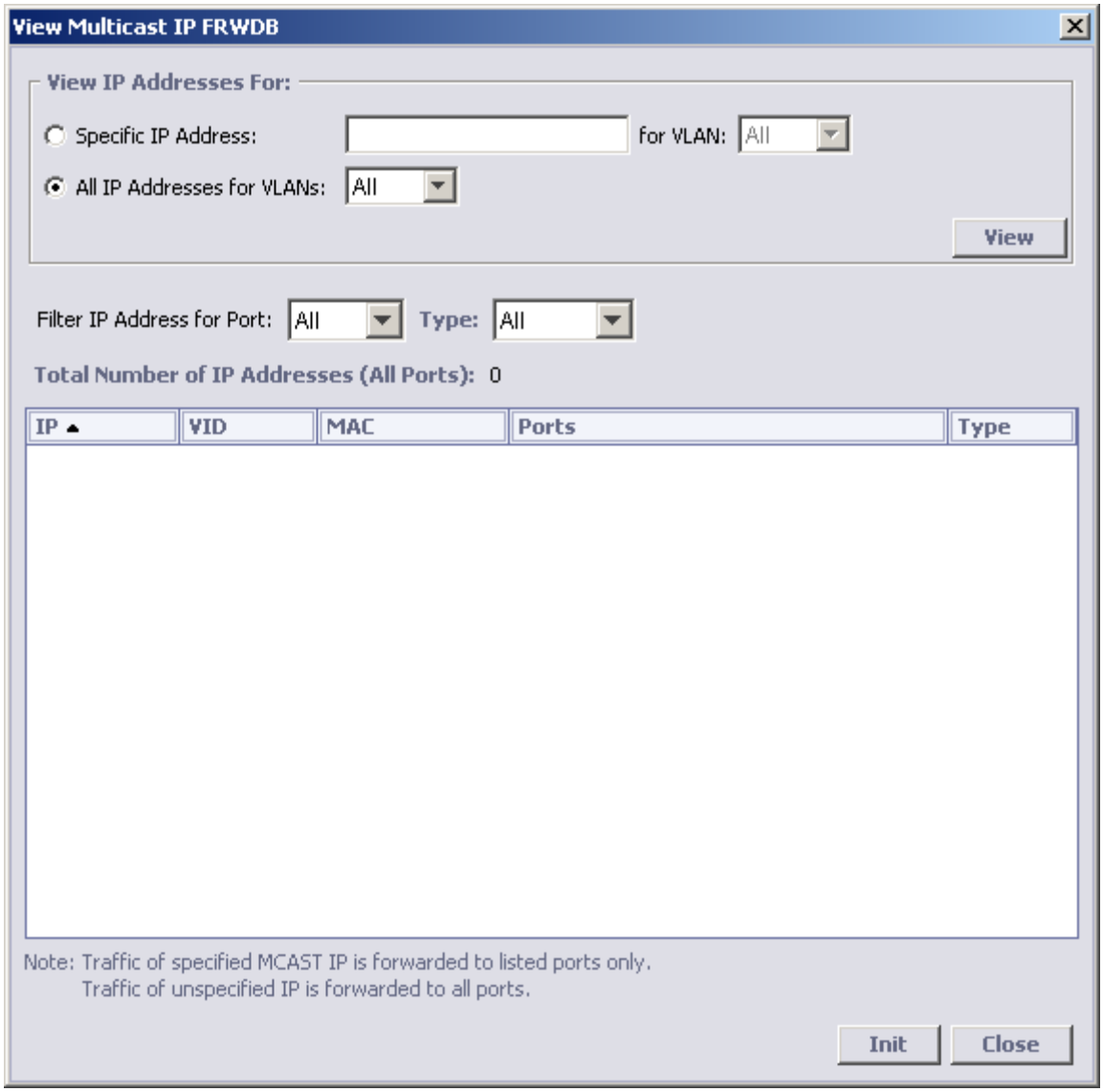
NOTE: Use the **Delete MCAST IPs** and **Delete ALL MCAST IPs** button to remove elements from the list.

IP Multicast Monitoring

You can view information on *user specified* multicast Group IPs. The viewed IPs are selected according to VLAN(s). The display can be further filtered according to ports and other criteria.

➢ **To view information on specific IPs**

1. In the **IGMP Pane**, **View Multicast IP** area, click the **View Multicast IP Forward** button. The following dialog appears.



2. Using the available options, choose the IP addresses to be viewed using one of the following criteria:
   - **Specific IP Address** - enter a specific IP MCAST Group Address and choose to view it for ALL or a selected VLAN.

- **All IP Addresses** - if this option is selected, all IPs for All or the selected VLAN are displayed.

3. Click **View**. The relevant IP addresses will be displayed along with VID, MAC, Ports and Type information.
4. You may filter the display according to port type and address type: Dynamic or Static.
   - In **Filter IP Address for Port** - choose the ports for which the IP addresses will be displayed (**All** displays the addresses for all ports).
   - In the **Type** field - choose **Dynamic** to show only dynamically identified IP addresses and **Static** to show only manually defined IP addresses.

NOTE: use the **Init** button to clear the display.

STP/RSTP and Provider Bridge Configuration

Spanning-Tree Protocol (STP) is a link management protocol used in Ethernet bridged networks to provide path redundancy while preventing undesirable loops in the network. This is done by verifying that only one active path exists at any one time between two stations since multiple active paths between stations cause loops in the network. Rapid Spanning-Tree Protocol (RSTP) evolved on the basis of STP and provides faster recovery of connectivity after an outage.

Another standard, IEEE 802.1ad (Provider Bridge), further extends STP/RSTP usage by enabling differentiation between STP/RSTP messages from the Customer Bridges and those from the Provider Bridges. This is done through the allocation of different MAC address space according to the type of bridge (Customer or Provider).

Spanning tree algorithm-aware bridges exchange configuration messages periodically. The configuration message is a multicast frame called BPDU (Bridge Protocol Data Unit) or Hello message. According to the BPDU, these STP-aware bridges will construct a loop free network with a tree architecture.

NOTE: The only difference between STP and RSTP implementation, is defining the addressing space which allows the coexistence of fully separated Customer and Provider loopless topologies.

Actelis ML devices support STP/RSTP in accordance to either Customer Bridge (IEEE 802.1d) or Provider Bridge (IEEE 802.1ad) standards, where STP/RSTP BPDU Address is configurable per Network Element:

- IEEE 802.1d uses the reserved MAC 0x01-80-0C-00-00-00 for STP/RSTP BPDU.
- IEEE 802.1ad uses the Reserved MAC 0x01-80-0C-00-00-08 for STP/RSTP BPDU.

ML device STP/RSTP configuration can be set at bridge level and at port levels. By default, STP is *disabled* at *bridge* level and *enabled* at *port* levels.

The two reserved MACs are additionally controlled by L2CP application. When L2CP is configured to DROP or TUNNEL, the reserved MAC, STP application is not triggered. The STP BPDU behavior that is described below, is valid only when L2CP control (port level configurable) for the chosen reserved MAC (0x01-80-0C-00-00-00 or 0x01-80-0C-00-00-08) is set to PEER handler. PEER handler accepts BPDU locally on NE, and performs according to the application configuration.

Table 18: STP Configuration Description

STP Configuration	Description
Bridge and Port level STP is Disabled	Does not Participate in STP. BPDUs are dropped.
Bridge and Port level STP is Enabled	Participates in STP. BPDUs are accepted and answered.

STP Configuration	Description
Bridge level STP is Enabled, Port level STP is Disabled	Does not Participate in STP. BPDUs are dropped.

STP/RSTP Configuration Principles

- **STP/RSTP configuration principles are as follows:**

1. Select a root bridge

Only one bridge can be selected as the root bridge in a given network. All other decisions in the network, such as which port is blocked and which port is put in forwarding mode, are made in reference to this root bridge. The root bridge is the "root" of the constructed "tree".

1. One of the important fields included in the BPDU is the bridge ID. Each bridge has a unique bridge ID. The root bridge is the bridge with the lowest bridge ID in the spanning tree network.
2. The bridge ID includes two parts, bridge priority (2 bytes) and bridge MAC address (6 bytes). The 802.1d default bridge priority is 32768. For example, a switch with default priority 32768 (8000 hex) has a MAC address of 00:A0:C5:12:34:56 and its bridge ID is 8000:00A0:C512:3456.
3. On the root bridge, all its ports are designated ports. Designated ports are always in the forwarding state. While in forwarding state, a port can receive and send traffic.

2. Select a root port for the non-root bridges

For the non-root bridges, there will be one root port. The root port is the port through which these non-root bridges communicate with the root bridge (the "leaf" side of the "tree").

4. The root port is the port on the non-root bridge with the lowest path cost to the root bridge. The root port is normally in the forwarding state.
5. Path cost is the total cost of transmitting a frame on a LAN through that port to the bridge root. It is assigned according to the bandwidth of the link. The slower the media, the higher the cost.

NOTE: When multiple ports have the same path cost to root bridge, the port with lowest port priority is selected as the root port.

3. Select a designated port on each segment

For each LAN segment (collision domain), there is a designated port. The designated port has the lowest cost to the root bridge. Designated ports are normally in the forwarding state to forward and receive traffic to the segment. If more than one port in the segment has the same path cost, the port on the bridge which has the lowest bridge ID is selected as a designated port.

4. Active Topology Monitoring and Update

After STP determines the lowest cost spanning tree, it enables all root ports and designated ports, and disables all other ports. Network packets are therefore only forwarded between root ports and designated ports, eliminating any possible network loops. STP-aware devices exchange BPDUs periodically. A new spanning tree is constructed when the bridged LAN topology changes.

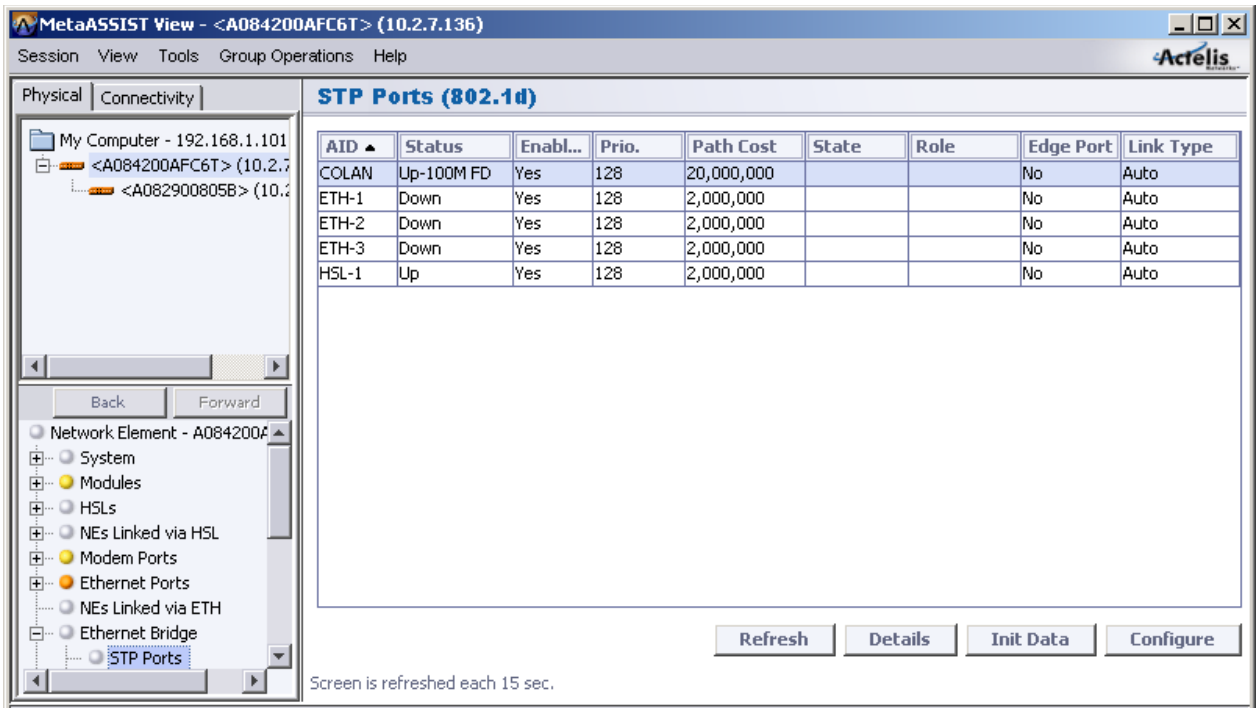
Once a stable network topology has been established, all bridges listen for Hello BPDUs transmitted from the root bridge. If a bridge does not get a Hello BPDU after a predefined interval (Max Age), the bridge assumes that the link to the root bridge is down. This bridge then initiates negotiations with other bridges to reconfigure the network to re-establish a valid network topology.

The STP Workspace

Several views are available for STP configuration, monitoring and analysis. Each view has a dedicated set of monitoring and configuration buttons, where *some* of the options are common to the different views (the left pane in each view shows how the view is accessed):

- STP Ports Glance View - lists all the STP Ports and their attributes in tabular format and provides various display and management options. In addition, the pane allows performing and GROUP operations by selecting a number of ports on which the operations are performed. The following buttons are available:
  - Refresh - updates the displayed data
  - Init Data - resets the data
  - **Details** (on page 5-26) - shows the *configured* and the *actual* information on a Bridge and Port level for the *selected* port.

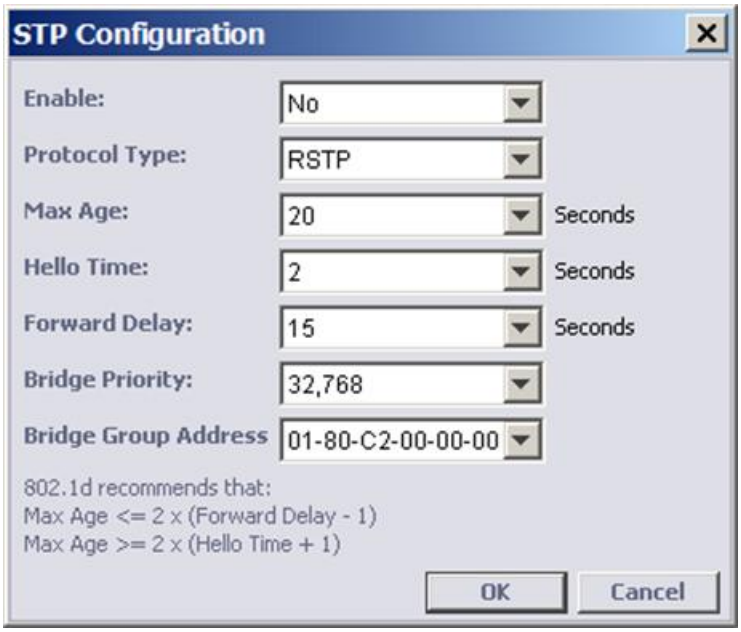
- **Configure** (on page 5-23) - invokes the STP configuration dialog



STP/RSTP Bridge Configuration

➢ **To Configure STP global parameter (per Ethernet Bridge):**

1. In the Network Element tree, open **Ethernet Bridge**. The **Ethernet Bridge** pane opens.
2. In the **STP** area, click **Configure**. The **STP Configure** dialog appears.



3. Configure the parameters according to the definitions in the table below and click **OK**.

Table 19: STP Bridge Level Parameters

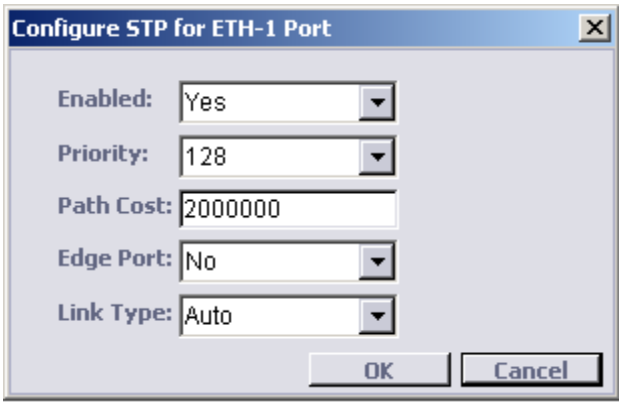
Parameter	Description
Enable	Enables or disables STP/RSTP BPDUs transportation • Enabled - STP/RSTP (according to the selected **Protocol Type** parameter) is set on a bridge level (enabled on all ports). • Disabled - STP/RSTP is not enabled on any of the ports. If required it is enabled on a port level.
Protocol Type	Determines which protocol is operational when it is enabled: • STP - Spanning Tree Protocol (usually used for Legacy networks) • RSTP - Rapid Spanning Tree Protocol (usually faster than STP) NOTE: The same protocol is to be used on all relevant network elements.
Max Age	Maximum time for keeping the received protocol information recorded for a port before discarding it. Select the maximum age (6 to 40 seconds).
Hello Time	Determines how often the switch broadcasts its hello message to other switches. Select the Hello Time (1 to 10 seconds)
Forward Delay	Defines the timeout to be spent by a port in the learning and listening states. It is the value of the forward delay parameter of the bridge.
Bridge Priority	The bridge with the highest priority is the Root bridge: The higher the Bridge's priority value, the lower its priority. Select the Bridge priority (0 to 61440 in steps of 4096)
Bridge Group Address	Select the address according to the bridge designation: • For systems designated as SP-Bridge provider - set the MAC to 0x0180C2000008 • For systems designated as CE-Bridge - set the MAC to 0x0180C2000000 The bridge will communicate on the defined MAC and will not accept another MAC, even if L2CP application is configured on the Ingress port to accept (as PEER) the RSRV MAC.

STP/RSTP Ports Configuration

➢ **To Configure STP/RSTP parameters on a port level**

1. In the Network Element tree, open **Ethernet Bridge**, **STP Ports**. The **STP Ports (802.1w** or **802.1d** for RSTP or STP accordingly) pane opens.
2. On the table, select an STP port.

3. Click **Configure**. The **Configure STP for <port name> Port** opens.



4. Configure the parameters according to the definitions in the table below and click **OK**.

The following table describes the defined parameters. Actual measured values on the Root port can be viewed by selecting a port in the STP View and clicking the **Details** button.

Table 20: STP Port Level Parameters

Parameter	Description
Enabled	Enables this port to operate with STP/RSTP according to the bridge level definitions.
Priority	Priority taken into account by STP when selecting a LAN port to put into the forwarding state. Higher Priority ports will be selected first. If all LAN ports have the same priority value, STP sets the LAN port with the lowest LAN port number in the forwarding state and blocks other LAN ports. Range: From 0 to 240 in steps of 16.
Path Cost	The STP/RSTP path cost default value is determined from the media speed of a LAN interface. Ranges: 1 - 200,000,000 for RSTP and 1 - 65535 for STP. Default values vary per AID; see Appendix A - Technical Specifications.
Edge Port	Configure the port as an Edge port if it is connected to a nonbridging device (for example, a host or a router). An edge port can start forwarding as soon as the link is up. Yes - port is configured as an Edge port No - port does not operate like an Edge port.
Link Type	Auto - Default. P2P - Recommended for rapid-PVST+ mode only. Specify that the link type for this port is point-to-point. If you connect this port (local port) to a remote port through a point-to-point link and the local port becomes a designated port, the switch negotiates with the remote port and rapidly transitions the local port to the forwarding state.

STP/RSTP Port Details

The configured and actual information can be displayed for selected STP ports, by *choosing the port* and clicking the **Details** button in the STP Glance view.

The following table only describes the *actual* parameter values. The configured parameter descriptions are available in the Bridge and Port configuration dialogs.

Table 21: STP Port Details

FIELD	Description
Transmission Limit	The maximum number of times BPDUs can be transmitted during Hello Time interval. Non-configurable parameter equal to 3.
Actual Root Bridge Priority	This is the actual unique identifier for this bridge, consisting of bridge priority plus MAC address. Only the bridge priority is displayed.
Actual Root Bridge MAC	This is the actual unique identifier for this bridge, consisting of bridge priority plus MAC address. Only the MAC is displayed in HEX.
Actual Root Port ID	Actual Root Port of this switch. This is the index of the port on this switch that is closest to the root. This switch communicates with the root device through this port. This is 0X0000 if your bridge is the root device.

FIELD	Description
Actual Root Path Cost	This is the cost for a packet to travel to the root in the current Spanning Tree configuration. The slower the media, the higher the cost. This is 0 if your bridge is the root device.
Actual Max Age	This is the maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. Value derived from the Root port.
Actual Hello Time	This is the time interval (in seconds) at which the root device (for STP) or any devices (for RSTP) transmit a configuration message. Value derived from the Root port.
Actual Forward Delay	This is the time (in seconds) a device will wait before changing states. Value derived from the Root port.

6 Modem Profiles Management Model

During the ML700 HSL Calibration (on page 4-21) process, the HSL is calibrated according to user selected, predefined profile templates. A number of factory configured templates are available, where the user can choose from these templates during the HSL calibration. The user selects the templates according to the site conditions and used technology. However, the advanced user may want to further customize the default templates or create new templates. This chapter provides detailed descriptions of these procedures for the advanced user.

DMT based systems, such as ML700, use customized *Modem Profiles* as specified in BBF TR-165 and TR-252, to set all modem operation parameters as specified in ITU-T G.997.1 standards. These include setting the range of data rates according to required SLAs, optimizing modem operation by for the specific infrastructure by adjusting and varying the SNR over specific frequencies to counter the effect of specific types of interference signals.

ML700 supports ADSL2, ADSL2 Plus and VDSL2 technologies. The modem profile customization criteria considers the DSL technology relevant for the site and standards for the region in which the site is located.

In This Chapter

xDSL Background

Digital Subscriber Line (DSL) technology makes use of existing twisted-pair telephone lines to transport high-bandwidth data, such as multimedia and video, to service subscribers over an existing infrastructure. The term xDSL covers a range of technologies. ADSL and VDSL services are dedicated, point-to-point, public network access over twisted-pair copper wire on the local loop ("last mile") between a network service provider's (NSP's) central office and the customer site, or on local loops creating either intra-building or intra-campus.

The table below details the different types of xDSL supported by Actelis network equipment:

Table 22: xDSL Technology Types

ADSL 2 (ITU G.992.3)	• Asymmetric - (usually) higher downstream bandwidth than upstream bandwidth • Data rates depend on a number of factors, including the length of the copper line, its wire gauge, presence of bridged taps, and cross-coupled interference. • Line attenuation increases with line length and frequency and decreases as wire diameter increases.
ADSL2+ (ITU G.992.5)	• Doubles the PSD bandwidth (of ADSL2) used for downstream data transmission. In best case scenario (short loops), may double the maximum downstream data rates. • ADSL2+ includes all the feature and performance benefits of ADSL2, in addition to ADSL2 it supports DPBO, PSD masking and RFI bands.
VDSL2 (Very-high-speed digital subscriber line 2)	• Standardized under ITU-T G.992.3 recommendation. This is the newest and most advanced standard of DSL broadband wireline communications. • Designed to support the wide deployment of triple play services such as voice, video, data, high definition television (HDTV) and interactive gaming. • Allows operators and carriers to gradually, flexibly, and cost-efficiently upgrade an existing xDSL infrastructure. • Supports data rates of up to 100DS/50US Mbps using bandwidth of up to 17MHz.

Profile Configuration Workspace

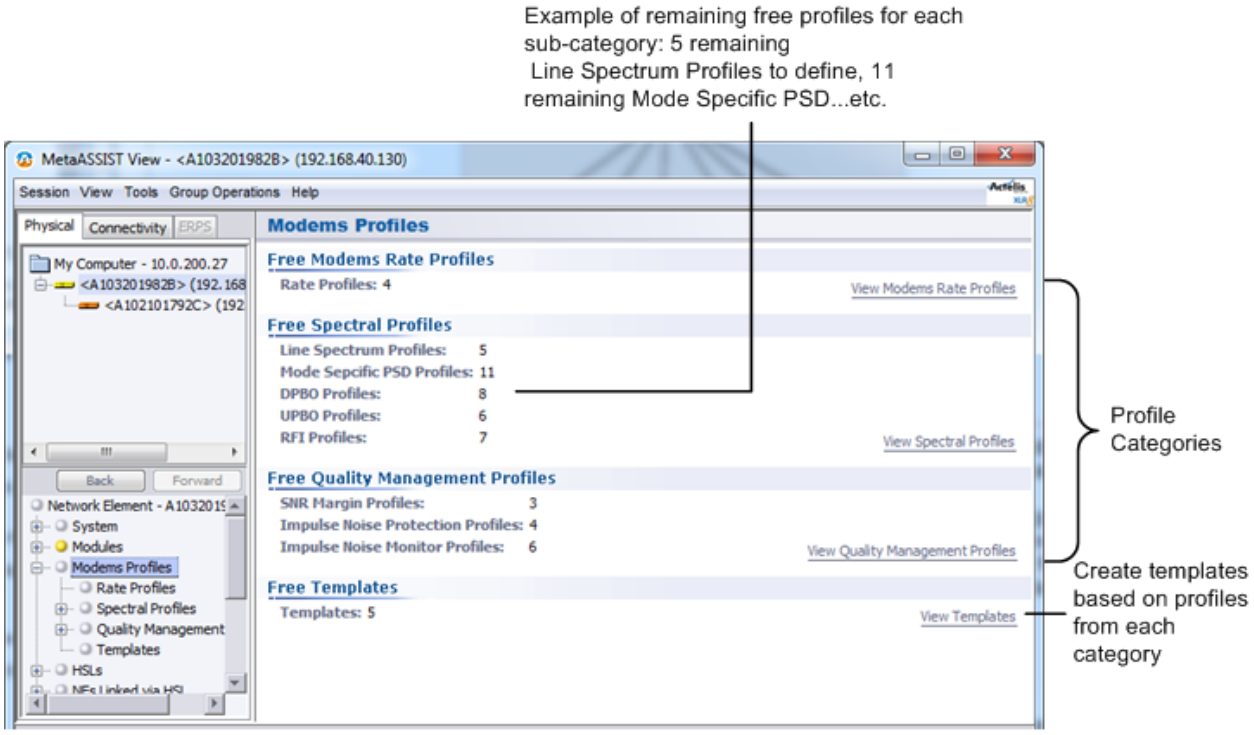
The Modem Profile templates consist of three categories of profiles:

- Rate related profiles - used to configure the upstream and downstream data rate that will be required for various services.
- Spectral Profiles - used to configure the line upstream and downstream power spectral density according to regional requirements and required DSL operation modes.
- Quality Management Profiles - used to configure the SNR settings, the Impulse Noise Protection and monitoring options to identify Impulse Noises.

➢ To access the Modem Profiles configuration options

1. Click **Modem Profiles** in the **Network Elements** tree.
2. Under **Modem Profiles** (and in the displayed pane), four groups of items are displayed: three types of modem profile categories (as detailed above) and **Templates,** where templates based on profiles selected from the pool are created.

   For each category, the number of profiles that may be configured is limited (the number varies according to the sub-category), where a default profile is always predefined. Profiles can be configured by setting each attribute or by uploading a predefined profile and modifying any required parameters and the number of remaining (*free)* for definitions is indicated.



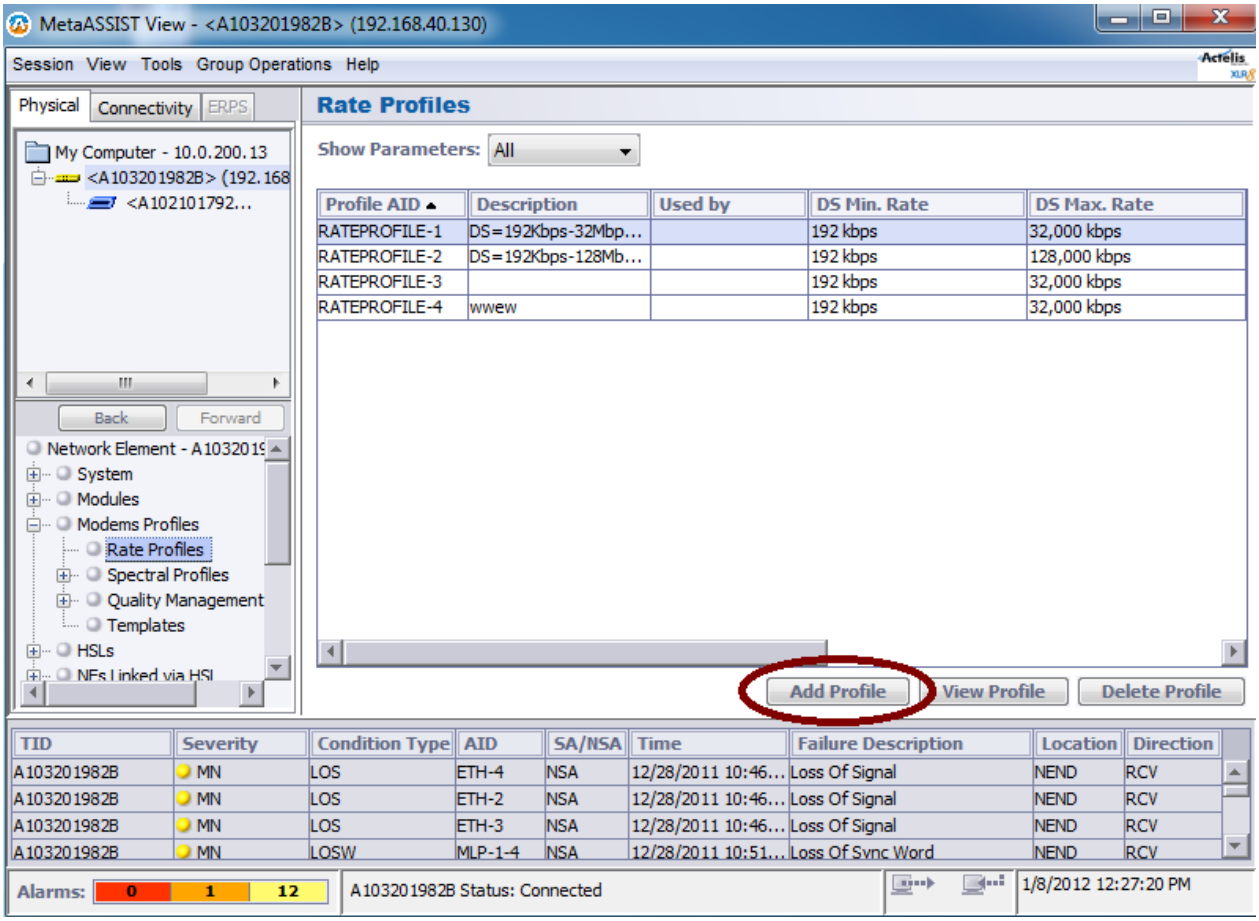
Rate Profiles

Rate Profiles are service related profiles that define modem's data rates. A dedicated data rate profile can be defined for the upstream and for the downstream channel.

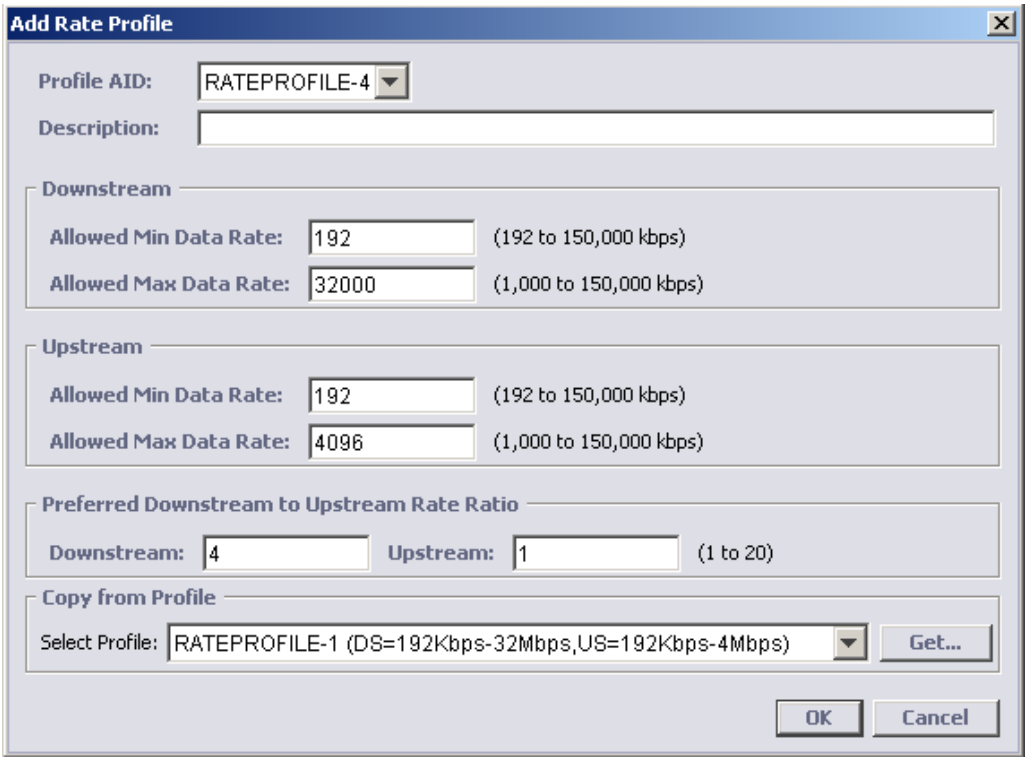
➢ To configure a Rate Profile

1. In the **Network Elements** tree, under **Modem Profiles,** select **Rate Profiles.** The available profiles are displayed in a tabular format. Each profile is displayed along with identifying information for the upstream (US) and downstream (DS) such as data rate range (Min and Max) and ratio.

NOTE: Use the Scroll bar to view more parameters and the **Add/View/Delete Profile** buttons to add a new profile or edit any of the listed defined profiles.



2. In the displayed pane, click **Add Profile.** The Add Rate profile definition dialog appears.



3. Under **Profile AID**, choose from the available AIDs (RATEPROFILE-x). After the profile is defined, it will no longer be available on the *available profile* list; however, it is modifiable from the Rate Profiles glance pane (shown under Step-1 above) using the **Edit** button.
4. In the **Description** field, enter an identifiable description of the profile such as the DS and US values (e.g. DS=64Kbps-32Mbps, US=32Kbps-4Mbps). This description will be very helpful when viewing profile lists.
5. You may either define all the remaining parameters or use the **Select Profile** field (under **Copy from Profile** at the bottom of the pane) to choose an existing profile that is very close to your needs and then modify the parameters. (If a description has not been entered, only the Profile AID will be displayed).

   To load the requested profile parameters, click **Get.**
6. Modify any of the parameters according to the descriptions below and click **OK.**

Table 23: Rate Profiles Parameter Descriptions

Parameter	Description
Profile AID	Lists the available (free) profile AIDs. Defined AIDs are not listed. They are available under Copy from Profile for reference or as templates.
Description	Assign a recognizable description. It will be displayed along with the saved profiles list under Select Profile (see above illustration).

Downstream/Upstream	Define the minimum and maximum values from the available range. Minimum Data Rate - Minimal rate of data (per bearer channel), below this rate the modem is considered as failed. The minimum-bitrate parameter specifies the fixed-rate component of the service. This could be used to ensure that sufficient bandwidth is available for minimum SLA and any traffic engineered service (i.e. VoIP or IPTV) that requires a fixed bandwidth allocation. The *Maximum Rate* parameter is set to the total bandwidth required for traffic engineered services in addition to best-effort services such as Internet Access. Allowed Maximum Data Rate Downstream/Upstream – specifies maximal data rate (cannot be exceeded). **Data Rate = Line Rate - Data Protection & EOC Overhead** *NOTE: Maximum Rate is used as the required rate in case that "Force Rate" is selected in SNR Margin Profile (see SNR Margin (on page 6-24)).*
Preferred Downstream to Upstream Rate Ratio	DS to US preferred ratio objective. The DS/US Ratio may have impact on modem's final DS and US rates in very short loops and in Interleaved or Retransmission modes. The Preferred Ratio may impact modem's rate in these cases since modem's rates are limited by internal resources limitations and not by link's capacity (e.g. modem's memory cannot serve all possible BW). Parameter default is 4:1 (objective for DS rate four times larger than US rate).

Spectral Profiles

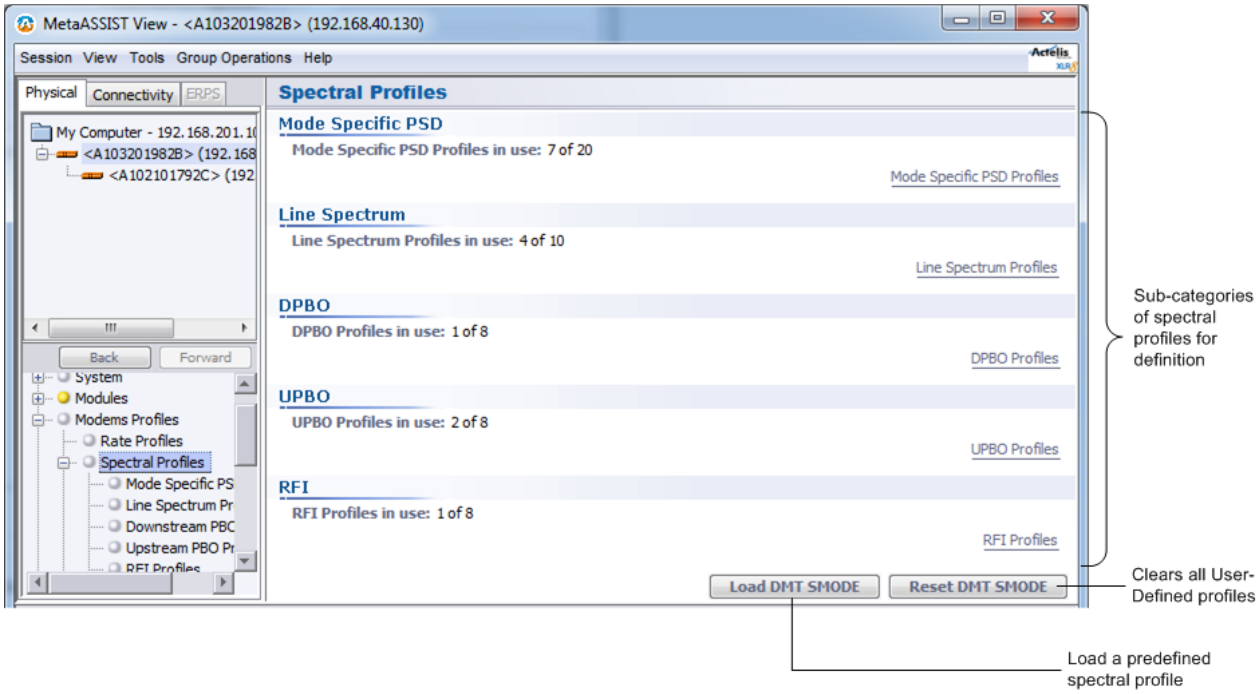
The Spectral Profile enables you to define the power spectrum according to the xDSL supported on your site, your region's spectrum requirements and the quality of your line. You may define spectrum profiles by either:

- **Loading a predefined spectral profile** (on page 6-8) or
- Configuring the spectral files

NOTE: You may also **reset all spectral files definitions.** (on page 6-9)

➢ **To configure a Spectral Profile**

1. In the **Network Elements** tree, under **Modem Profiles,** select **Spectral Profiles.**



2. For each type of Profile, the number of available profiles to define, out of the maximum available, is specified.
3. To configure the Spectral Profiles, several Profile groups are available, allowing a range of customization levels:

Table 24: Spectral Profile Glance View

Mode Specific PSD	Define the Power Spectral Density profiles per mode: ADSL2, ADSL2 Plus or VDSL2, where the relevant parameters and Annexes are available according to the selected mode.
Line Spectrum	Define single or multiple allowed transmission modes. Each of the transmission modes is combined with the selected Mode Specific PSD profile.

DPBO*	Downstream Power Backoff profile. Used to reduce downstream interference for long ADSL lines (originated at the exchange) in case of unit installation at remote cabinets. DPBO is applicable only for ADSL2+ and VDSL2 transmission modes.
UPBO*	Upstream Power Backoff profile. Used to reduce upstream interference of near CPE units to far CPE units. UPBO is applicable only for VDSL2 transmission mode.
RFI*	Radio Frequency Interference - Used to suppress interference from RFI sources (e.g. radio stations).

*Optional profile used to fine tune the Line Spectrum Profile.

Loading Predefined Spectral Profiles

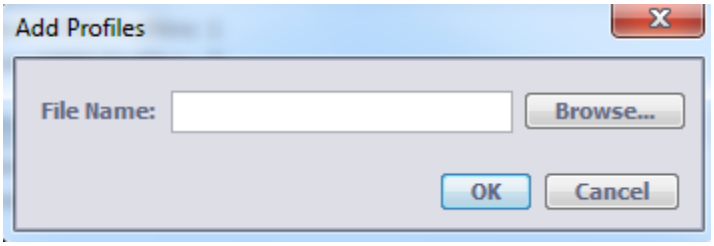
MetaASSIST View installation is provided with pre-defined, default, spectral attributes organized in a set of CSV files. These files are located in the Installation directory, under "DMT-SMODE". Instead of defining the individual spectral profiles, you can load a predefined file.

➢ **To load a predefined spectral attributes file**

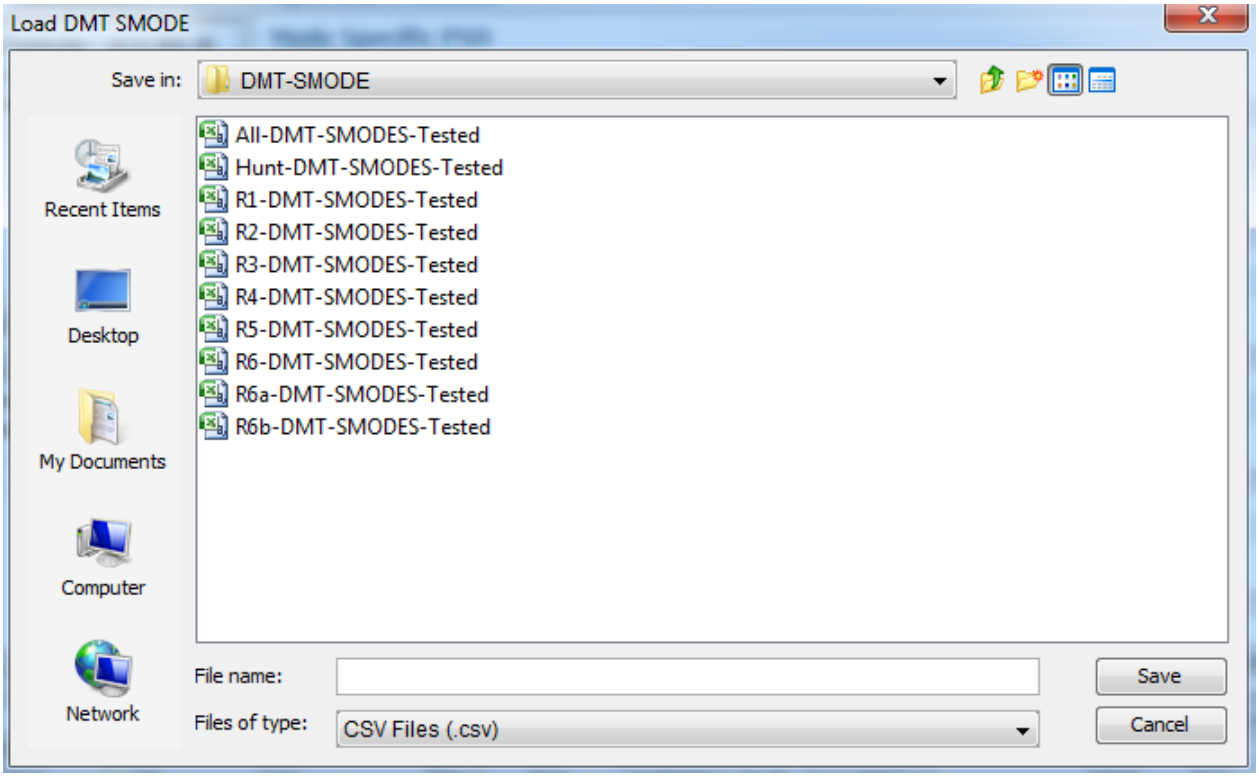
1. In the **Network Elements** tree, under **Modem Profiles,** select **Spectral Profiles.**

NOTE: Use the **Add/View/Delete Profile** buttons to define and manage the profiles.

2. Click the **Load DMT-SMODE**. The following dialog appears.



3. Click **Browse.** The available files are displayed (see the example below). Contact Actelis Networks customer support at techsupport@actelis.com for details on the appropriate SMODE for the region.



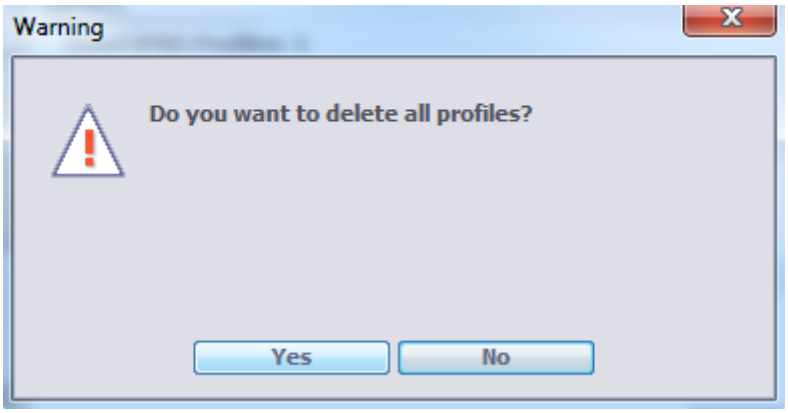
4. Select the desired file, click **Save** and **OK**.

Resetting All Spectral File Definitions

NOTE: It is recommended you back-up the profile settings before you reset the definitions.

➢ **To delete all spectral file definitions**

1. In the **Network Elements** tree, under **Modem Profiles,** select **Spectral Profiles.**
2. Click the **Reset DMT-SMODE** button at the bottom of the pane. The following dialog appears.



3. Click **Yes** to delete all definitions.

Mode Specific Power Spectral Density Profile

This dialog is used to create a pool of PSD (Power Spectral Density) profiles according to the transmission Mode ADSL2+, VDSL), region, existing underlying infrastructure (i.e. ISDN, POTS), specific upstream mask required of a site and other criteria relevant to the site conditions.

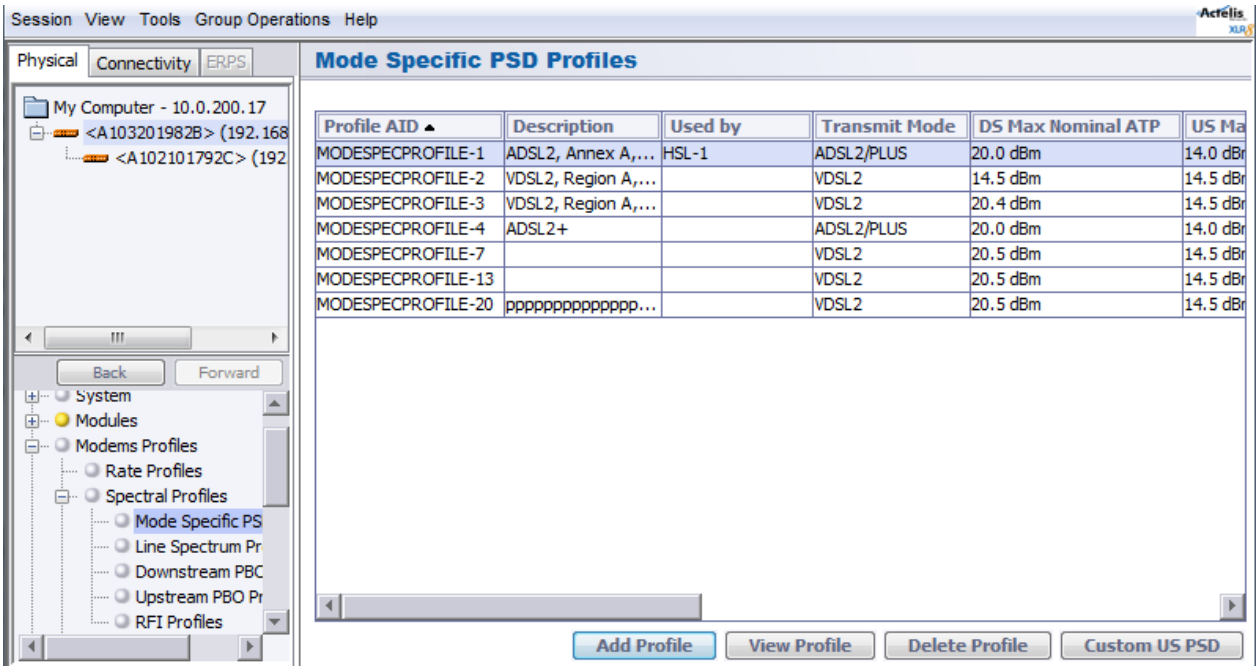
The PSD profiles are used when configuring the **Line Spectrum Profiles** (on page 6-14). Each Mode Specific PSD Profile is associated with a specific Line Spectrum Profile. When the vector of profiles refers to a Line Spectrum Profile it also implicitly refers to all Mode Specific PSD Profiles associated with it. Each transmission mode enabled in a Line Spectrum Profile is covered by one and only one of the Mode Specific PSD Profiles contained in that Line Spectrum Profile.

NOTE: Instead of defining each profile, you can download an existing file to use as a reference, customize to your needs by making the desired changes and save under another name.

➢ To configure the Mode Specific Spectral Density Profile

1. In the **Network Elements** tree, under **Modem Profiles** and under **Spectral Profiles**, select **Mode Specific PSD Profiles.** The defined profiles are listed in the pane according to their user assigned description and characteristics.

NOTE: Use the **Add/View/Delete Profile** buttons to define and manage the profiles.



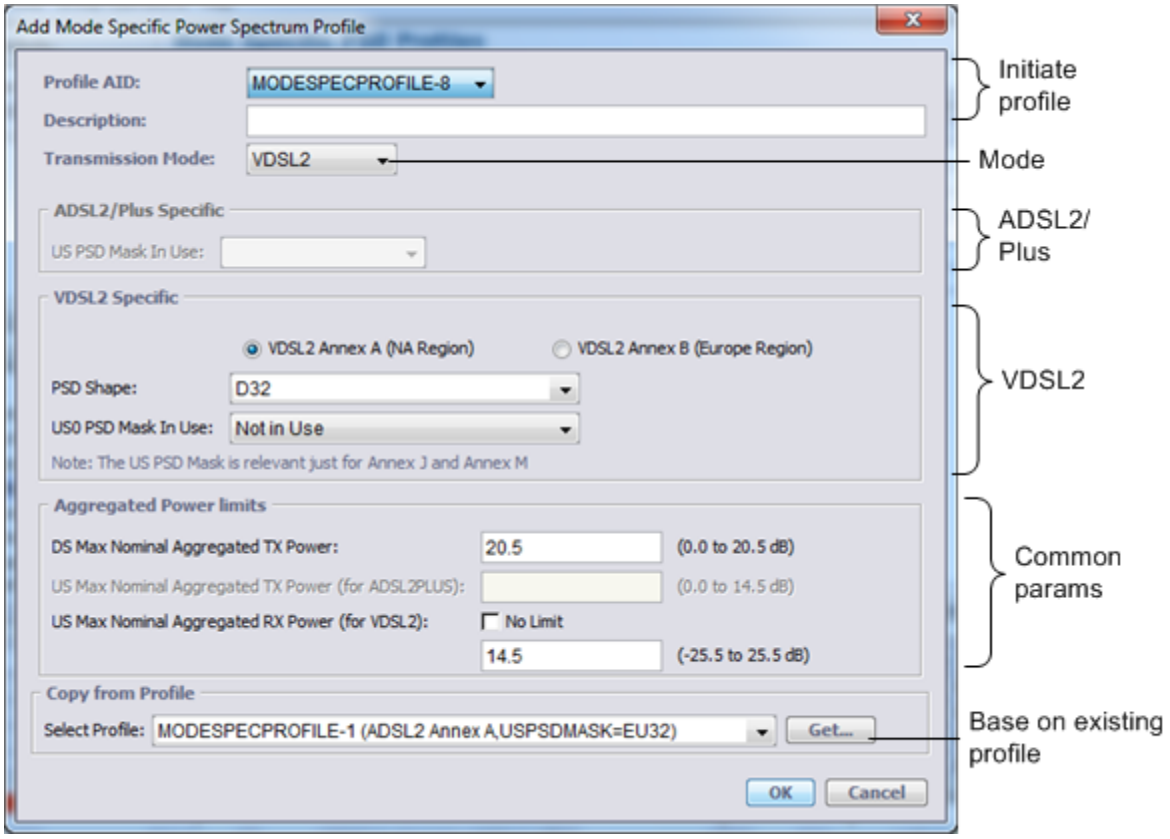
The **Custom US PSD** is used to customize the Upstream PSD Mask according to specific requirements. To do so:

- Define **at least Two** Sub-carrier frequencies.
- Define the corresponding PSD Mask values.

NOTE: Custom US PSD Masks may be applied *only* to profiles set to VDSL2 transmission mode.

2. Click **Add Profile.** The Power Spectral Density Profile definition dialog appears.

   The dialog supports ADSL2/Plus and VDSL2 parameters. As the Transmission mode is selected (or the template profile is loaded using **Select Profile)**, the relevant parameters become available.



3. Configure Mode Specific PSD Profiles according to the following table and click **OK** to save. The new profile will be listed in the **Mode Specific** glance pane. It will also be removed from the list of available profile AIDs and added to the available profiles for use as templates under the **Copy from Profile** option.

Table 25: Configuring Mode Specific PSD Profiles

To....	Do this....
Initiate a new profile:	• Choose from the available **Profile AIDs**. • Assign the profile an identifiable **Description** (i.e. ADSL2 Plus...) • Do one of the following: either upload values from an existing file and modify them according to the following step, or define each parameter as described in the next steps.
Copy values from an existing profile:	• Under **Copy from Profile** (bottom of the pane), choose from the list of predefined profiles. • Click **Get.** The parameters will be updated. • Modify the required parameters to customize them to your needs. • Click **OK.** The new profile will be added to the Mode Specific Profile pane.
Define the mode specific **ADSL2/Plus** parameters:	Under **Transmission Mode,** select ADSL2/Plus. The relevant fields will be available. Define the (Upstream) **US PSD Mask In Use** by choosing the relevant Annex options.
Define the mode specific **VDSL2** parameters:	Under **Transmission Mode,** select **VDSL2**. The relevant fields will be available. Select the regional band-plan annex and the relevant PSD parameters. The annex specifies the PSD Mask for numerous regional bandplans and are designed to provide coexistence with other services: • **Annex A/B:** ▪ Annex A- specifies band-plans for the North American region and enables VDSL2 to be deployed with traditional POTS telephony or in an all-digital mode (similar to Annex J in ADSL2). ▪ Annex B - specifies band-plans for Europe and enables VDSL2 deployment with POTS, ISDN or all digital compliant PSD. • Select the **PSD Shape** and if US0, first band, is used (**US0 PSD Mask in Use),** select the PSD for that band. • Select the profile according to your regional deployment architecture (e.g. country, CO unit location)
Define the **Aggregated Power Limits:**	Define the relevant Maximum Nominal Aggregated Tx and Rx power limits.

Line Spectrum Profiles

The Line Spectrum Profile sets the allowed transmission modes and their corresponding Mode Specific profiles.

The Line Spectrum Profile configuration simultaneously supports Line Spectrum attributes for VDSL2, ADSL2 and ADSL2 Plus. This dialog enables selecting any combination of the technologies, as well as profile subsets; e.g. VDSL2 Annex A, 8b, 12a and 17a. The system will try to sync in one of the technologies according to user (predefined) priority as follows: VDSL2 -> ADSL2Plus -> ADSL2

NOTE: Multiple technology selection may prolong system calibration time.

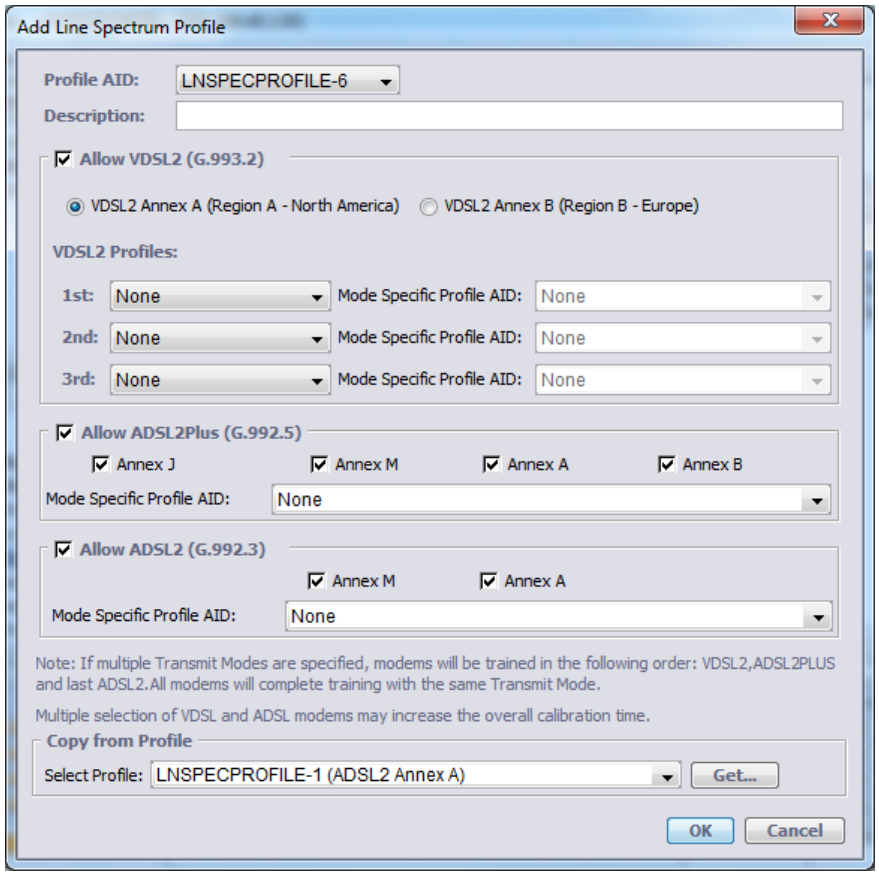
➢ To create a Line Spectrum Profile

1. In the **Network Element** tree, under **Modem Profiles** and under **Spectral Profiles**, select **Line Spectrum Profiles.** The defined profiles are listed in the pane according to their user assigned description and characteristics.

   NOTE: Use the **Add/View/Delete Profile** buttons to define and manage the profiles.

2. In the displayed pane, click **Add Profile.** The Line Spectrum profile definition dialog appears.

   Note that a wide range of Line Spectrum attributes are supported.



3. Configure Line Spectrum Profiles according to the following table and click **OK** to save. The new profile will be listed in the glance pane. It will also be removed from the list of available profile AIDs and added to the available profile for use as templates under the Copy from Profile option.

Table 26: Configuring Line Spectrum Profiles

To....	Do this....
Initiate a new profile:	• Choose from the available **Profile AIDs**. • Assign the profile an identifiable **Description** (i.e. ADSL2 Plus...) • Do one of the following: either upload values from an existing file and modify them according to the following step, or define each parameter as described in the next steps.
Copy values from an existing profile	• Under **Copy from Profile** (bottom of the pane), choose from the list of predefined profiles. • Click **Get.** The parameters will be updated. • Modify the required parameters to customize them to your needs. • Click **OK.** The new profile will be added to the Line Spectrum Profile pane.
Define **VDSL2** parameters	• Enable the **Allow VDSL2** check box • Select **Annex A** or **Annex B** according to your region (Europe or North America). • Select up to three VDSL2 options (priority ranked), each option with its profile (e.g. 8b, 12a, 17a) and the corresponding Mode Specific Profile.
Define **ADSL2/Plus** parameters	• Enable **Allow ADSL2Plus** and/or **ADSL2** check box • Under **Transmission Mode**, select **ADSL2** or **ADSL2Plus**. The relevant fields will be available. • Define allowed annexes (e.g. Annex J, annex M), multiple selection is allowed. In case of multiple annexes selection the Annexes have predefined priority left to right. For example, in case of ADSL2Plus: Annex J, then Annex M, Annex A and Annex B.

Downstream PBO Profiles

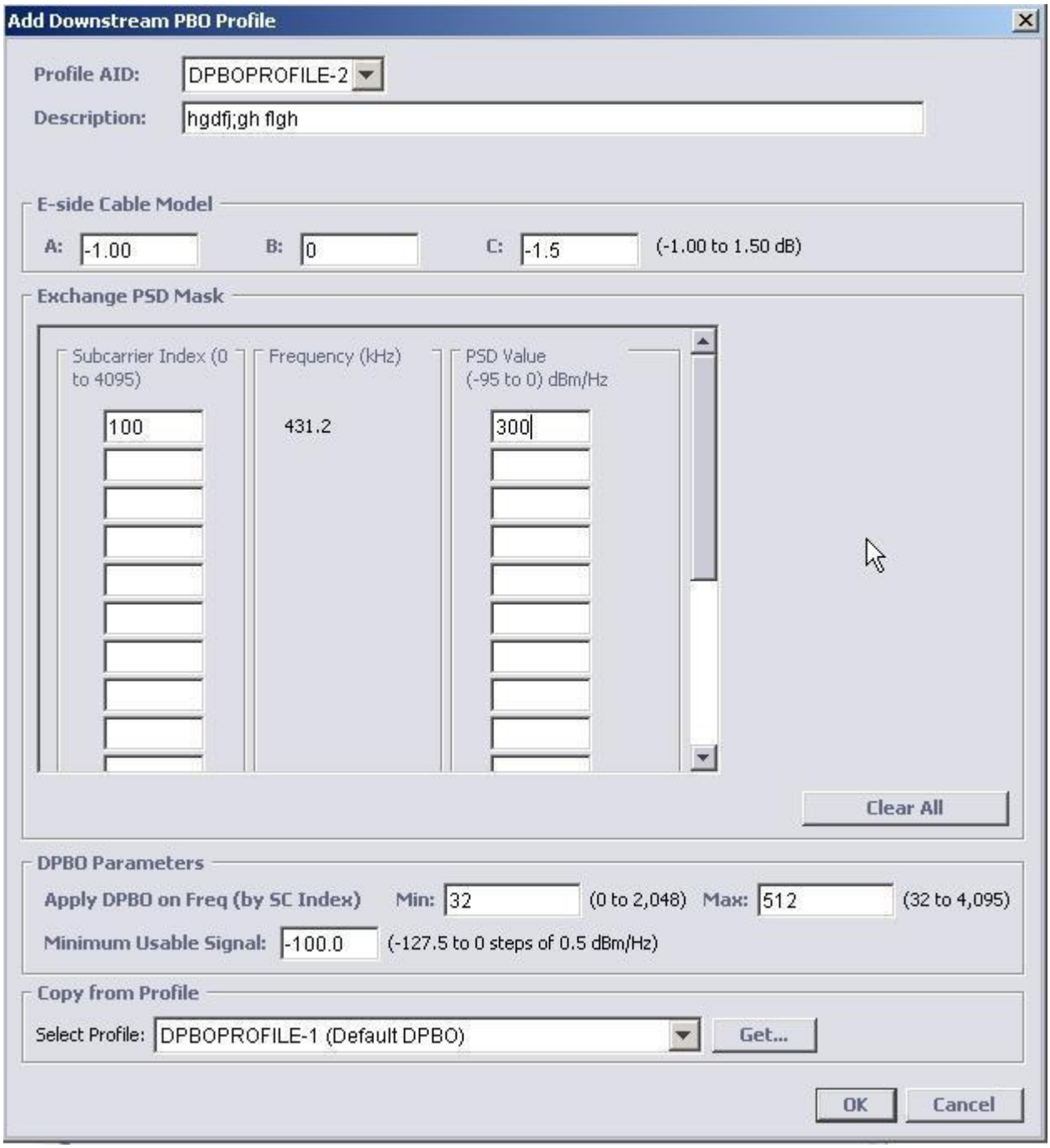
DPBO is required to minimize the cross-talk to adjacent services in case that the CO unit is not installed at the exchange (e.g. at outdoor cabinets). DPBO affects the transmission PSD from CO unit in order to guarantee spectral compatibility. DPBO is supported only in ADSL2plus and VDSL2 transmission modes. In this profile, the line configuration parameters must be set to generate a modified downstream PSD mask for Downstream Power Back-off.

➢ To generate a DPBO Profile

1. In the **Network Element** tree, under **Modem Profiles** and under **Spectral Profiles**, select **Downstream PBO.** The defined profiles are listed in the pane according to their user assigned description and characteristics.

   NOTE: Use the **Add/View/Delete Profile** buttons to define and manage the profiles.

2. In the displayed pane, click **Add Profile.** The Downstream PBO profile definition dialog appears.



3. Define the profile according to the following table and click **OK** to save. The new profile will be listed in the glance pane. It will also be removed from the list of available profile AIDs and added to the available profile for use as templates under the Copy from Profile option.

Table 27: Configuring DPBO Profiles

To....	Do this....
Initiate a new profile:	• Choose from the available **Profile AIDs**. • Assign the profile an identifiable **Description** (i.e. ADSL2 Plus...) • Do one of the following: either upload values from an existing file and modify them according to the following step, or define each parameter as described in the next steps.
Copy values from an existing profile:	• Under **Copy from Profile** (bottom of the pane), choose from the list of predefined profiles. • Click **Get.** The parameters will be copied. • Modify the required parameters to customize them to your needs. • Click **OK.** The new profile will be added to the DS PBO Profile pane.
	• **E-side Cable Model** - define the line between the Exchange and the cabinet (where ML700-C is installed): ESCM**A**, ESCM**B**, ESCM**C** - These parameters, defined in G.997.1, are used in a formula that describes the frequency dependent loss of signal on the cable between the Exchange and the cabinet. Range: 1 to 1.5. **Exchange PSD Mask -** enter the Exchange PSD Mask by up to 16 breakpoints, each breakpoint with: ▪ Carrier Index – Range 0 to 4096 ▪ PSD (dBm/Hz) – Range 0 to -127.5 ▪ Frequency (KHz) - will appear once ranges of the above parameters are set.
Define the frequencies in which DPBO will be applied:	Define the area in which DPBO will be applied: • FMIN - Defines the minimum frequency from which DPBO will be applied. • FMAX - Defines the maximum frequency at which DPBO will be applied. • Minimum Usable Signal - Defines the assumed Minimum Usable receive PSD, that is, the signal level under which the CPE modem will not be able to decipher information. The range is -127.5dBm/Hz to 0dBm/Hz. In frequency bands that the assumed received PSD (of the victim) is too low DPBO is not provided.

Upstream PBO Profiles

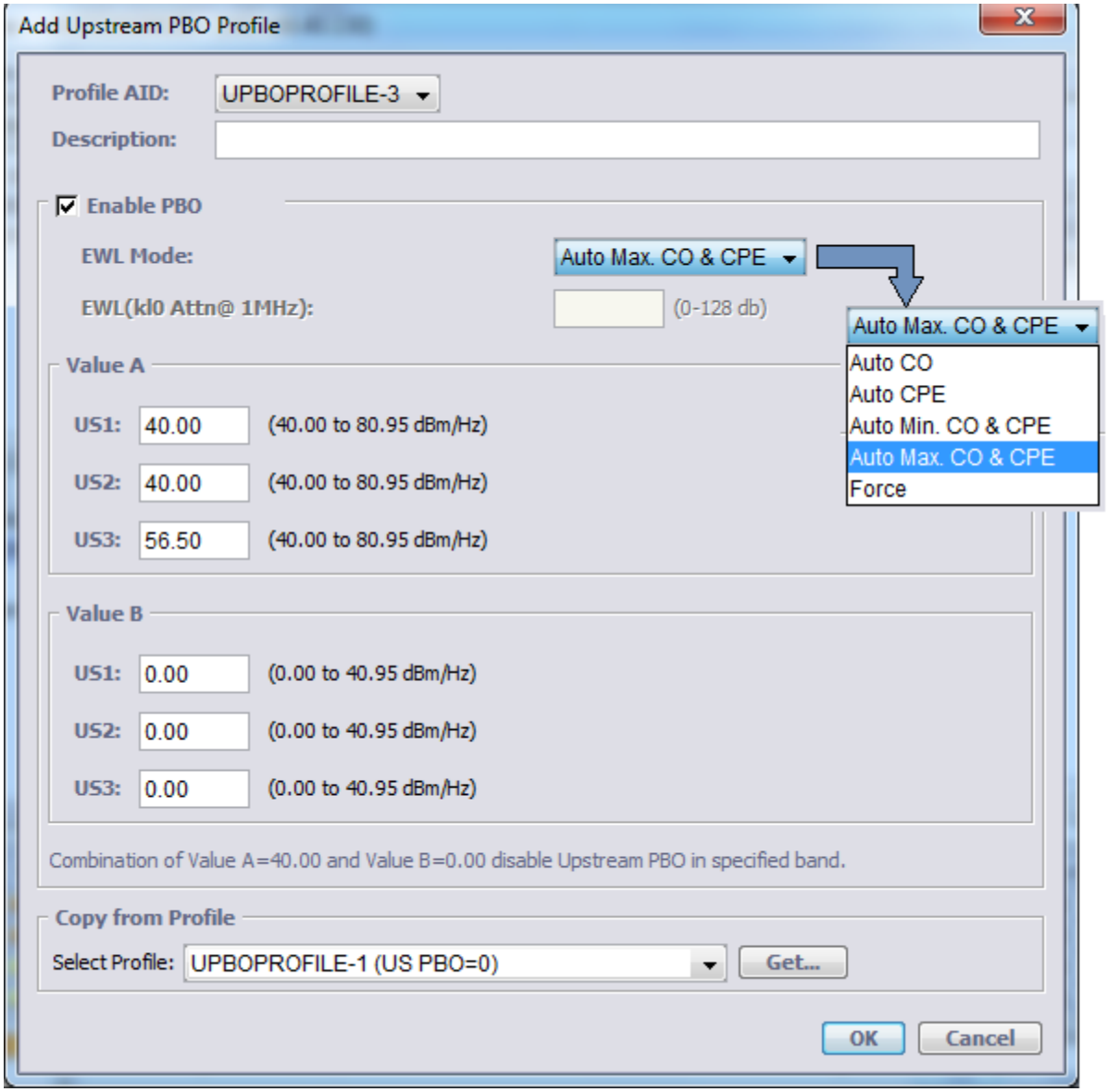
The Upstream PBO profile is used to generate a modified upstream PSD mask for Upstream Power Back-off in order to limit the cross-talk in case of Near-Far topology (i.e. close and far CPE units). It is defined according to Electrical Working Length (EWL) and cable specifications. You may define up to eight Upstream PBO (Power Backoff) profiles. UPBO is used only by VDSL2 transmission mode. US0 is not altered by UPBO, just the upper US band are shaped.

➢ To create an Upstream PBO Profile

1. In the **Network Element** tree, under **Modem Profiles** and under **Spectral Profiles**, select **Upstream PBO**. The defined profiles are listed in the pane according to their user assigned description and characteristics.

NOTE: Use the **Add/View/Delete Profile** buttons to define and manage the profiles.

2. In the displayed pane, click **Add Profile.** The Upstream profile definition dialog appears:



3. Define the profile according to the following table descriptions. Click **OK** to save. The new profile will be listed in the glance pane. It will also be removed from the list of available profile AIDs and added to the available profile for use as templates under the Copy from Profile option.

Table 28: Configuring UPBO Profiles

To....	Do this....
Initiate a new profile:	• Choose from the available **Profile AIDs**. • Assign the profile an identifiable **Description** (i.e. ADSL2 Plus...) • Do one of the following: either upload values from an existing file and modify them according to the following step, or define each parameter as described in the next steps.

Copy values from an existing profile:	• Under **Copy from Profile** (bottom of the pane), choose from the list of predefined profiles. • Click **Get.** The parameters will be updated. • Modify the required parameters to customize them to your needs. • Click **OK.** The new profile will be added to the US PBO Profile pane.
Configure a profile	• Verify that **Enable PBO** is checked-mark.
Set the electrical length that will be used for the calculation of the UPBO PSD mask:	• For manual definitions - under **EWL Mode**, select **Force**. The electrical length (K10) is the attenuation of the signal at 1MHz from the CPE to the cabinet. The range is 0 to 127 dB (0.1 dB steps). • For automatic calculation - choose one of the Auto parameters. The EWL is auto-calculated according to the selected item (CO or CPE, minimum or maximum CO and CPE).
Define two sets of parameters (A and B), for each of the three upstream bands.	Set the Value A and Value B for US1, US2 and US3 fields. A and B values depend on customer's cable specifications and are used by the modem in the US PSD mask calculations. *Note: the combination of 40/0 for A/B parameters disables UPBO in the band.*

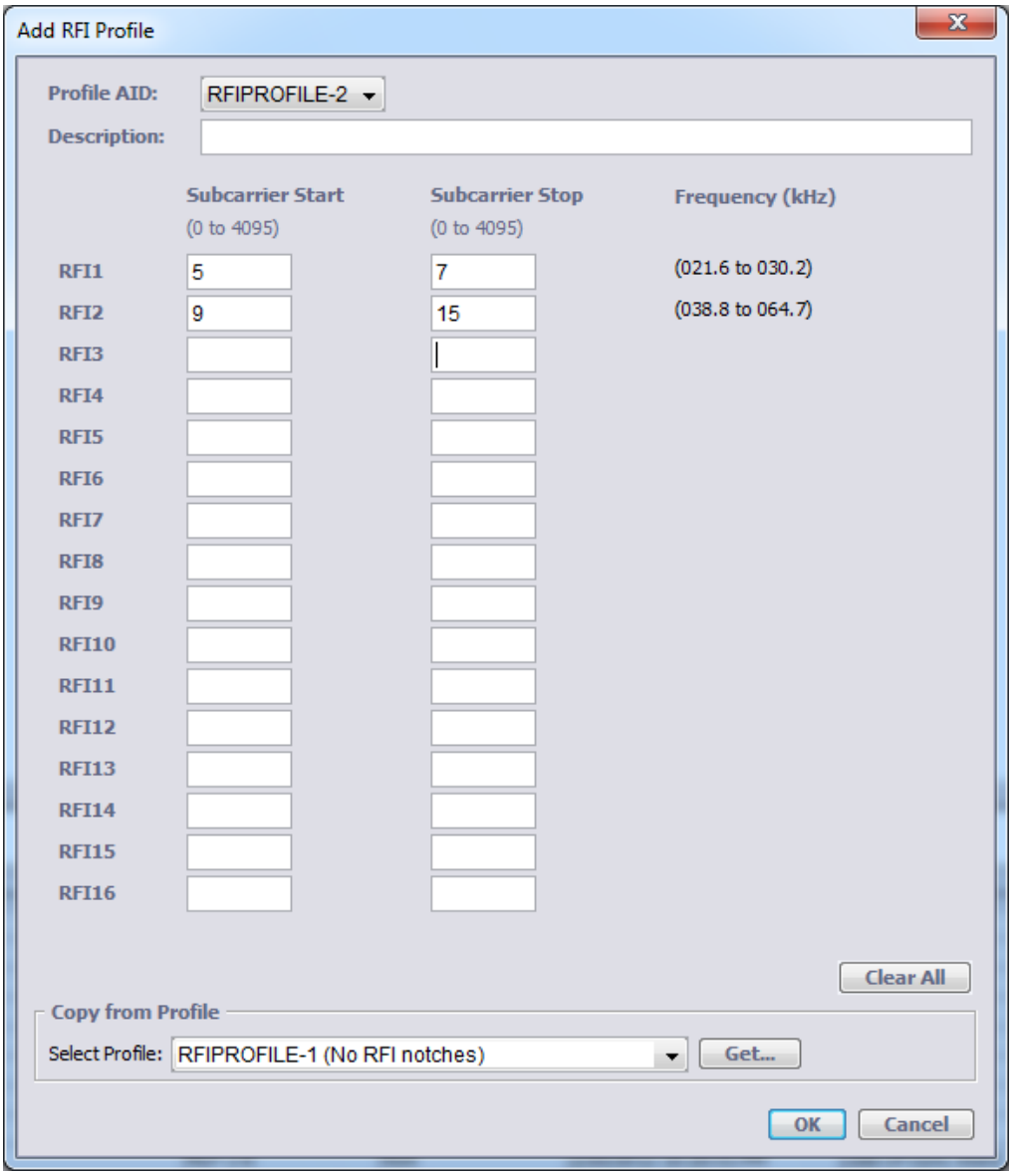
RFI Profiles

RFI Notching is used to suppress RFI (Radio Frequency Interference) disturbers. The used spectrum excludes the interfered spectrum. *RFI notches are necessary only when radio services may disturb during operation.* If RFI notching is desired, up to 16 notches can be defined. Both the start and stop tones must be configured for each notch.

➢ To create an RFI Profile

1. In the **Network Element** tree, under **Modem Profiles** and under **Spectral Profiles**, select **RFI.** The defined profiles are listed in the pane according to their user assigned description and characteristics.

NOTE: Use the **Add/View/Delete Profile** buttons to define and manage the profiles.



2. Define the profile according to the following table descriptions. Click **OK** to save. The new profile will be listed in the glance pane. It will also be removed from the list of available profile AIDs and added to the available profile for use as templates under the Copy from Profile option.

Table 29: Configuring RFI Profiles

To....	Do this....
Initiate a new profile:	• Choose from the available **Profile AIDs**. • Assign the profile an identifiable **Description** (i.e. ADSL2 Plus...) • Do one of the following: either upload values from an existing file and modify them according to the following step, or define each parameter as described in the next steps.

To....	Do this....
Copy values from an existing profile:	• Under **Copy from Profile** (bottom of the pane), choose from the list of predefined profiles. • Click **Get.** The parameters will be updated. • Modify the required parameters to customize them to your needs. • Click **OK.** The new profile will be added to the RFI Profile pane.
Configure a profile	Define up to 16 notches: • Start - Defines Start tone index for the notch. Range: 0 to 4095. • Defines Stop tone index for RFI notch. Range: 0 to 4095. • The corresponding frequency values will automatically be displayed.
To clear all values	• Click **Clear All.**

Quality Management

The Quality Management Profiles determine the required Service Quality options. These include setting the valid Signal to Noise Ration margins, protection from Impulse Noises and criteria for monitoring Impulse Noises.

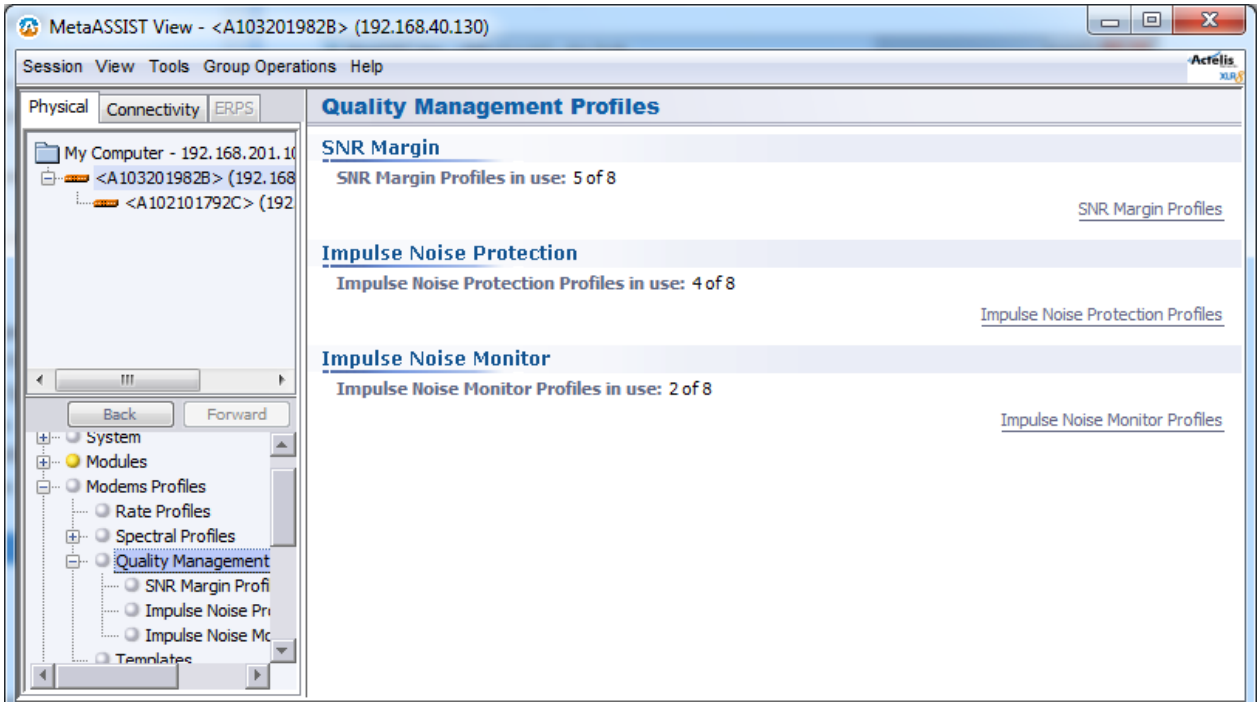


Table 30: Quality Management Profiles

Profile	Description
SNR Margin	Determines the allowed level of Signal to Noise Ratio Margin and the system response if the level is exceeded (i.e. lowering data rates, increasing power, etc.)
Impulse Noise Protection	Determines the type and level of protection from Impulse Noise where several options are available, each with the corresponding configurable parameters (Interleaved, Fast, Retransmission, and more).
Impulse Noise Monitoring	Determines the profile used for the measurement of Impulse Noises via the selection of histogram type and counting method.

SNR Margin

The SNR is defined as the Signal Power to Noise Power ratio. Noise margin is important for line robustness. SNR profile parameters may be adjusted to compensate for varying line conditions and maintain required data rates.

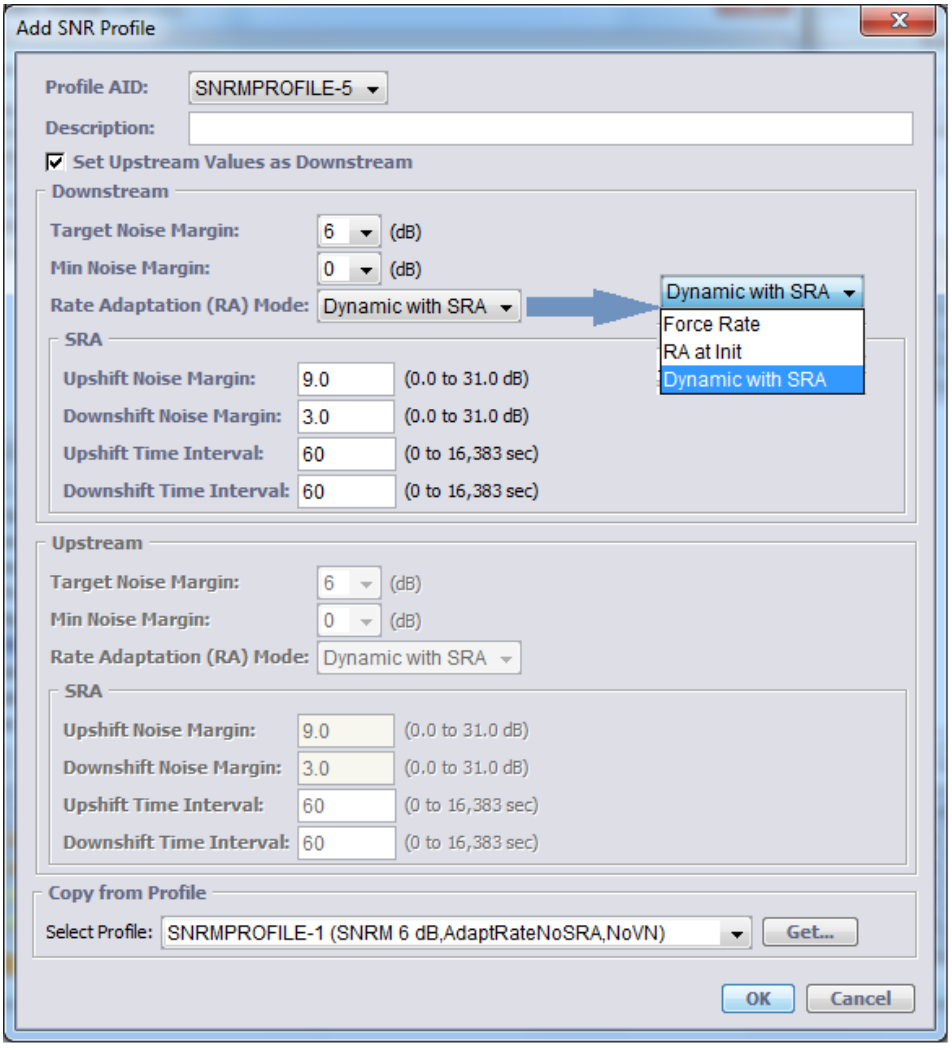
➢ To create an SNR Profile

1. In the **Network Element** tree, under **Modem Profiles** and under **Quality Management** select **SNR Margin Profiles.** The defined profiles are listed in the pane according to their user assigned description and characteristics.

   NOTE: Use the **Add/View/Delete Profile** buttons to define and manage the profiles.

2. In the displayed pane, click **Add Profile.** The Add SNR profile definition dialog appears:

   Note that the dialog is divided into two areas containing the same parameters: Downstream and Upstream. To facilitate the configuration process, you may set the Upstream values to equal the defined Downstream values by checkmarking the options **Set Upstream Values as Downstream** (or define each set of parameters).



3. Define the profile according to the following table descriptions. Click **OK** to save. The new profile will be listed in the glance pane. It will also be removed from the list of available profile AIDs and added to the available profile for use as templates under the Copy from Profile option.

Table 31: Configuring SNR Margin Profiles

To....	Do this....
Initiate a new profile:	• Choose from the available **Profile AIDs**. • Assign the profile an identifiable **Description** (i.e. ADSL2 Plus...) • Do one of the following: either upload values from an existing file and modify them according to the following step, or define each parameter as described in the next steps.
Copy values from an existing profile:	• Under **Copy from Profile** (bottom of the pane), choose from the list of predefined profiles. • Click **Get.** The parameters will be updated. • Modify the required parameters to customize them to your needs. • Click **OK.** The new profile will be added to the SNR Profile pane.
Set the US = DS	• Checkmark **Set Upstream Values as Downstream** if US & DS settings are identical.
Set the general parameters	**Target Noise Margin** - The required Noise Margin that the modem must achieve during activation (the margin is calculated from the SNR that provides BER of 10-7). *Note: during multi-pair activation (bonded link) the final SNR margin (once the calibration process has finished) may slightly differ from the configured Target SNR Margin.* **Minimum Noise Margin** - minimum Noise Margin that the modem will tolerate. If the noise margin falls below this level, the modem should attempt to increase its power output. If that is not possible, the modem will attempt to re-initialize. **Rate Adaptation Mode** This parameter defines the modem's behavior during initialization and during show time towards noise changes. Three Rate Adaptation Modes are supported: • **Force Rate** - Modem is "forced to initialize at the Maximum rate defined in the Rate Profile (see **Data Rate Profile configuration** (on page 6-4)). The modem fails initialization if the Target SNR Margin cannot be supported at the required rate. • **RA at Init** - Modem is initialized with data rate between the Minimum Maximum data rate that satisfies the Target SNR Margin. The Modem fails initialization if the target SNR margin cannot be supported by the minimal required rate (the required rate cannot be maintained). Data rate is automatically selected at startup only and does not change after that. • **Dynamic with SRA** - Rate is automatically selected at init (as in the case of RA at Init) and is continuously adapted during operation. Rate Adaptation is performed when the conditions specified for Upshift Noise Margin and Upshift Interval - or for Downshift Noise Margin and Downshift Interval - are satisfied. Rate Upshift (or Downshift) occurs when the noise margin is above Upshift (or below downshift) Noise Margin threshold for a period longer than Minimum Time Interval for Upshift (or downshift).

SRA Parameters	Relevant if the Rate Adaptation Mode was set to **Dynamic with SRA.** • Upshift Noise Margin - Noise Margin threshold for Upshift (rate increase). • Downshift Noise Margin - Noise Margin threshold for Downshift (rate decrease). • Upshift Time Interval- Defines the interval of time the Noise Margin should stay above the Upshift Noise Margin before the modem will attempt to increase data rate. • Downshift Time Interval -This parameter defines the interval of time the Noise Margin should stay below the Downshift Noise Margin before the modem will attempt to decrease data rate.

Impulse Noise Protection

Impulse noise is a burst of energy spikes with random amplitudes, spectral and inter-arrival time. Impulse Noise can be introduced in the loop either by man-made or natural electromagnetic events, e.g. communication equipment, electrical appliances, lightning discharges etc. Due to its non-stationary nature, impulse noise does not lend itself easily to a statistical description. Impulse noise can be caused by various electronic devices, both inside and outside the network and it can cause network errors. Actelis provides several INP (Impulse Noise Protection) modes to reduce the number of errors that are caused by impulse noise: interleaving, retransmission, fast or fast with delay.

The selected **INP Mode** can be common to both upstream and downstream or can be individually set for each direction.

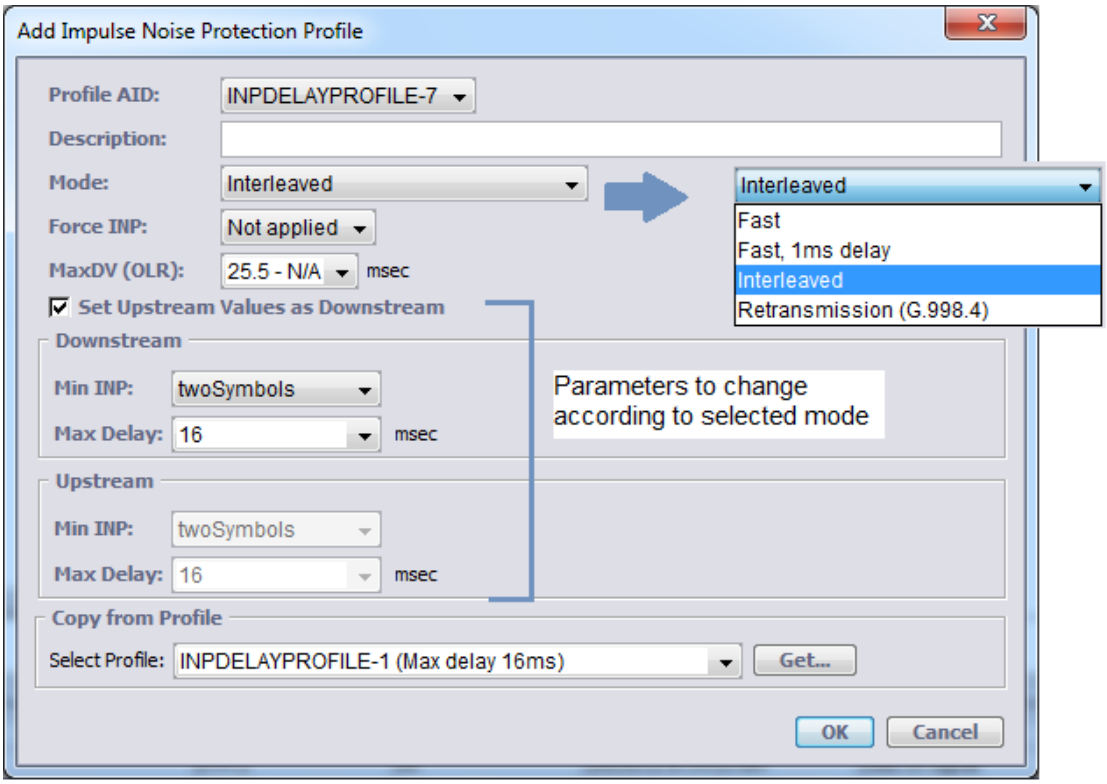
➢ To create an Impulse Noise Protection Profile

1. In the **Network Element** tree, under **Modem Profiles** and under **Quality Management,** select **Impulse Noise Protection.** The defined profiles are listed in the pane according to their user assigned description and characteristics.

   NOTE: Use the **Add/View/Delete Profile** buttons to define and manage the profiles.

2. In the displayed pane, click **Add Profile.** The Impulse Noise Protection profile definition dialog appears:

Note that the dialog is divided into two areas with the same parameters: Downstream and Upstream. To facilitate the configuration process, you may set the Upstream values to equal the defined Downstream values by check marking the options **Set Upstream Values as Downstream.**



3. Define the profile according to the following table descriptions. Click **OK** to save. The new profile will be listed in the glance pane. It will also be removed from the list of available profile AIDs and added to the available profile for use as templates under the Copy from Profile option.

Table 32: Configuring INP Profiles

To....	Do this....
Initiate a new profile:	• Choose from the available **Profile AIDs**. • Assign the profile an identifiable **Description** (i.e. ADSL2 Plus...) • Do one of the following: either upload values from an existing file and modify them according to the following step, or define each parameter as described in the next steps.
Copy values from an existing profile:	• Under **Copy from Profile** (bottom of the pane), choose from the list of predefined profiles. • Click **Get.** The parameters will be updated. • Modify the required parameters to customize them to your needs. • Click **OK.** The new profile will be added to the INP Profile pane.
Set the Upstream Value as Downstream	• Checkmark **Set Upstream Values as Downstream** if US and DS settings are identical.
Set the INP Mode	Select the desired **INP Mode**. The relevant parameters will be enabled.

For **Fast** INP Mode	No interleaving and no Error corrections. Designed for delay sensitive applications such as Voice. • Under **INP Mode**, select **Fast.** No other parameters are required.
For **Fast with 1msec delay** INP Mode	**Fast with 1msec delay -** minimal interleaving and minimal Error corrections with a maximum of 1msec delay. Designed for delay sensitive applications such as Voice. • Under **INP Mode**, select **Fast, 1ms delay.** No other parameters are required.
For **Interleaving** INP Mode	Interleaving provides greater immunity to impulse noise but adds a constant delay. Designed for loss sensitive applications such as IPTV or streaming. The "interleaved" path interleaves the data to optimize error protection in the presence of impulse noise sources that are common to DSL. Under **INP Mode**, select **Interleaved** and define the following parameters: • Force INP - select Applied or Not Applied. If it is enabled (Applied), Min INP is forced; if Not Applied ("relaxed" mode), allows reaching show-time with less than Min INP protection. • MaxDV (OLR) - Maximum Delay Variation in case of On-Line Reconfiguration (rate change during show time). OLR is supported if SRA (Seamless Rate Adaptation) is enabled. • Minimum INP - protection in symbols (0.25ms each symbol). The Min INP parameter defines the minimum number of DMT symbols that will be protected from impulse noise and thus the maximum duration of impulse noise which error correction should be able to recover. To provide maximum error protection, Min INP should be set as high as possible without unduly compromising bit-rates and latency. • Max Delay - used to balance maximum downstream impulse noise protection against transmission delay.
For **Retransmission** INP Mode	Provides robust protection against impulse noise (much stronger than Interleaving). Retransmission, unlike interleaving, may have a large delay variation in case retransmission occurs and thus is not applicable to applications that require low-packet delay variation. Under **INP Mode**, select **Retransmission (G.998.4)** and define the following parameters: • Min INP - see definition under Interleaved. • Max Delay - Maximal allowed delay (by retransmission) • Min Delay - Minimal allowed delay (by retransmission) • Min REIN - Minimum impulse noise protection against REIN (Repetitive Electrical Impulse Noise), counted is symbols

Impulse Noise Monitoring

Impulse Noise Monitoring (INM) is a profile used for the *measurement* of Impulse Noise - it is *not* required for modem operation. The INM assists end-user to understand what the required INP settings are to protect the system from Impulse Noise. The modem monitors the detected impulses and counts them according to the pre-configured INM settings. The INM provides two histograms that are displayed according to user defined parameters.

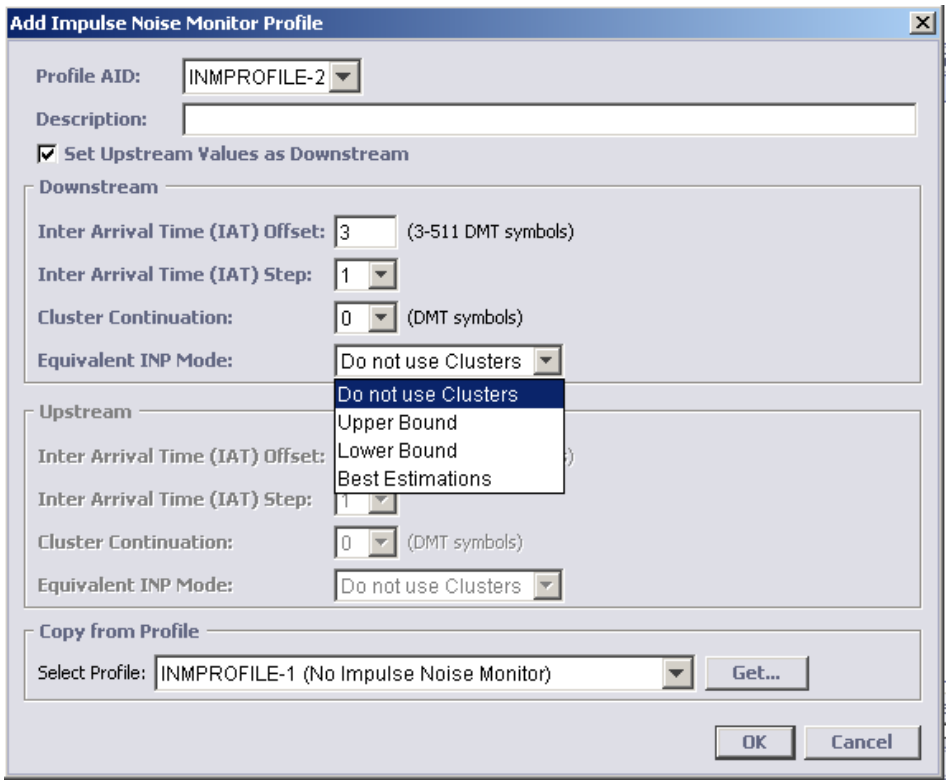
➢ To create an Impulse Noise Monitor Profile

1. In the **Network Element** tree, under **Modem Profiles and under Quality Management,** select **Impulse Noise Monitor Profiles.** The defined profiles are listed in the pane according to their user assigned description and characteristics.

   NOTE: Use the **Add/View/Delete Profile** buttons to define and manage the profiles.

2. In the displayed pane, click **Add Profile.** The Impulse Noise Protection profile definition dialog appears:

   Note that the dialog is divided into two areas with the same parameters: Downstream and Upstream. To facilitate the configuration process, you may set the Upstream values to equal the defined Downstream values by checkmarking the options **Set Upstream Values as Downstream.**



3. Define the profile according to the following table descriptions. Click **OK** to save. The new profile will be listed in the glance pane. It will also be removed from the list of available profile AIDs and added to the available profile for use as templates under the Copy from Profile option.

Table 33: Configuring Impulse Noise Monitoring Profiles

To....	Do this....
Initiate a new profile:	• Choose from the available **Profile AIDs**. • Assign the profile an identifiable **Description** (i.e. ADSL2 Plus...) • Do one of the following: either upload values from an existing file and modify them according to the following step, or define each parameter as described in the next steps.
Copy values from an existing profile:	• Under **Copy from Profile** (bottom of the pane), choose from the list of predefined profiles. • Click **Get.** The parameters will be updated. • Modify the required parameters to customize them to your needs. • Click **OK.** The new profile will be added to the INP Monitor Profile pane.
Set the US=DS	Checkmark **Set Upstream Values as Downstream** if US and DS settings are identical.
Set the counting of the two histograms according to the following parameters:	• Inter Arrival Time Offset (INMIATO) - specifies the minimal duration of impulse (cluster) that would be counted at bin 0 of INMIAT histogram. • Inter Arrival Time Step (INMIATS): specifies the time step in INMIAT histogram, the step size is 2^INMIATS • Cluster Continuation (INMCC): specifies the maximal gap between bursts of impulses that would still be considered as one cluster • Equivalent INP Mode: o Do not use Clusters - Each consecutive set of severely degraded symbols is counted as a separate impulse event o Upper bound – Histograms provide upper bound for the required INP o Lower bound – Histograms provide lower bound for the required INP o Best Estimation – Histograms provide best estimation for the required INP

An INM Setting Example is given below.

Setting:

- INMIATO is set to 10 (valid values are 3-511, default is 3).
- INMIATS is set to 3 (valid values are 0-7, default is 0).
- Cluster Continuation is set to 4 DMT symbols (valid values are 0-64, default is 0).

Result:

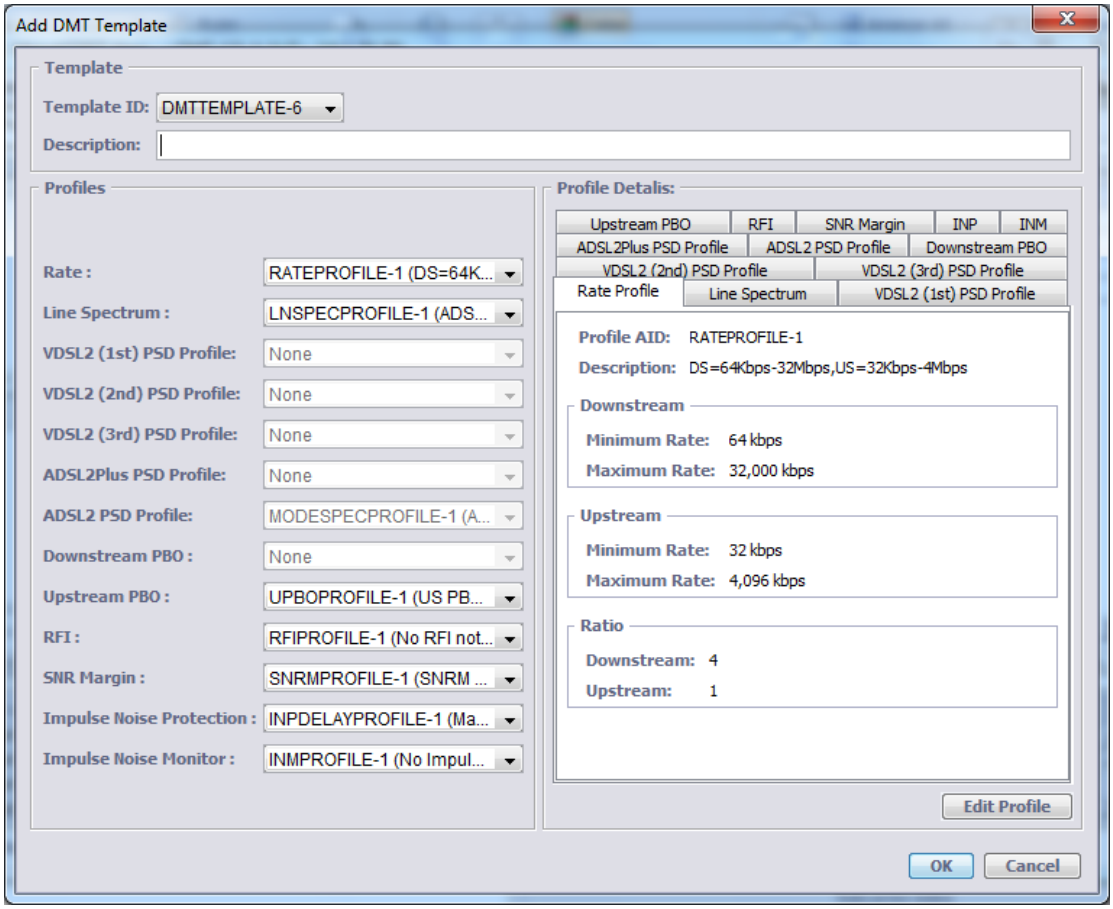
- Cluster Continuation=4 implies that the burst of impulses that doesn't cease for more than 1ms (4 symbols as configured by Cluster Continuation) are considered as one cluster and counted as a single impulse noise in the Impulse Noise Histograms.
- INMIATO=10 implies that impulse clusters with a gap of up to 10 DMT symbols (2.5ms) would be counted in INMIAT histogram at bin 0, impulses with longer gaps would be counted at higher bins according to the INMIATS value.
- INMIATS=3 implies that each bin the INMIAT histogram collects the data to bins of 2^3=8 symbols. In this example the first bin counts cluster occurrences with inter-arrival time of up to 10 symbols, the second bin counts occurrences of up to 18 (10+8) symbols, the next 26 symbols (10+2x8), etc.

Configuring Templates

The HSL calibration templates consist of a predefined set of profile *types*, where not all profile types are relevant to each template. Each profile type supports a pool of previously defined profiles. To generate a template, simply choose the relevant predefined profile for each type that is relevant to the required template.

➢ To configure HSL Calibration templates

1. In the **Network Element** Tree under **Modem Profiles**, click **Templates**. A summery view of the defined templates and their profiles appears.
2. Click **Add Template.** The following dialog appears.



3. Choose the **Template ID** from the list and assign the new template a description.
4. For each relevant Profile, select from the available pool. (Note that not all profile types are accessible for all templates).

   NOTE: the content of each selected profile may be seen in the right pane by selecting the required tab.

5. Click **OK.**

7 Quality of Service (QoS)

This chapter describes how to configure the QoS on ML700 units.

In This Chapter

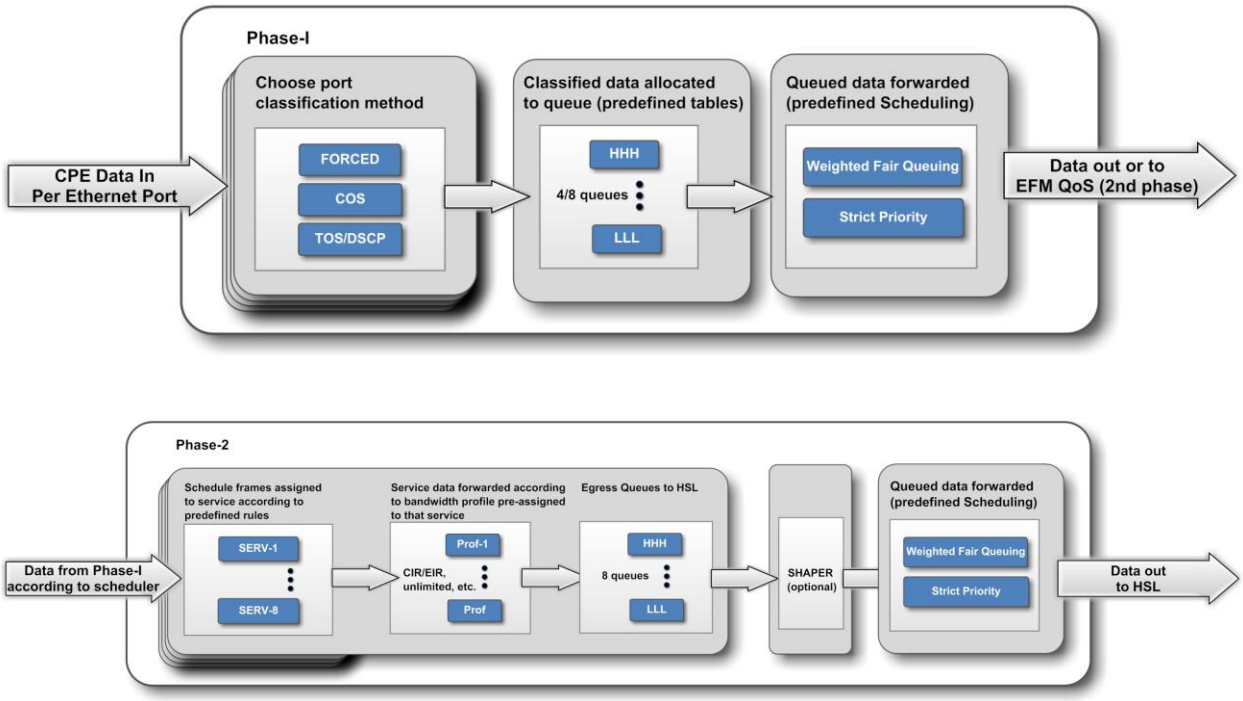
Overview

ML700 units apply user configured QoS on traffic received on the Ethernet ports and again on the same traffic as it is processed and forwarded to the HSL ports.

The following QoS elements can be configured on each **Ethernet port**:

- Classification method - forced, COS or TOS/DSCP, according to the method which the data received on that port is analyzed and classified.
- Queuing - assignment of the *original* data traffic to one of four or eight queues (model dependent) according to its classification marking (i.e. COS frame 3 to queue 4, COS frame 6 to queue 8, etc.). The markings to queue allocation are determined by the (system level) **classification tables** (on page 7-6).
- Scheduling - priority mechanisms to be applied to the queues to match Traffic Management objectives of jitter, latency and frame loss ratio.

On Ethernet (ETH-x) ports, L2/L3 Priority-to-Traffic Class mapping is applied on original frame data. On an HSL port, L2 Priority-to-Traffic Class mapping is applied only after L2 Priority COS bits translation (regeneration) is applied, see CoS Marking Configuration. Thus, Classification result on an HSL port depends on the configuration of two tables (Translation and then Classification).



Classification Method

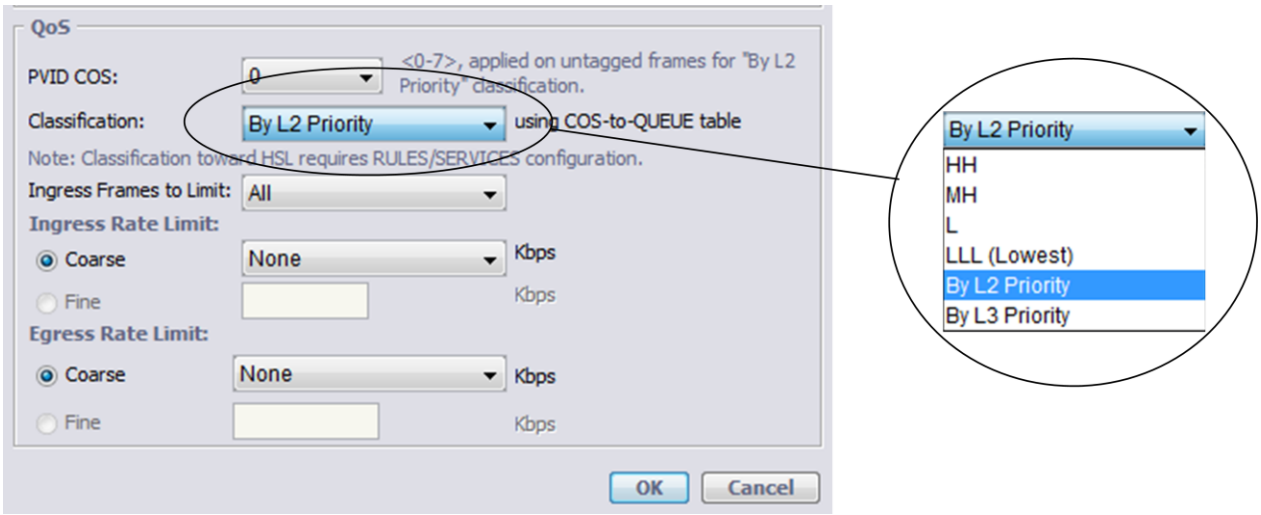
Traffic ingressing the port, is classified according to Forced, Layer-2 or Layer-3 method. The classified frames are assigned to specific queues according to the **L2/L3 Queuing Priorities** (on page 7-6) tables (defined on a system level).

Identification Rules and Services (see **Ethernet Service Configuration** (on page 10-1)) configured for HSL only, are additionally applied to the traffic and may be either equal to or differ from the all-ports-applicable Classification Tables.

NOTE: Traffic may be briefly disrupted during the implementation of Ethernet port configuration changes.

➢ To configure the classification type per port

1. In the **Network Element** tree, expand **Ethernet Ports** and select the Ethernet port to be configured and in the Ethernet port pane **Configuration** area, click the **Configure** button. The Configure Ethernet Port dialog appears - partial dialog displayed below.



2. PVID COS – relevant for By Layer 2 Priority classification method (see below).
3. In the Classification list box, select the required port priority:
   - Layer 2 Priority - Default. Incoming frames are mapped to a queue corresponding to the COS priority bits of the external VLAN tag. If traffic is VLAN-untagged, the configured PVID COS parameter value is assigned to the frame

     NOTE: L2 Priority classification cannot be assigned to the Port if "PPP" encapsulation is selected on the bridge. If PPP encapsulation was applied after By L2 Priority classification was selected on the port(s), this setting of these port(s) is automatically reverted to the following forced priority: LOW on ETH ports and HIGHEST on COLAN and HSL.
   - Layer 3 Priority - incoming frames are mapped to a queue (of egress port) corresponding to their DSCP or ToS bits detected in the IP header of the frame. Both VLAN-tagged and VLAN-untagged frames can be classified.

NOTE: By L3 Priority classification is limited to a single port only, if "PPP" encapsulation is selected on bridge.

- HH, MH, L or LLL - provide forced priority. ALL of the port's incoming frames are mapped to the selected queue: HH - Highest, MH - High, L - Medium or LLL - Lowest.

4. Limiting Rates – note that frames are further handled when egressing (prior to being forwarded to the HSL wire), at a maximum throughput of 1000 Mbps. If the GBE option(s) enabled, is will be required to limit the throughput. This can be done by limiting either the Ingress or the Egress rate:
   - Limiting Egress Rate – recommended option. See Rate Limit for Egress Rate configuration criteria for Eth-x and HSL ports.
   - Limiting Ingress Rate – (available only on Eth-x ports). It is not recommended to used this option: since the ingress rate limit is applied prior to classification, this type of limiting conflicts with Quality of Service objectives configured on the NE. See **Rate Limiting** (on page 7-5) for more information.
   - Click **OK**.

Rate Limit

Data can be limited either **ingress** (prior to classification) port traffic, **egress** (after classification and switching decision is made) port traffic or both **ingress and egress**. *Note that ML does not consider IFG (Inter-frame-gap) and Preamble bytes as part of the Ethernet Service BW. Rates specified for limit are for NET Ethernet traffic (bytes of ETH frames).*

NOTE: It is recommended to apply limiting on ETH-x port facing the customer by setting egress rate limit on the customer side of the link, on the port of device attached to the ML NE port

Egress Rate Limits - RECOMMENDED:

- Egress rate limit on HSL ports should be set symmetrically on CO and CPE side.
- Egress rate limit "Fine granularity" is enabled for HSL ports only (not for ETH-x ports).
- Egress rate limit is not applied (even configured) to ETH-x port(s) operating in Half-Duplex (HD) mode.
- Egress rate limit applied on ETH-x ports using values selected from the Coarse Granularity list, guarantee up to 95% accuracy of limited rate value. Values selected from Fine Granularity (free text typed values) may provide less accuracy of limited rate value.
- Egress rate limit applied on HSL port(s), may pass 30% more traffic (then in case of 1636 bytes frames) in case of frames of 64-bytes size. This is due to the NET traffic calculation method and lack of Ethernet media overhead (IFG (Inter-frame-gap) and Preamble bytes) on HSL "wire", which transmit Ethernet NET frames via MEF aggregation over DSL modems.

Ingress Rate Limits:

- Since the ingress rate limit is applied prior to classification, this type of limiting *conflicts* with Quality of Service objectives configured on the ML700.
- Ingress rate limit on ANY type of traffic is available on ETH-x ports only - not on HSL (where this option is blocked to prevent in-band management loss)
- Ingress rate limit less than 10 Mbps, may operate inaccurately for TCP traffic.

  Some applications that use TCP transport will be affected by blocking ingressing traffic, causing low utilization of Ethernet transmission bandwidth (significantly below the configured limit). This may be improved by allowing ingress limit burst (per bridge configured); however, for UDP type of traffic this setting will increase the Ethernet transmission bandwidth above the configured limit.

L2 (CoS) / L3 (DSCP/ToS) Queuing Priorities

Each classification method (selected on a port level) operates according to a priority queue defined on a system level. The default definitions are detailed in the table below. For example, if L3 DSCP method is selected on the relevant Ethernet port, and bit 18 is identified, the frame will be allocated to queue L; if L2 Priority classification method is selected and bit 6 is identified, the frame will be allocated to queue HHH and so forth. The classification priorities (for each classification method) can be modified on a system level.

The following table shows the default Classification settings available on all models.

Table 34: L2/L3 Default Classification

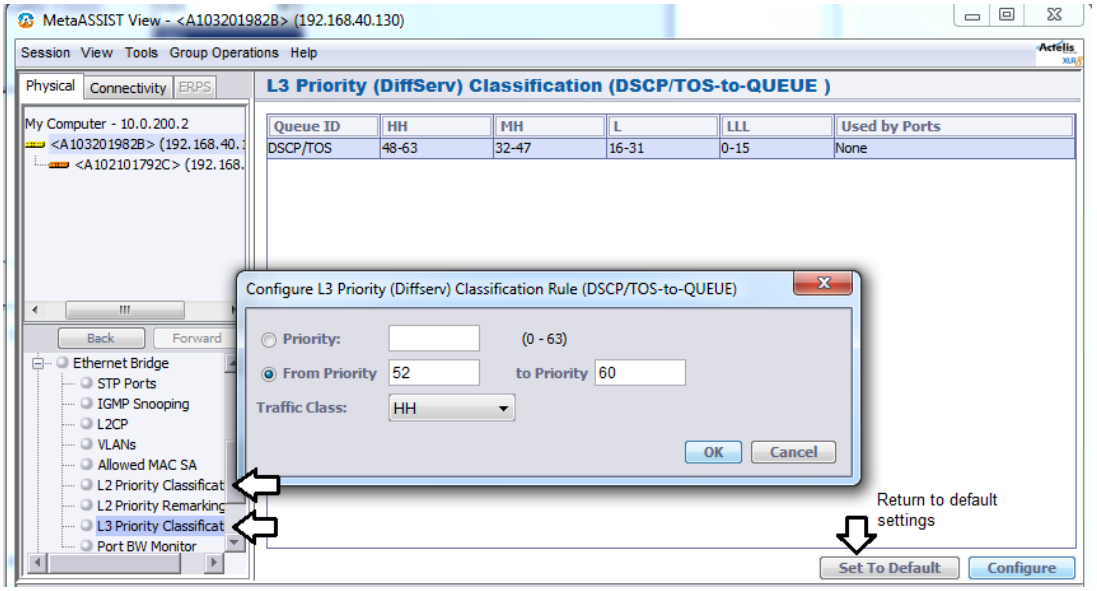
Class (QUEUE)	L2 CoS Priority bits	L3 DSCP bits	L3 ToS bits
LLL	0-1	0-15	0-1
L	2-3	16-31	2-3
MH	4-5	32-47	4-5
HHH	6-7	48-63	6-7

➢ **To change default L2/L3 Priority (COS)**

1. In the Network Element tree, expand **Ethernet Bridge** and select **L2/L3 Priority classification**.

   The current classification mapping rules are displayed, along with the ports on which *L2/L3 Priority* is configured (i.e. ports on which L2 or L3 Priority will be used).

2. In the invoked pane, click **Configure**. The L2/L3 Priority configuration dialog appears. (Below is an example of L2 Priority Configuration dialog).



3. For *each class*, configure the priority level(s) as follows:
   - From the **Traffic Class** list box, select the traffic class (e.g HH).
   - Either configure a single priority using the **Priority** field, or
   - configure a range of priorities using the **From Priority** and **To Priority.**
   - Click **OK**. The priority range appears in the table. Multiple ranges in each class are separated by a comma.
4. Repeat the procedure for additional priority configurations.
5. To restore default priorities, click **Set to Default**.

NOTE: Unmodified priority values remain at their current values.

Classification

As specified in the general QoS flow scheme (see **Quality of Service (QoS)** (on page 7-1)), frames are additionally handled on egress direction of HSL port prior to being forwarded to the HSL wire. Throughput of this additional functionality is up to 1000 Mbps. For this reason,for proper QoS functioning, summary of rates on access ports (ETH-x) should not exceed 1000 Mbps.

NOTE: Access can be limited by either:

- Egress rate limiting on ports of the NE connected to the ML NE (preferred solution, as the frames are dropped according to the NE classification results).
- By ingress rate limiting on ML NE ports (not recommended, since frames arriving to the wire are dropped prior to being classified on the ML NE).

Identification Rules and Services (see **EVC Configuration** (on page 10-1)) configured for HSL only, are additionally applied to the traffic and may be either equal to or differ from the all-ports-applicable Classification Tables.

ML700 models by Factory default provide rules which are equal to the By L2 Priority classification scheme selected on all Ethernet ports, and apply default according to the L2 Priority (COS) Classification Configuration table settings.

CoS Marking

ML700 devices allow flexible COS bits marking in aware-from-HSL direction, using "COS bits Translation" (applied on HSL Ingress) table. This marking is applicable only for tagged ETH frame ingressing the TAGGED HSL and egressing the TAGGED ETH-x ports. In other configuration VLAN tag, even with modified COS bits, will be just stripped (on ingress or egress) from the original VLAN tag.

The classification results can be propagated to the L2 Priority COS bits of the original frame either directly in the original Customer TAG or in the external Service Provider Added TAG.

ML700 devices allow flexible COS bits marking towards the HSL using the following configurable parameters:

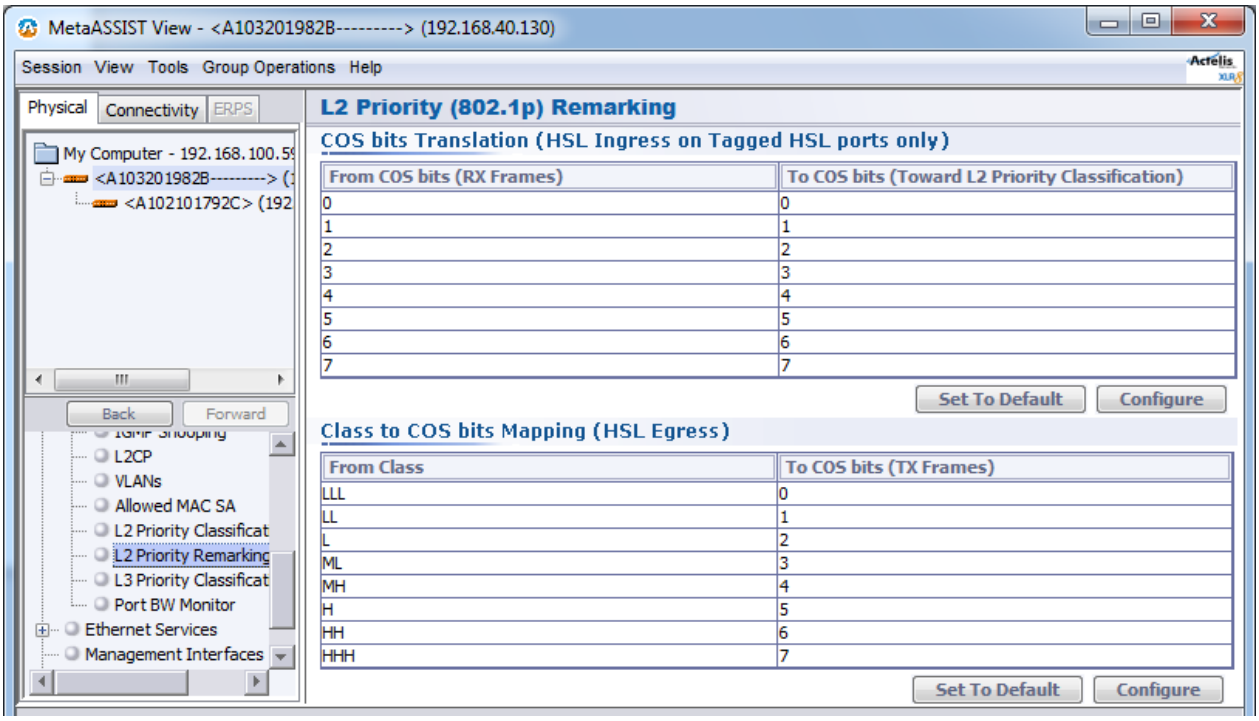
- RULE MARKING - determines if marking CLASS-TO-COS should be applied, see **ML 700 Identification Rules Definition** (on page 10-13)
- SERVICE QUEUE ID - specifies the CLASS of the Ethernet frame, see **ML 700 EVC Services Definition** (on page 10-10)
- CLASS to COS bits Mapping table - maps between CLASS assigned to the frame and COS bit to be written in outer tag.

Marking flow is continued on CO NE, where ML devices allow overwriting COS bits of external VLAN tag (usually already Service Provider tag), using COS bits translation table, which is per-bridge configurable. Mapping is applied for Incoming traffic on HSL ingress ports, before classification, on the systems.

➢ To view and modify COS marking

1. In the **Network Element** tree, expand **Ethernet Bridge** and select **L2 priority Re-marking.** The pane shown below appears.

The pane shows the classification results translation table (and the translation configuration dialog). *By default, marking is transparent.*



2. To modify the COS bits translation table:
   - Click the **Configure** button in the window area (Egress or Ingress). The Configure L2 Priority dialog appears as show above.
   - For each COS bit to be translated, select the corresponding value in the **To COS bits** column.
3. Click **OK.**

Scheduler and Queue Congestion Control

As specified in the general QoS flow scheme (see **Quality of Service (QoS)** (on page 7-1)), each port in the egress (toward wire) direction has four queues, which allow prioritizing the traffic which was classified before switching, on another port in ingress (from wire) direction.

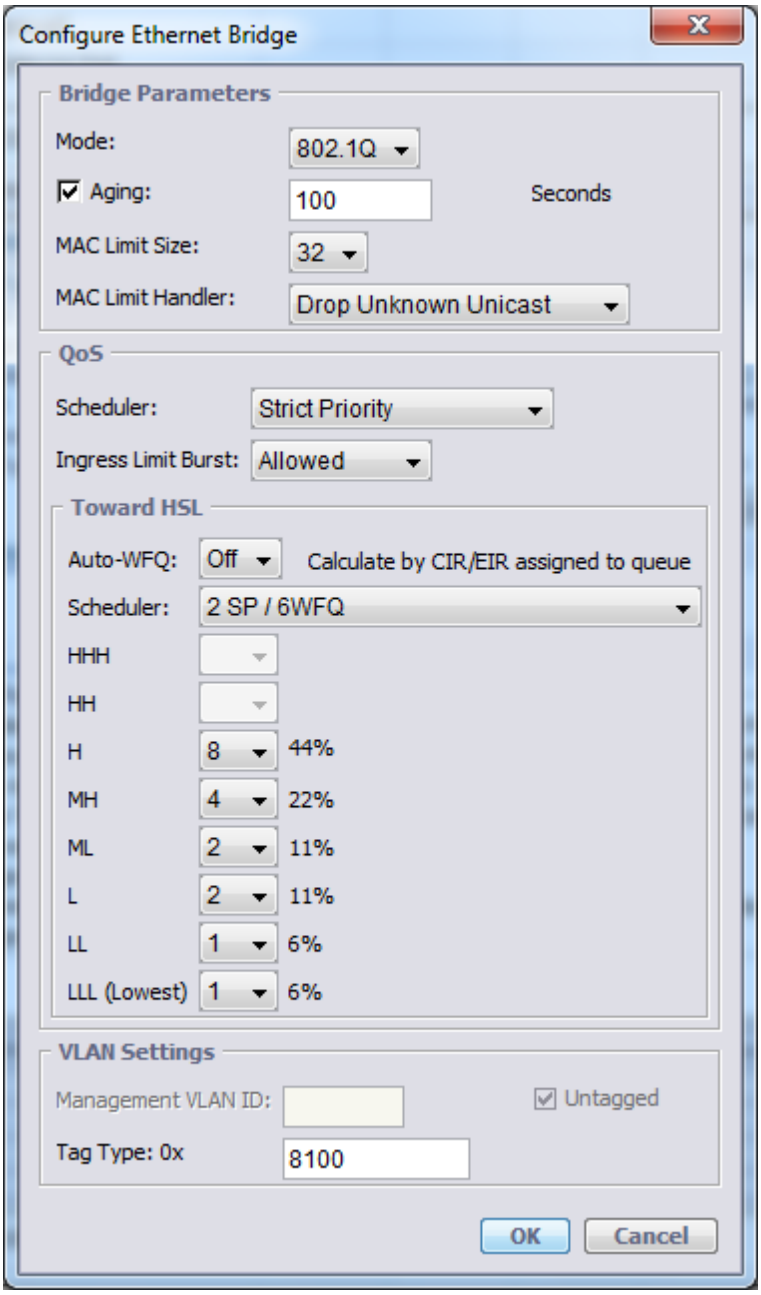
Frames are extracted from these four queues using the scheduler mechanism. ML700 allows selecting either Weighted Fair Queue (WFQ) or Strict Priority (SP) scheduler (per-bridge selectable).

As specified in the general QoS flow scheme, HSL ports support 8 queues operating in hybrid scheme, utilizing SP scheduler for higher priority queues and WFQ scheduler for lower priority queues – with configurable weights per each WFQ queue. SP or WFQ mechanism can be applied on 8 queues in combination of 8 (SP):0(WFQ), 6(SP):2(WFQ), 4(SP):4(WFQ), 2(SP):6(WFQ), 0(SP):8(WFQ).

Scheduler Configuration

➢ **To configure the Scheduler Scheme (applied to traffic towards the HSL only)**

1. In the Network Element tree, select **Ethernet Bridge** and in the invoked pane, click the **Configure** button. The Configure Ethernet Bridge dialog appears.



2. Select **Ingress Limit Burst** behavior, applied only when Ingress Rate Limit is specified on the Ethernet port(s):

- If Ingress Limit Burst is **Allowed** (default) and Ingress Rate Limit is set on the Ethernet port, an additional memory buffer is allocated on the ingress direction of the port, which allows - in case of TCP traffic (with burst nature), to accept more traffic without dropping it immediately, and to forward toward egress port, where egress behavior is applied. The ingress burst buffer doesn't guarantee that all accepted traffic will be forwarded, but it improves the TCP traffic utilization through the Ingress Limited Port.
- If Ingress Limit Burst is **Not Allowed** and Ingress Rate Limit is set on the Ethernet port, the port accepts an exact amount of traffic as specified within ingress rate limiting.

3. In addition to the above, WFQ Weights and Strict Priority queues can be determined by configuring the **Scheduler** field located under **Toward HSL** as follows:

   The Scheduler values are displayed in the following format: *number* SP- *number* WFQ, where the *number* of SP determines the number of Strict Priority queues, and the *number* of WFQ determines the number of Weighted Fair Queues. For example, when selecting **2 SP - 6 WFQ**:

   - Queues HHH and HH are handled by strict priority scheduling.
   - Queues H to LLL are handled by weighted fair queue scheduling. Each of these queues can be assigned weight that determines the number of frames that will be forwarded from this queue before the next (lower) queue is given priority (switched).

4. Configure the WFQ Weights assignment mode by setting the **Auto-WFQ** field as follows:

   - **Off** - enables setting WFQ manually. This mode is recommended if all configured Ethernet Services use unlimited BW profiles. Therefore, the final prioritization between service Flows output is achieved by assigning the weights of the queues. Range: 1 to 15, counted in frames, where default settings can be used.
   - **On** - sets WFQ automatically. This setting is recommended, if all configured Ethernet Services use CIR/EIR specified BW profiles. Therefore, the final prioritization between Ethernet Service traffic output should be done according to the CIR/EIR configured per Service/all Services. Such calculation is performed automatically by the ML, setting weights per queue in a way that CIR quantity of all WFQ queues is prioritized above EIR quantity of all WFQ queues. See **Auto WFQ** (on page 7-14)for more details.

5. Click **OK**.

Auto WFQ

This section provides additional explanations on the Auto-WFQ options set in the **Ethernet Bridge** (on page 7-12) dialog.

When WFQ is set manually, weights assigned on WFQ queues are not coordinated with CIR and EIR rates. CIR and EIR rates reserved on these queues are set via the BW profile of a Service.

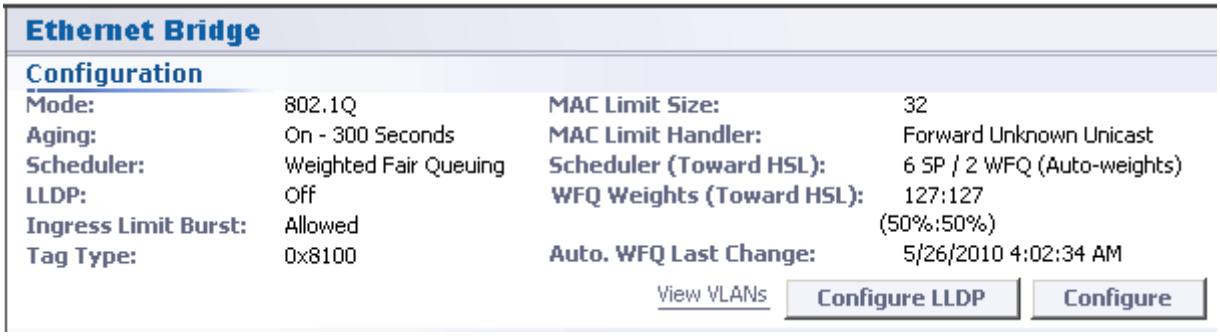
Moreover, manual (and static) configuration of weights does not allow correlating between HSL BW available which can be reduced when MLP fails (modem out-of-sync or modem rate reduced to adjust the environment). When HSL BW is not enough for all CIR in all WFQ queues, manual (and static) weights will cause usage of remaining HSL BW unfairly for EIR of higher (in WFQ it means a queue with bigger weight) priority queue instead of fair approach to use remaining HSL BW for CIR of lower (in WFQ it means a queue with smaller weight) priority queue.

Applying Auto-WFQ, the ML automatically and dynamically calculates weights each time when Service configuration is changed (CIR/EIR values) or HSL BW is changed (reduced/restored).

➢ **To enable the Auto-WFQ feature, the following flow should be applied:**

1. Set Bridge: configure the Hybrid Scheme and keep WFQ Weights default assignment (applied per selected Hybrid scheme).
2. Define BW profiles for Default services to avoid use of BWPROFILE-0 (CIR/EIR = Unlimited). For example: Apply BW profile with CIR=3Mbps/EIR=0MBps for Services which are assigned to SP queues and Apply BW profile with CIR=0/EIR=Unlimited for Services which are assigned to WFQ queues.
3. Define BW profiles to be used by user-defined services.
4. Set Services, using BW profiles and Queues (regardless of WFQ)
5. Set Rules – to identify service flows and assign them to Services.
6. In the **Bridge dialog** (on page 7-12), enable Auto-WFQ. The feature is now operative.

The resulted auto-weights can be seen on Bridge pane as follows:



8

VLAN Configuration

Actelis products use VLANs for cross-connections between Ethernet ports, providing both Ingress and Egress VLAN Forwarding Rules in a single operation using the VLAN configuration. VLANs are configured via the VLAN configuration pane.

In This Chapter

VLAN Configuration Principles

VLANs are separately configured for Customer service traffic (Traffic VLANs) and Actelis Product NE management traffic (Management VLAN). Traffic VLANs can be edited, added and deleted, while the Management VLAN can only be edited. (Detailed examples of VLAN topologies are provided in **Appendix G - VLAN Topologies** (on page G-1)).

NOTE: VLAN Editing operation causes a short disruption in the traffic flow.

➢ **The following parameters are configured per VLAN:**

- VLAN ID - defines a unique identification of a cross-connect between ML device ports, which participate in the specific Virtual LAN.
- VLAN name - textual description of the cross-connect.
- VLAN type - defines the VLAN as either TRAFFIC, MANAGEMENT or PWE (ML model dependant). Only Management VLAN includes implicitly (not user configurable) a CPU of the ML Device, which allows ML device Management access. Traffic and PWE VLANs will *never* access the CPU of the ML Device.
- VLAN port member parameter - defines the group of ports, which belong to the particular Virtual LAN. The traffic is forwarded between VLAN members only, limiting unknown MAC broadcasts.

VLAN membership type parameter is specified per each VLAN port member and defines both frame filtering and frame modification behavior of the port by a single parameter.

Table 35: Filtering and Modification Behavior Types

Filtering action types	Modification action types
• Accept ANY traffic (VLAN-tagged or VLAN-untagged). • Accept only VLAN-untagged traffic. • Filter particular VLAN-tagged traffic.	• Do not modify the frame. • Strip (on egress) and insert (on ingress) a new Tag.

Actelis products support 3 combinations of membership type called Untagged, Tagged, Stacked. For more information see VLAN **Membership Principles** (on page 8-8).

Management VLAN Configuration

By factory default, the management VLAN is set to 100, allowing VLAN-unaware management traffic via COLAN (MGMT) port (out-of-band only).

In the following case you may want to change the default:

- If it is required to use in-band management to eliminate the need for a separate connection to the COLAN (MGMT) port of the ML device. In this case, modify the Management VLAN ID accordingly, and select one of the service ports as a member;
- If out-of-band management traffic is tagged. In this case, modify the COLAN (MGMT) port to be a tagged member of the Management VLAN;
- If the assigned Management VLAN ID is already used in the MAN/WAN for traffic. In this case, select a different VLAN ID for Management, equal to that used in MAN/WAN for management purposes.

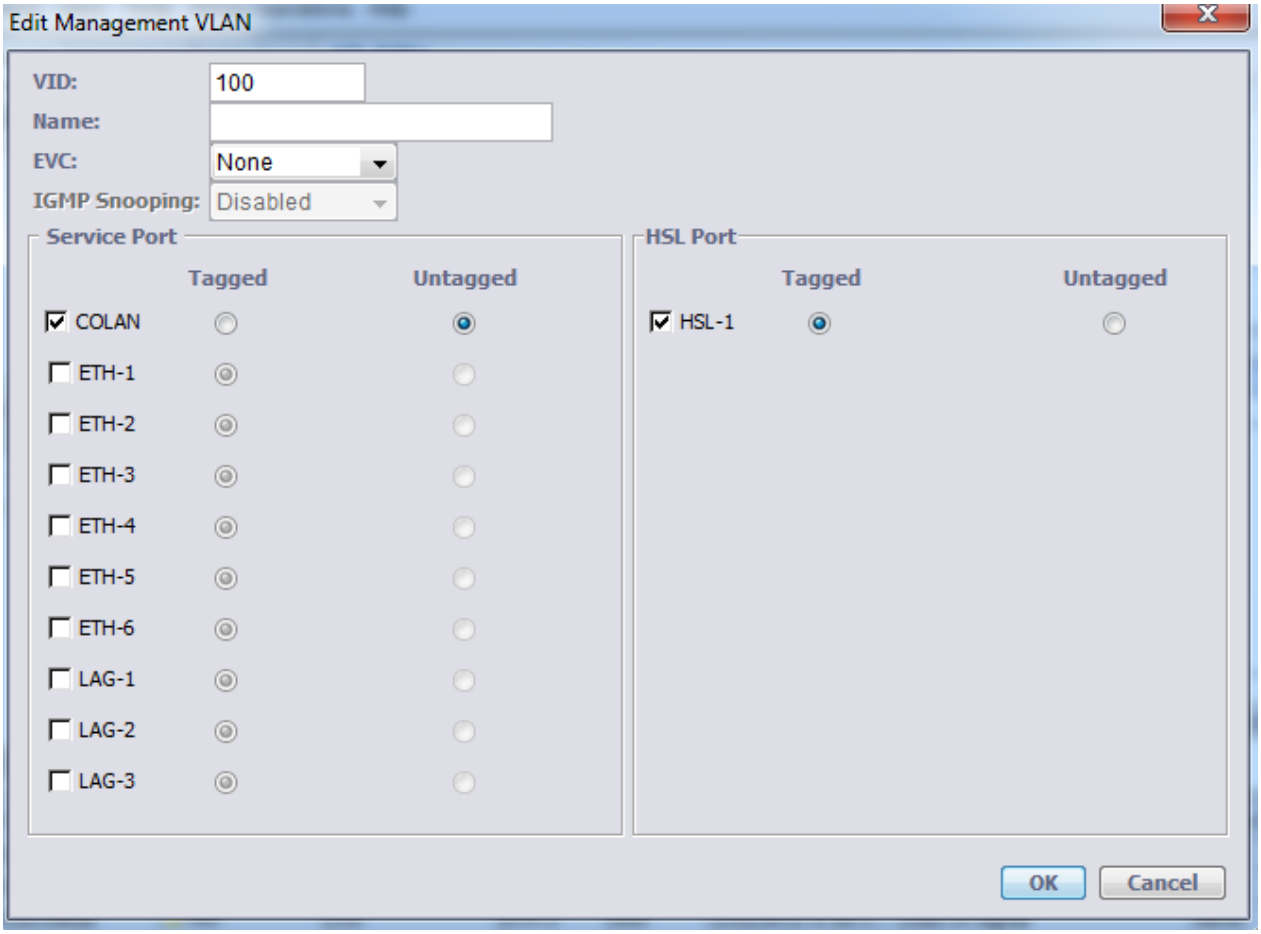
The following limitations are applied on the COLAN port/MGMT VLAN:

- A single Management VLAN is allowed in Actelis systems;
- Management VLAN cannot have stacked members;
- COLAN can be deleted from the MGMT VLAN and must be specified in MGMT VLAN;
- MGMT VLAN = 100 is defined on all HSLs (as Tagged member) regardless of their provisioning status (even deleted).

➢ **To edit the management VLAN:**

1. In the Network Element tree, open **Ethernet Bridge**.
2. Open **VLANs**. The **VLANs** pane opens.
3. From the VLANs table, select the management VLAN ID.

4. Click **View VLAN**. The **Edit Management VLAN** dialog appears (dialog may vary depending on the ML model).



5. In the **VID** box, type the VLAN number.
6. For VLAN name, in the **Name** box, enter the VLAN name (up to 16 characters).
7. In the **Service Port** area, select either **COLAN** or **ETH <ID>** check box. Also select the VLAN membership option (Untagged, Tagged or Stacked) for this port according to Provider/Customer network requirements.

   NOTE: ETH <AID> as a regular Ethernet port, can be assigned as member of management VLAN, providing in-band management.

8. In the **HSL Port** area, select the **HSL** check box (only Tagged membership option is available for HSL).
9. Click **OK**.

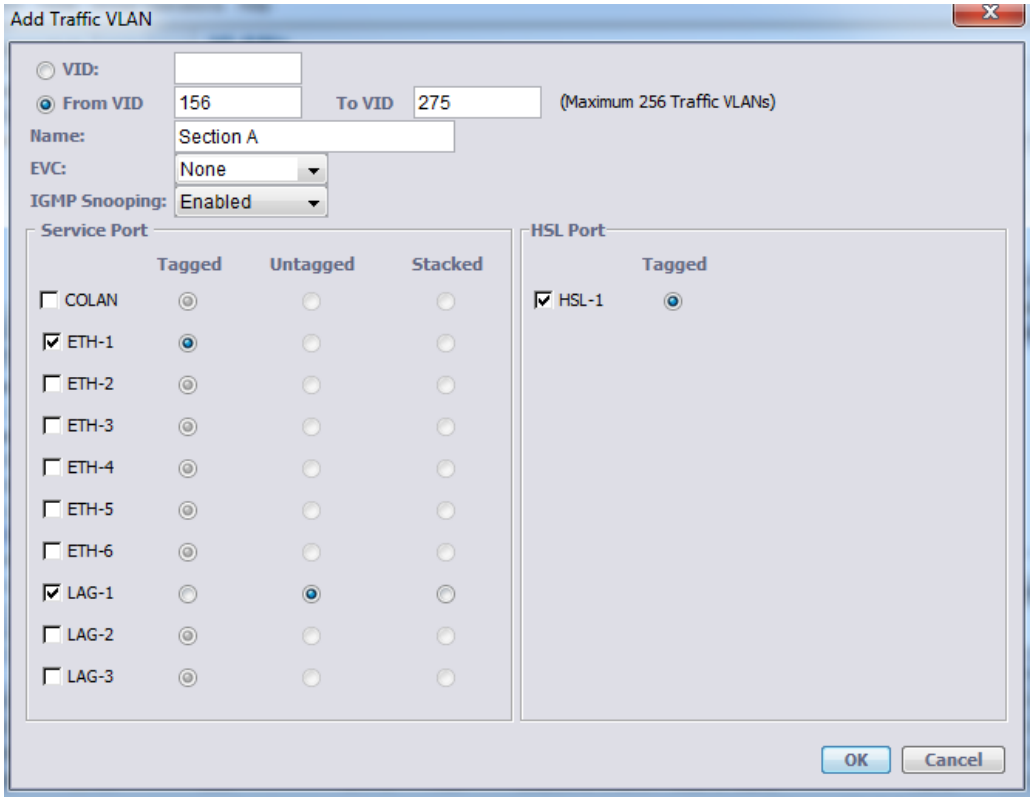
Traffic VLAN Configuration

When configuring a Traffic VLAN, take the following into account:

- Coordinate the VLAN number with the customer switch (network environment).
- If PPPoE option is enabled, VID=4094 and 4093 are reserved for system use and cannot be configured.
- VID 4092 is the system's default PWE VLAN (management type) on HSL-1 and it CAN be modified.
- ML700 supports **IGMP** (on page 5-13) configuration.
- All Ethernet ports including COLAN can be an Untagged, Tagged or Stacked member of the traffic VLAN.
- If the VLAN has Stacked and Tagged ports, when Customer traffic is untagged, L2 Classification does not work on Tagged port (HSL). Therefore, if HSL BW is greater than the ETH BW (limited by Port Mode), congested packets will be randomly dropped.

➢ To configure a VLAN

1. In the Network Element tree, expand **Ethernet Bridge** and open **VLANs**. The **VLANs** pane opens in the work area.
2. Click **Add VLAN**. The **Add Traffic VLAN** dialog appears.



3. The EVC option is used to **associate the VLAN with EVC** (on page 10-6).

4. The **IGMP Snooping** (on page 5-13) option is used to enable IGMP Snooping on the VLAN. IGMP snooping is configured and controlled on a system level. When it is enabled on the level, IGMP snooping is applied only in VLANs with IGMP snooping enabled. In other VLANs, IP multicast traffic pass transparently. The option is enabled by default.
5. To assign one or more ports to a single VLAN:
   - Enable **VID** and assign the VLAN number.
   - You may assign the VLAN a name, in the **Name** box. Range: up to 16 characters.

   To ports simultaneously to a number of VLANs, use the **From VID** and **To VID** fields to enter a range of VLANs. Range: up to 4095
6. In the **Service Port** area, select either **COLAN** or **ETH <ID>** check box.

NOTE: COLAN as a regular Ethernet port, can be assigned as member of any traffic VLAN.

7. Select the VLAN membership type for this port according to Provider/Customer network requirements: : Untagged, Tagged or Stacked
8. In the **HSL Port** area, select the **HSL-1** check box (HSLs are always tagged members)
9. Click **OK**.

VLAN Control Overview

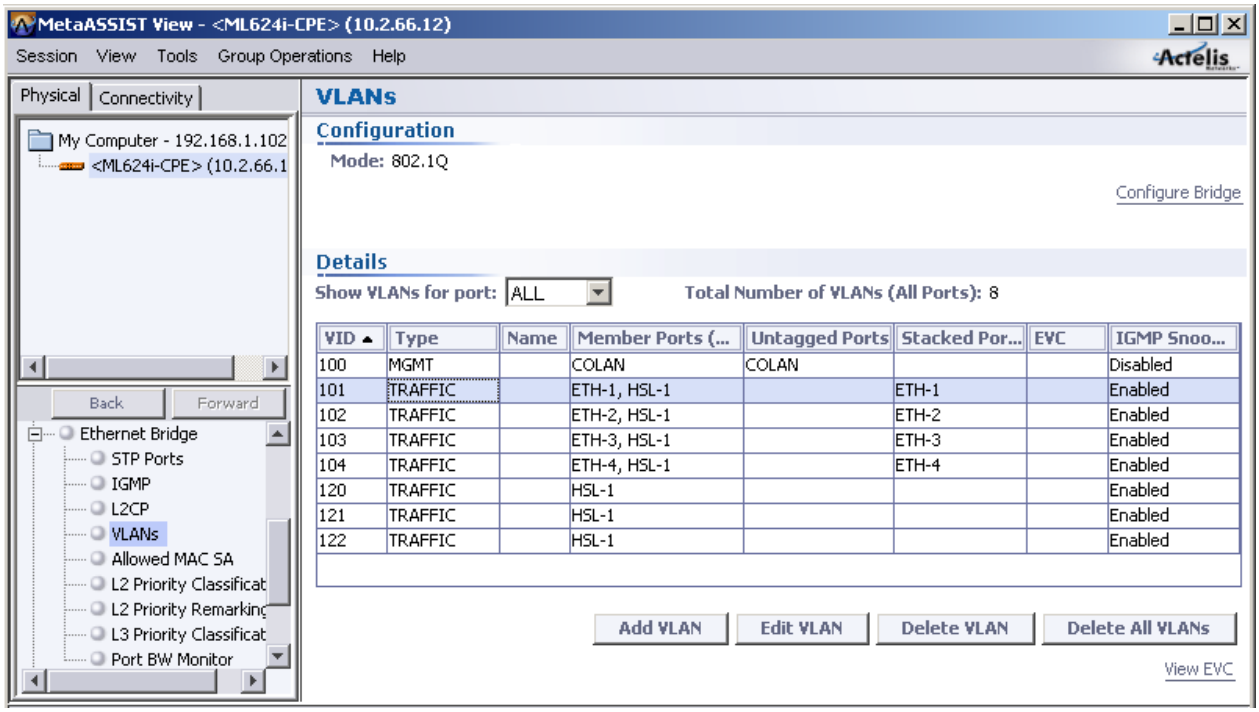
The VLAN Management pane provides a list of the currently configured VLANs and provides VLAN management options (Add VLAN, Edit VLAN VLANs, etc.).

➢ **To access the VLAN management pane**

In the Network Element tree, select **Ethernet Bridge** and choose **VLANs.** Open **VLANs**. The **VLANs** pane opens.

Navigating the VLAN display:

- The VLANs can be sorted according to relevant ports (under **Details** - Show **VLANs for port**:....).
- The VLANs can also be sorted by clicking on the column headers (Type, Name, etc.)
- Each VLAN is displayed along with various configuration parameters.
- The management options (Edit VLAN, Delete VLAN) are relevant to the selected VLAN.
- The **View EVC** option (under Delete All VLANs) can be used to access the EVC management dialog.



VLAN Membership Principles and Rules

Port membership to a VLAN is determined by the bridge port on which data frames are received. VLAN cross-connections provide forwarding rules applied on each port configured as a member in a specific VLAN. The guidelines provided in this section explain various VLAN port membership forms and rules.

VLAN Membership Principles

IEEE 802.1Q provides support for 'virtual bridged LANs' where a single bridged physical LAN network may be used to support multiple logical bridged LANs, each of which offers a service approximately the same as that defined by IEEE 802.1D. Such virtual LANs (VLANs) are an integral feature of switched LAN networks. A VLAN can be viewed as a group of end-stations on multiple LAN segments and can communicate as if they were on a single LAN. IEEE 802.1Q defines port-based Virtual LANs where membership is determined by the bridge port on which data frames are received.

Generally, ports can be specified as Tagged, Stacked or Untagged per VLAN and can be allocated to multiple VLANs. However, there are some membership limitations as described in this section. Some of the limitations apply to all ML models while other limitations are model specific.

VLAN cross-connections provide forwarding rules applied on each port configured as a member in a specific VLAN. There are three membership forms for ports participating in a VLAN:

- Ports that are **tagged** members of a VID
- Ports that are **untagged** members of a VID
- Ports that are **stacked** members of a VID

Tagged Members

The following figure shows how ports that are *tagged members of a VID* handle incoming and outgoing frames.

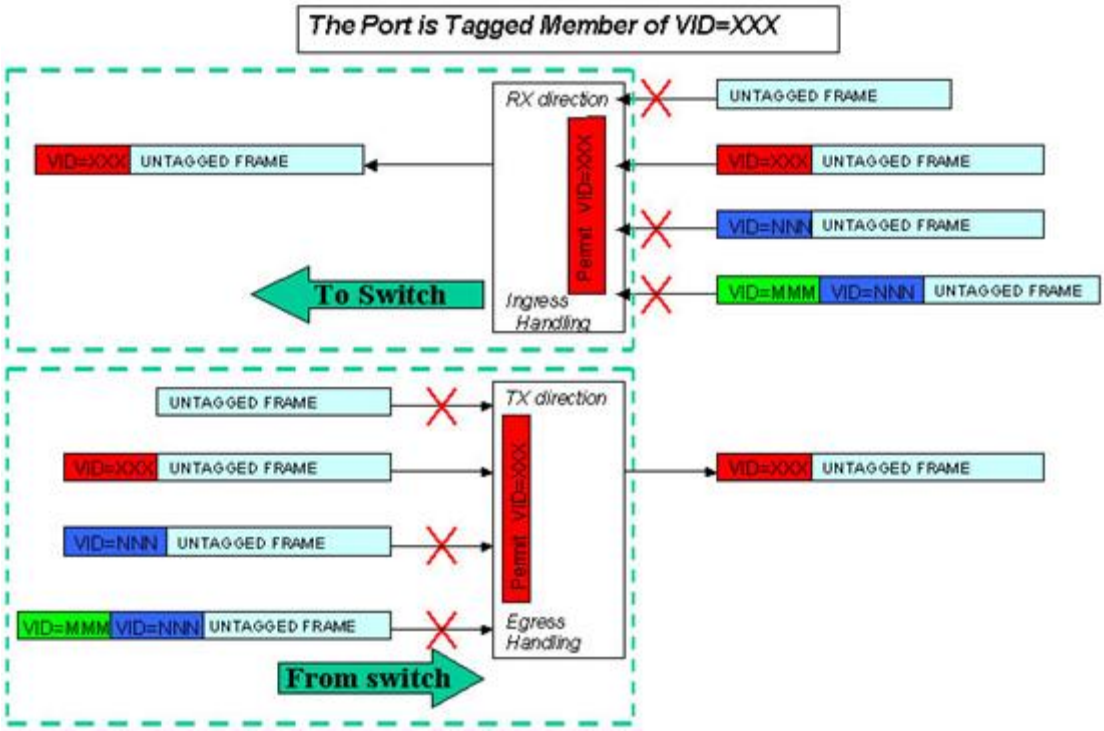


Figure 11: Port is Tagged Member of VID=XXX

Table 36: Tagged Member Description Summary

Direction	Description
In	Allows Tagged (=VID) Traffic only.
Out	No change (tagged traffic).

Stacked Members

The following figure shows how ports that are *stacked members of a VID* handle incoming and outgoing frames.

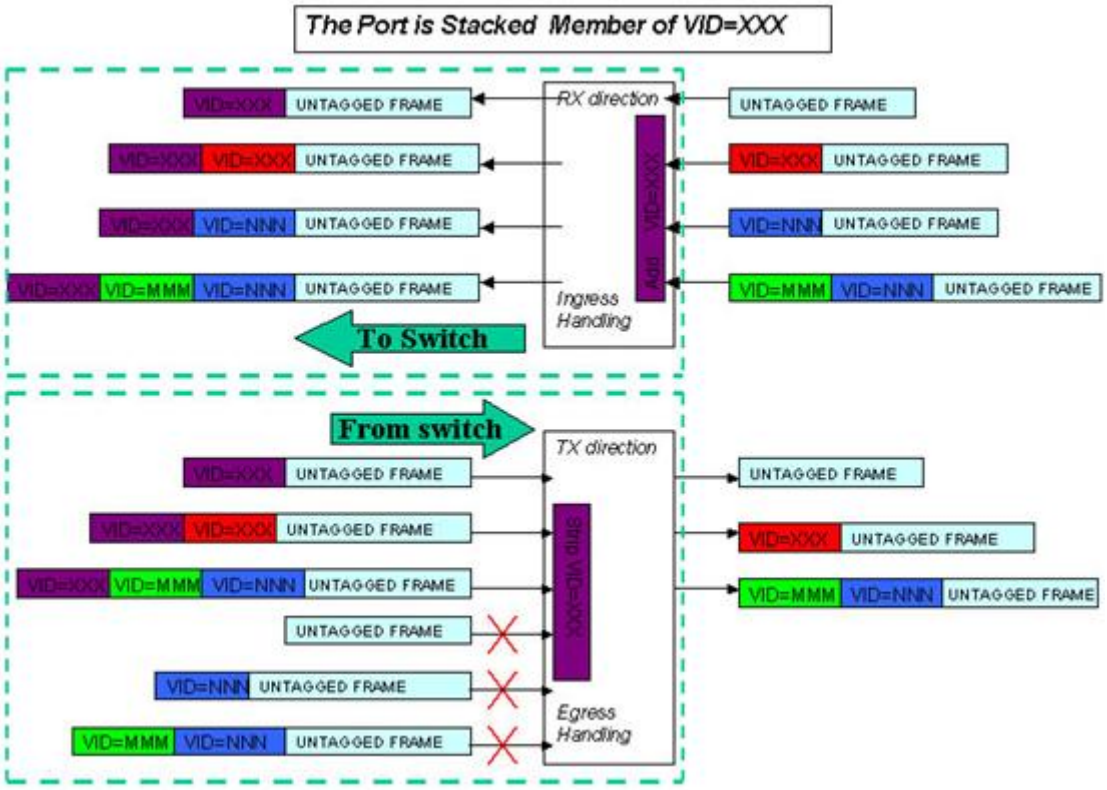


Figure 12: Port is Untagged Member of VID=XXX

Table 37: Stacked Member Description Summary

Direction	Description
In	Allows any traffic and always adds a VLAN tag
Out	Strips VLAN Tag (PVID)

Untagged Members

The following figure shows how ports that are *untagged members of a VID* handle incoming and outgoing frames.

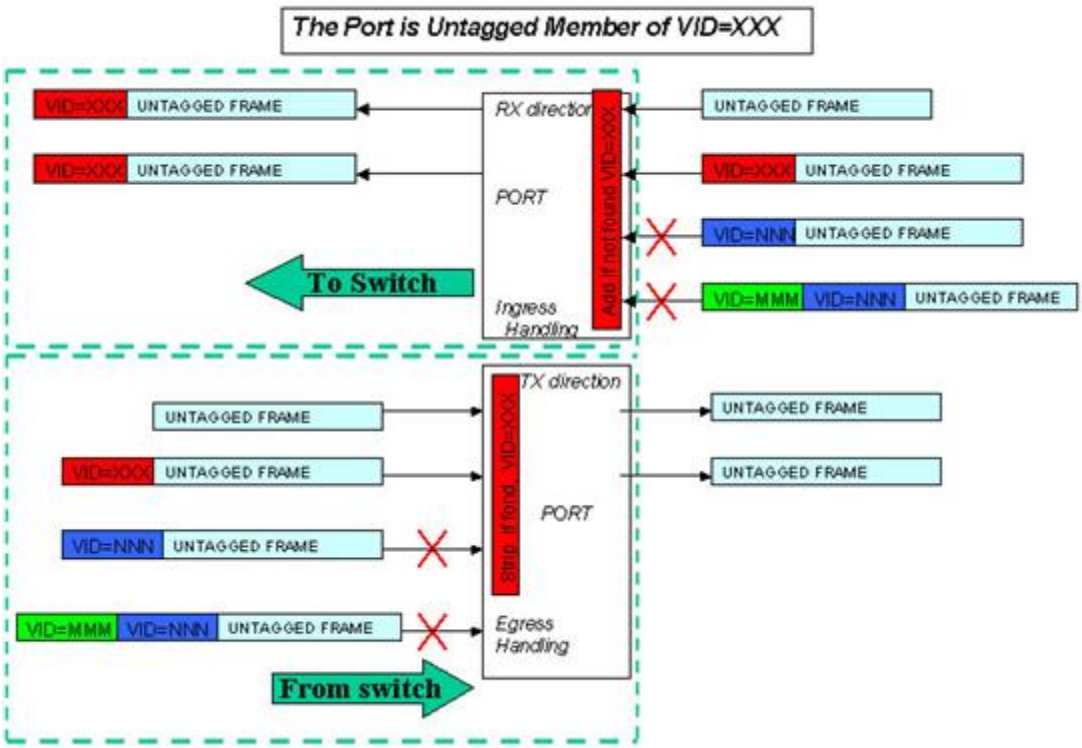


Figure 13: Port is Untagged Member of VID=XXX

Table 38: Untagged Member Description Summary

Direction	Description
In	Allows Untagged Traffic and Tagged Traffic with VLAN ID equal to PVID. For Untagged Traffic adds VLAN tag equal to PVID.
Out	Strips VLAN Tag (PVID). NOTE: When TAGGED (TRFC VLANs) & UNTAGGED (MGMT VLAN) are specified on HSL, do not Strip PVID tag in UNTAGGED MGMT VLAN.

Membership Rules

Generally, ports can be specified as Tagged, Stacked or Untagged per VLAN and can be allocated to multiple VLANs. However, there are some membership limitations as described in this section.

Table 39: Valid Membership Rules

Valid membership combinations on the same PORT	**Valid membership combinations of multiple ports in the same VLAN**	**port participates as a tagged member of a VLAN which includes another port(s) as stacked member(s) then:**
• Port is an untagged member of a single VLAN. Port can be specified as untagged only in one VLAN, i.e. cannot be untagged in multiple VLANs. • Port is a tagged member of a single VLAN. • Port is a tagged member of multiple VLANs. • Port is a tagged member of multiple VLANs and an untagged member of another (single) VLAN. • Port is a stacked member of a single VLAN. Port can be specified as stacked only in one VLAN, i.e. cannot be stacked in multiple VLANs.	• all ports with tagged membership; • all ports with untagged membership; • all ports with stacked membership; • multiple ports, each one with tagged or untagged membership; • multiple ports, each one with stacked or tagged membership; Note1: A VLAN with stacked member(s) can include more than one tagged member. Note2: Stacked and Untagged membership cannot be used in the same VLAN.	• This port (tagged in a VLAN) can be specified as a tagged member of another VLAN which includes other stacked ports. • This port (tagged in a VLAN) can be specified as a tagged member of another VLAN which includes other untagged ports. • This port (tagged in a VLAN) cannot be specified as a tagged member of another VLAN which includes other tagged ports. • This port (tagged in a VLAN) cannot be specified as a stacked member of another VLAN. • This port (tagged in a VLAN) a port tagged in a VLAN can be specified as an untagged and sole member of another VLAN (MGMT VLAN only).

9

L2CP Processing

Layer 2 Control Protocols (L2CP) is a group of protocols standardized by IEEE 802.1, which are used by both Service Provider and Customer L2 Switching Devices. The group of protocols is identified by its destination MAC address. Each ML system allows per port behavior control over each MAC address of an L2CP group. The following behavior types can be defined:

- **Discarding of undesired L2CP frames** in Service Provider-Customer Network and vice versa, which provides full demarcation (as specified in IEEE 802.1ad standard) between Service and Customer L2 Switching devices.

- **Peering (accepting and locally handling) of all L2CP frames**, which provides convergence of all L2 Switching devices into the one common network.

- **Tunneling** (as specified in MEF-10), i.e. ability to forward Customer L2CP frames through a Provider Network. The following types of tunneling are supported: Transparent, VLAN Tagged, Tunneling by MAC.

In This Chapter

Supported L2CP Protocols

IEEE 802.1 defines L2CP Reserved MAC addresses in a range from 01-80-C2-00-00-00 to 01-80-C2-00-00-2F. ML systems support control only on those addresses, which are already assigned by IEEE 802.1 standard of defined and working protocols: 01-80-C2-00-00-00 to 01-80-C2-00-00-0F , 01-80-C2-00-00-10 , 01-80-C2-00-00-20 to 01-80-C2-00-00-21.

All other future-use reserved MAC addresses in the range are handled as regular traffic, i.e. accepted, dropped or modified according to VLAN membership of the port and received frame format.

ML systems additionally allow control on Cisco Reserved MAC addresses per each port separately, supporting Layer 2 Cisco Frames (like PVST+, CDP, ISL) behavior control.

Initially, the ML system handles Cisco Reserved MAC addresses as a regular traffic, i.e. Cisco frames are accepted, dropped or modified according to VLAN membership of the port and received frame format. To change the behavior, and enable per ML port control over Cisco Reserved MAC addresses, change checkbox configuration on L2CP table pane.

Three dedicated MAC Addresses are handled as configured. These are:

- ISL 01-00-0C-00-00-00
- CDP 01-00-0C-CC-CC-CC
- PVST 01-00-0C-CC-CC-CD

All other MAC in "X" range will behave as regular traffic, i.e. they will be accepted, dropped or modified according to VLAN membership of the port and received frame format.

The following L2CP MAC application-protocols are supported with PEER handler:

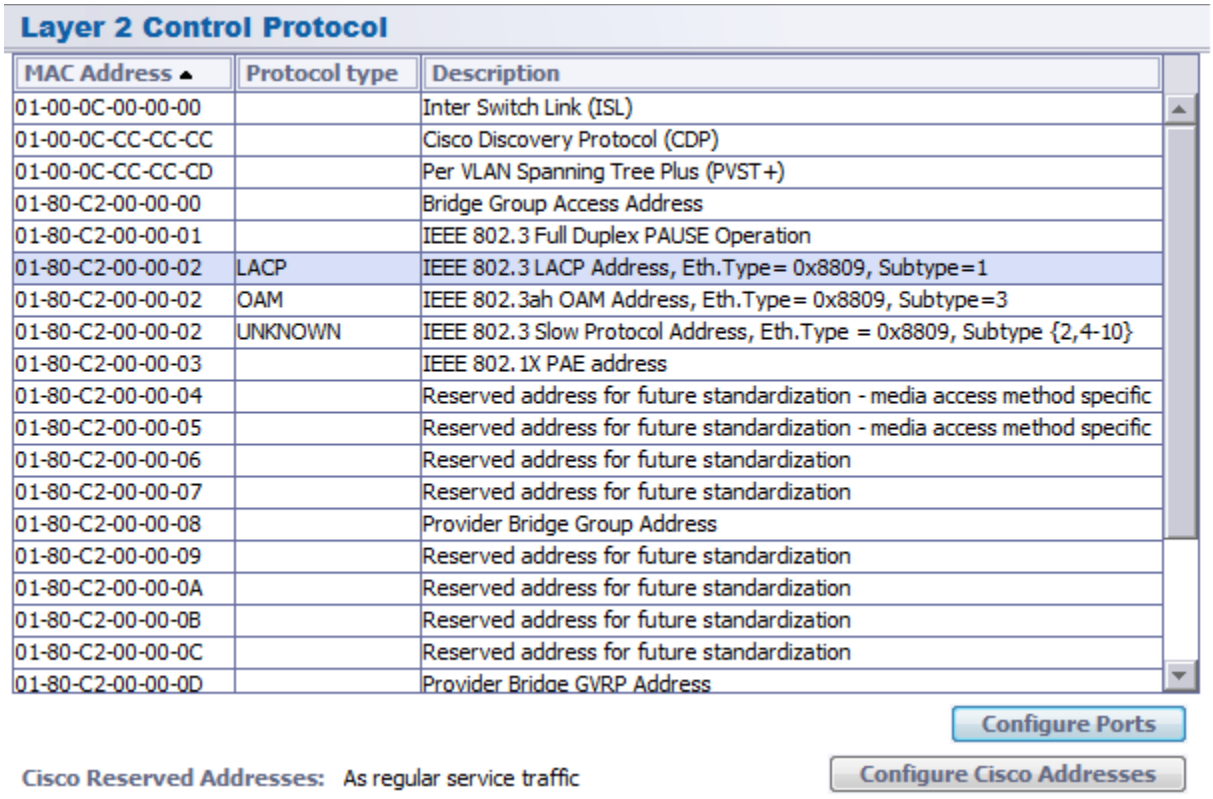
- **STP** (on page 5-20)
- OAM
- **LLDP** (on page 5-7)

Configuring Handling of L2CP Frames

➢ **To configure processing of L2CP frames**

1. In the **Network Element** tree, under **Ethernet Bridge,** select **L2CP.** The L2CP MAC Addresses pane showing the list of available L2CPs and corresponding MAC addresses appears. The list includes dedicated rows for specific L2CP MAC applications (e.g. LACP).

NOTE: Available MAC applications (protocol types) may vary according to ML model.

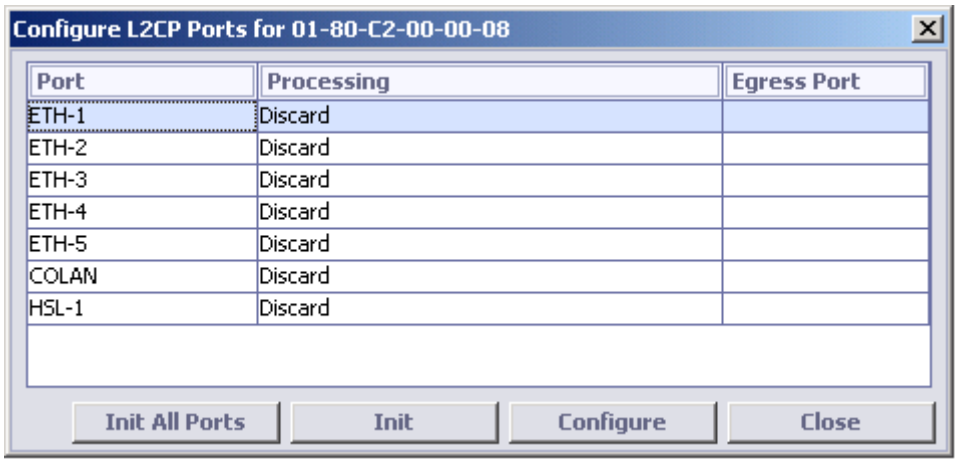


NOTE: To configure Cisco Frames behavior, click the **Configure Cisco Address** button. Choose to either Drop the frames (default) or transparently transfer the frames to specified multiple ports - regardless of the VLAN membership rules for these ports.

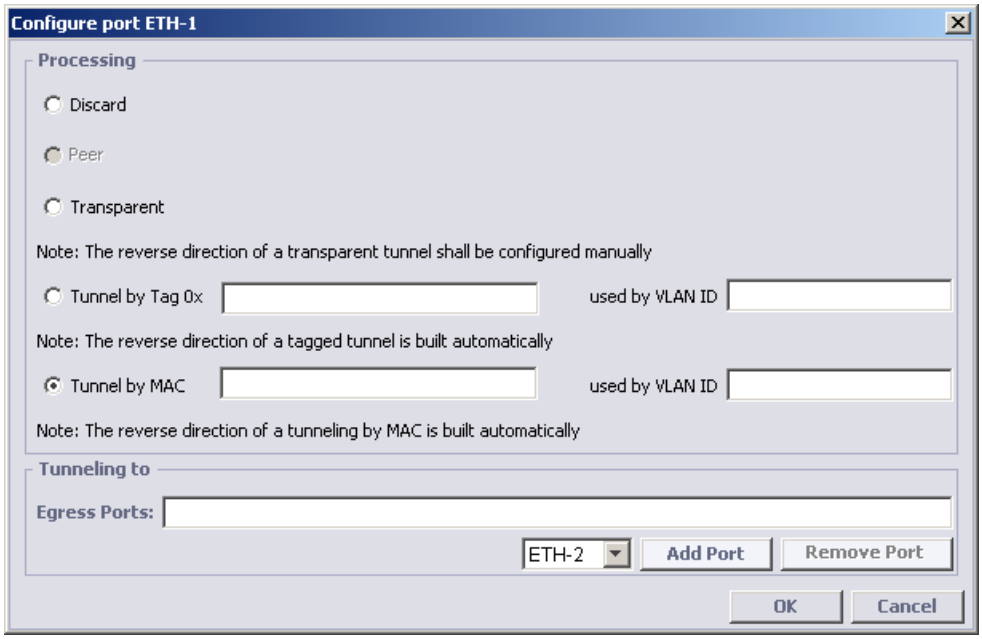
2. Select the MAC address corresponding to the protocol to be applied on the port and click **Configure Ports** at the bottom of the pane. The following dialog appears.

   The dialog shows all the ports along with the way they will process the corresponding frames and the egress ports.

NOTE: The **Init** button is used to reassign a selected port its default L2CP definitions. The **Init All Ports** button is used to assign all ports their default L2CP definitions.



3. Select the port on which the previously selected protocol will be processed and click **Configure.** The Behavior Configuration dialog appears. Note that only processing relevant to the selected protocol are enabled.



4. Select the method according to which the protocol frame will be processed:
   - **Discard** - frame will be deleted providing demarcation (security) between the customer and provider networks.
   - **Peer** - frame locally processed according to frame protocol. Requires that the ML is configured to support the application (i.e. STP, OAM, Pause Frame, etc.).
   - **Tunneling** - Tunneling passes the *customer* control frames invisibly through to the *provider's* bridge. Three types of tunneling are available: **Transparent**, **by Tag** (VID + Ethernet Type option), **by MAC** (MAC DA+VID option):

- **Transparent** - passes the customer control frames invisibly through to the provider's defined **Egress Port** without modifying the header. *Be sure tunneling is unidirectional and defined properly on either side of each link along the route.* Manually configure the reverse direction of a transparent tunnel on all ports specified as Egress Ports.
- **Tunnel by Tag Type** - tags the frame and assigns it a VLAN ID. The frame is then passed to the defined **Egress Port** and tunneled through the network as if it was a regular data frame, according to the defined Tag and VLAN ID. After reaching its destination (UNI) the tag and VLAN ID are removed. *The modifications are made only once on the CPE side. On the CO side, transparent tunneling is used.* The reverse direction of a tagged tunnel is defined automatically on all ports specified as Egress Ports.
- **Tunnel by MAC and VLAN ID** - Modifies the customer frame DST address to a configurable MAC (only unicast address can be set) and encapsulates the frame within a VLAN tag (with a configurable VLAN ID and Ethernet Type which is set according to Bridge configuration). The frame is then passed to the provider's defined **Egress Port** and tunneled through the network as if it was a regular data frame, according to the defined MAC and VLAN ID. After reaching its destination (UNI), the MAC and VLAN ID are removed. *The modifications are made only once on the CPE side. On the CO side, transparent tunneling is used.* The reverse direction of a MAC tunnel is defined automatically on all ports specified as Egress Ports.
  NOTE: When using MAC tunneling, it is important to note the following:
  a. MAC tunneling, when applied on STACKED ETH ports, works with UNTAGGED L2CP reserved frames only.
  b. MAC tunneling requires Actelis ML700 on both sides. The mechanism might not work if the MAC tunnel is not terminated by an ML NE.

5. Define the **Egress Port** (any ETH, HSL or COLAN port) via which the handled frame will be forwarded to the network as follows:
   - From the drop-down options box adjacent to the Add Port button, choose the Egress port.
   - Click **Add Port.** The selected port will be added to the Egress Port list. (To remove a port, choose the port from the list and click **Remove Port**).
   - Repeat to add another port (up to two) to the list.
6. Click **OK**.

Deployment Considerations

Special traffic (IEEE reserved multicast MAC addresses, Cisco management MAC addresses) from the customer's LAN can be tunneled through the service provider WAN without triggering L2 features (like STP) on service provider devices. This section provides several examples to illustrate the issue.

Table 40: Examples of Deployment Considerations

CASE	Description
CASE1 (on page 9-6)	Customer LAN uses Cisco equipment and Cisco's STP (but not PVST+), Provider WAN does not use STP
CASE 2 (on page 9-7)	Customer LAN uses Cisco PVST+, Provider WAN does not use STP
Case 3A (on page 9-8)	Customer uses Cisco PVST+, Provider uses IEEE 802.1 STP/RSTP or Cisco PVST+
Case 3B (on page 9-8)	Customer uses Cisco PVST+, Provider uses IEEE 802.1 STP/RSTP

Case 1

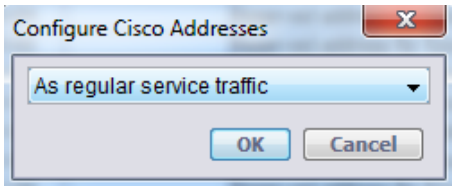
CASE1. Customer LAN uses Cisco equipment and Cisco's STP (but not PVST+), Provider WAN does not use STP

In most cases, Cisco equipment can be used in the customer's LAN without requiring complex configuration of the ML - ML default L2CP configuration is sufficient.

By default, each ML NE forwards all Cisco traffic (0x01-00-0C-**-**-** reserved for proprietary Cisco protocols such as ISL, CDP, VTP, PVST+) as regular traffic (according to VLANs membership rules configured on the NE).

➢ **To restore the default setting:**

1. In the MetaASSIST View, **L2CP pane** (on page 9-3), click the **Configure Cisco Addresses** button



2. Select **as Regular Service Traffic**, and click **OK**.
3. Repeat on all ML NEs participating in the forwarding.

NOTE: Cisco frames can be also enforcedly forwarded ignoring regular traffic VLAN rules, and using another VID dedicated for this purpose. For such deployment, use transparent tunnel (see below) on CPE and tunnel by TAG on CO.

Case-2

CASE 2. Customer LAN uses Cisco PVST+, Provider WAN does not use STP

In some customer LAN configurations, where Cisco proprietary PVST+ works as standard MSTP, it is additionally required to tunnel a standard BPDU frames (IEEE 802.1 Bridge Group Access address 0x01-80-C2-00-00-00). Such tunnel should be configured on CPE and CO ML on all Customer LAN sites using the following options:

- Build a transparent tunnel on the CPE. This tunnel will forward the frame unchanged, cut-through from Ingress to specified Egress ports, and ignore all VLAN filter, modification and forwarding rules configured on the NE. The transparent tunnel should be set on all directions – on port(s) facing Customer LAN and port(s) facing Network WAN. Repeat configuration on CPEs of all other customer site(s).
- Build a tunnel by TAG (VID and optionally ETH-Type) on CO. This tunnel will forward the frame after inserting a TAG with the specified VID and ETH-Type. The VID should be set exactly as the Service VID (representing the Customer in WAN). This will allow to merge this special frame with all other customer traffic that is forwarded toward the service provider WAN. Tunnel by TAG is set manually only on ports ingressing from Customer side (the HSL on CO).
  Note that the reverse direction of the tunnel on the same NE (ETH-x to the HSL) is built automatically (and invisible in L2CP table). Repeat configuration on COs of all other customer site(s).

Note the following:

- You can apply TAG tunnel starting CPE (not very reasonable, but possible).
- Do not use 0x8100 Eth. type if frame is tunneled via stacked ETH port.

➢ Case 3A. Customer uses Cisco PVST+, Provider uses IEEE 802.1 STP/RSTP or Cisco PVST+.

In cases when BPDU frames (MAC 0x01-80-C2-00-00-00) are common for customer and service provider devices it can be recommended to use MAC tunneling applied on CPE (requires another MAC multicast address to be used instead of MAC 0x01-80-C2-00-00-00).

When using MAC tunneling, it is important to note the following:

- *MAC tunneling, when applied on STACKED ETH ports, works with UNTAGGED L2CP reserved frames only.*
- *MAC tunneling requires units with R7.0 SW (or higher) on both sides. The mechanism mighty not work if MAC tunnel is not terminated by an ML NE.*

The following configuration is allowed only if CPE has ETH port facing the customer switches as Untagged or Tagged.

- Build a tunnel by MAC (and VID) on CPE .This tunnel will forward the frame with MAC DA modified to specified multicast address and also tagged with VID equal to one of the VID used for regular customer traffic forwarding. Tunnel by MAC is set manually only on port(s) facing Customer LAN. Note that the reverse direction of the tunnel on the same NE (HSL-1 to ETH-x) is built automatically. Repeat configuration on CPEs of all other customer site(s).

- Use regular traffic VLANs on CO. Repeat configuration on COs of all other customer site(s).

Case 3A

Case 3A. Customer uses Cisco PVST+, Provider uses IEEE 802.1 STP/RSTP or Cisco PVST+.

In cases when BPDU frames (MAC 0x01-80-C2-00-00-00) are common for customer and service provider devices it can be recommended to use MAC tunneling applied on CPE (requires another MAC multicast address to be used instead of MAC 0x01-80-C2-00-00-00).

When using MAC tunneling, it is important to note the following:

- *MAC tunneling, when applied on STACKED ETH ports, works with UNTAGGED L2CP reserved frames only.*
- *MAC tunneling requires units with R7.0 SW (or higher) on both sides. The mechanism mighty not work if MAC tunnel is not terminated by an ML NE.*

The following configuration is allowed only if CPE has ETH port facing the customer switches as Untagged or Tagged.

- Build a tunnel by MAC (and VID) on CPE .This tunnel will forward the frame with MAC DA modified to specified multicast address and also tagged with VID equal to one of the VID used for regular customer traffic forwarding. Tunnel by MAC is set manually only on port(s) facing Customer LAN. Note that the reverse direction of the tunnel on the same NE (HSL-1 to ETH-x) is built automatically. Repeat configuration on CPEs of all other customer site(s).
- Use regular traffic VLANs on CO. Repeat configuration on COs of all other customer site(s).

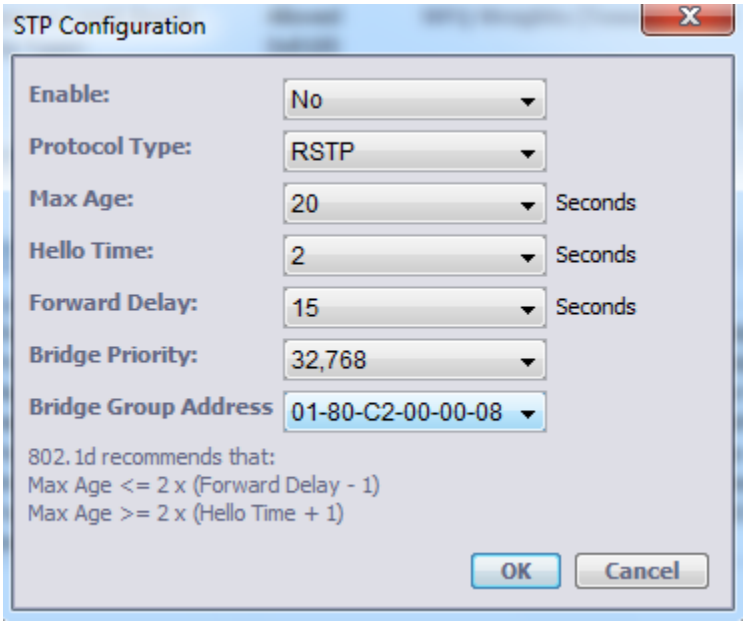
Case 3B

Case 3B. Customer uses Cisco PVST+, Provider uses IEEE 802.1 STP/RSTP

In cases when BPDU frames (MAC 0x01-80-C2-00-00-00) are common for customer and service provider devices it can be recommended to switch Service Provider network (all devices, including ML CO and even ML CPE NEs) to Provider Bridge MAC BPDU frames (MAC 0x01-80-C2-00-00-08).

1. In the MetaASSIST View, **L2CP** **pane** (on page 9-3), ensure that PEER handler is not configured on any port for MAC 0x01-80-C2-00-00-00.
2. On L2CP pane, for MAC 0x01-80-C2-00-00-08, apply PEER handler on all ports participating in the Provider Network and configure Drop handler on all Customer Facing (demarcation) ports. See **Configuring Handling of L2CP Frames** (on page 9-3) for more details.
3. On the **Ethernet Bridge** pane, click the **Configure** button in the **STP** section

4. Select **Bridge Group Address** equal to 0x01-80-C2-00-00-08 and Enable STP or RSTP.



5. Click **OK**.
6. Repeat on all ML NE participating in the service provider STP.

NOTE: As demarcation between Provider / Customer Networks has no STP/RSTP solution, ensure that ETH loops are avoided there.

10 Ethernet Service Configuration

This chapter describes how ML700 models implement Advanced Ethernet Services MEF features.

In This Chapter

Introducing MEF Terminology

EVC, EVC Service, Identification Rules, and BW Profile abstracts are used on ML NE for advanced Ethernet Services MEF features configuration.

Identification Rules handle a fundamental MEF concept of Ethernet traffic analysis; the rule inspects the frame, searching for specific values at specific offsets, according to which the Ethernet frame is identified by the Ethernet Service to which it belongs.

The filters of the identification rules consist of:

- Ingress PORT (from which the frame has arrived)
- MAC Destination or Source Addresses
- External VLAN TAG with Ethernet Type, VLANID and COS bits
- Internal VLAN TAG with Ethernet Type, VLANID and COS bits
- IP Destination or Source Address
- TOS/DSCP bits
- Transport type (L3)
- Protocol type, source and destination ports (L4)

The identification rules can also be used:

- For additional L2 Priority CoS bits remarking (CoS out)
- As a firewall - to drop frames matched with specified filter(s)

The Bandwidth Profile handles a fundamental MEF concept of Ethernet Service throughput control. A pool of up to 32 profiles can be configured on each ML device. The same BW profile can be used by various Ethernet Services, simplifying the configuration process.

On the ingress port (prior to switch decision), the total bytes length and bits-per-second is metered for each frame and it is determined whether the rate for this Ethernet Service agreement (BW profile) was exceeded.

Three meter colors are used to distinguish between Committed (agreed for transmission with guaranteed quality of service) and Excessive (allowed for transmission but with no quality guarantee) Informational rates (CIR and EIR). CIR and EIR rates are also provided with Burst Buffer Size (to allow some fluctuations of traffic rate). These are named: CBS (committed burst size) for CIR, and EBS (excessive burst size) for EIR. Traffic above CIR+EIR+CBS+EBS is dropped (policed) on ingress, avoiding switching resources usage.

On the egress port (after switch decision), each Ethernet service flow can be (optionally) shaped providing continuous un-bursty traffic transmission. The shaper rate is determined according to the assigned BW profile (as CIR + EIR), and prevents from arriving ingress bursts to be forwarded towards the next hop wire.

EVC Service handles the rest of the MEF fundamentals: a need for the Ethernet Service classification (i.e. a decision regarding the appropriate queue in which the frame will be stored prior to the transmission) and congestion avoidance control (how to schedule the queue, allowing the prioritization of one service flow versus another). EVC Service on ML NE is used for combining all of the above listed attributes:

- Identification Rule(s), identifying the EVC Service flow
- BW profile, to set throughput limits control on the EVC service flow
- Egress Class/Queue, Scheduler and Shaper

EVC (Ethernet Virtual Connection) handles a fundamental MEF concept of End-to-End Ethernet Services configuration. An EVC is an association of two or more User Network Interfaces (UNI), where the UNI is a standard Ethernet interface that is the point of demarcation between the Customer Equipment and the service provider's network.

EVC on ML NE is an abstract identification, which is not passed through the network via Ethernet Service frames, but is used as a group identifier of different local resources (specified by VLANs) used on each NE participating in the same Ethernet Service. VIDs configured on CPE and CO NE may differ (as C-VLAN and SP-VLAN), but when belonging to the same EVC, can be easily found for monitoring and management.

In addition, EVC on ML NE is a place to keep a list of all the EVC services belonging to it. This allows to easily trace multiple EVC Services (like VoIP, FTP and HTTP) of the same EVC (like "Customer A").

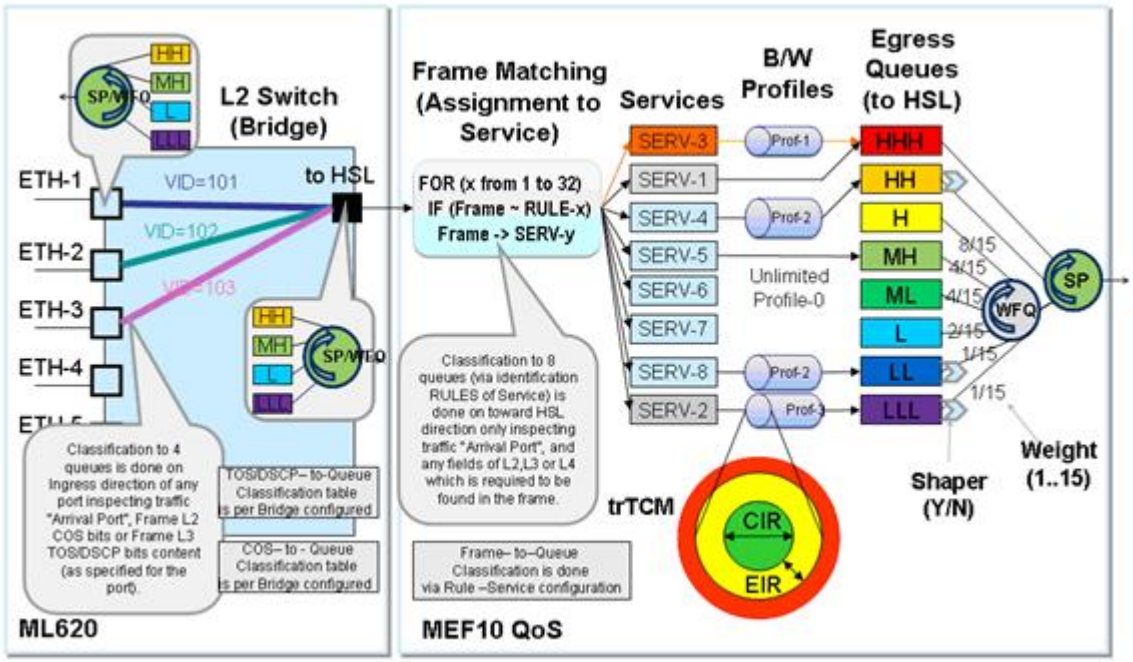
EVC, once configured through ML CO and CPE with the same EVC description (i.e. "Customer A"), can be easily retrieved in glance on all NE and per each NE.

MEF10 QoS flow Overview

MEF10 QoS handling is applied only toward HSL direction and is combined with basic Quality of Service handling. As shown below, MEF10 QoS setting do not provide Ethernet Service traffic connectivity between ports. Connectivity is provided by VLANs, which must be configured in advance.

Ethernet Service configuration flow is:

- **Define EVC** (on page 10-5) (pool up to 8)
- **Create BW profiles** (on page 10-7) (pool up to 32) – for Service Throughput limitation.
- **Define SERV** (on page 10-10) (pool of 8) with selected BW profile to apply. Assign the SERV to EVC. Up to 8 SERV can be assigned to the same EVC.
- **Define identification RULE** (on page 10-13) (pool of 32 – seven of which are internally used) with particular L2, L3, L4 flow identification. Assign the RULE to SERV. Up to 32 RULES can be assigned to the same SERV.

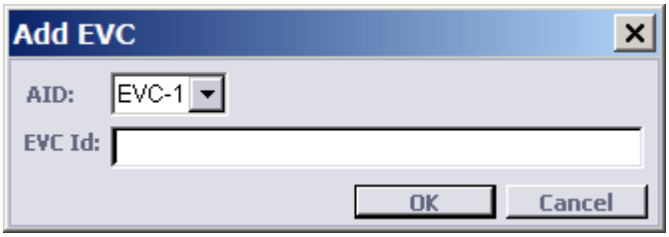


EVC Connection Definition

You may define up to eight EVC services.

➢ **To define an EVC**

1. From the Network Topology tree, under **Ethernet Services**, select **EVCs**. The EVCs pane appears. The pane lists the currently defined EVCs according to their EVC AID and EVC ID and provides EVC management functions.



2. To add an EVC:
   - Click the **Add** button at the bottom of the pane. The Add EVC dialog appears.
   - Select the relevant **EVC AID** from the list.
   - Assign the EVC AID a meaningful **EVC ID.**
   - Click **OK.** The description will be added to the EVC pane list.

NOTE: The defined EVC may be modified or deleted by selecting it and clicking the corresponding buttons at the bottom of the pane.

VLAN and EVC Mapping

Traffic VLANs can be associated with predefined EVCs when the VLAN is defined or any time afterwards using the Edit option in the VLAN configuration pane.

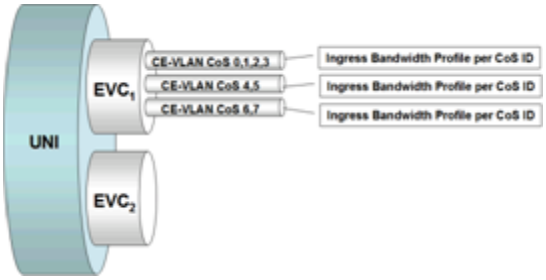
NOTE: The following steps refer only to VLAN association to EVC. For a full description of the VLAN configuration procedure, refer to Traffic VLAN Configuration.

➢ To associate a VLAN with an EVC

1. In the Network Element tree, expand **Ethernet Bridge** and select **VLANs**. The **VLANs** pane opens in the work area.
2. Invoke the configuration pane for the required VLAN using one of the following methods:
   - To add an existing VLAN to an EVC, select the VLAN row and click **Edit VLAN.**
   - To add a new VLAN to an EVC, click **Add VLAN.**
3. In the invoked Traffic VLAN pane, define the necessary parameters and select the **EVC** with which the VLAN will be associated.

BW Profile Definition

ML systems supports the bandwidth profile definition (*throughput*) for each EVC service. A single Bandwidth Profile is applied to all ingress Service Frames. In the example illustrated below, there are three services, each identified by a CoS ID of the specific CE-VLAN - each with a separate Bandwidth Profile.



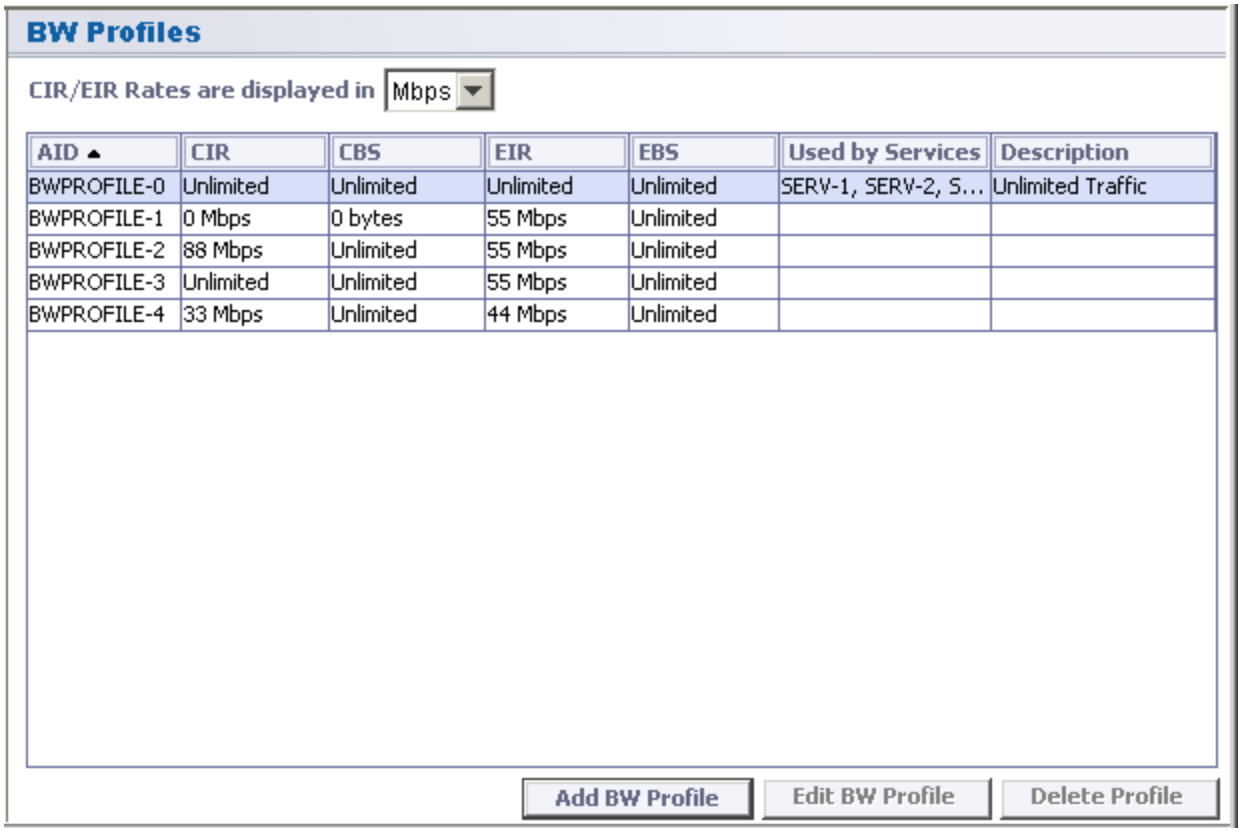
This section describes how to create a pool of bandwidth profiles (up to 32) with meaningful names. The profiles should be created according to the service provider's needs. They can then be used as part of the attributes that make up definitions for various services.

➢ To define a bandwidth profile

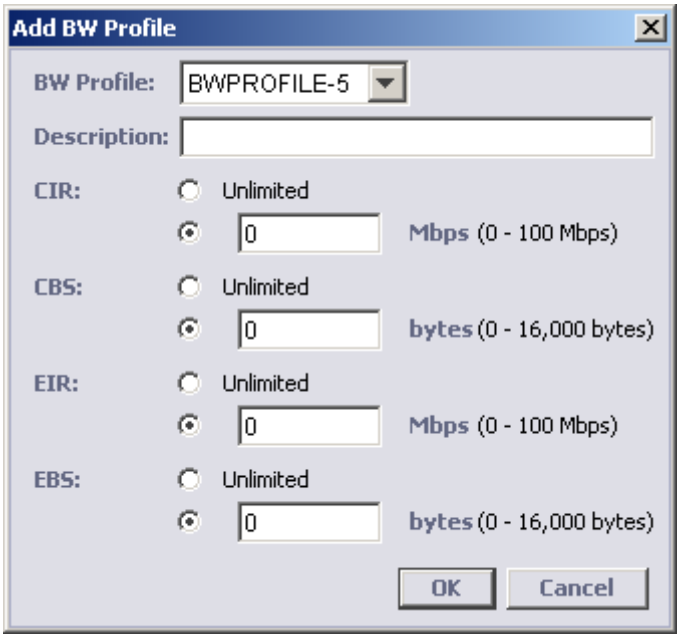
1. From the Network Element tree, under **Ethernet Services**, select **BW Profiles**. The BW Profile pane appears.

   The pane lists the currently defined pool of BW profiles (AID) along with their defined rate limits (CIR, CBS, EIR and EBS) and the services to which each profiles were assigned (Used by Services).

The operation buttons at the bottom of the pane are used to create and manage BW Profiles. Use the option 'CIR/EIR Rates are displayed in' to define the BW display units.



2. Click the **Add** button at the bottom of the **BW Profiles** pane. The Add BW Profile dialog appears.



NOTE: Ranges may vary according to ML model type.

3. Select a new BW profile AID from the list of the available (not in use) **BW Profiles**.The following BW profiles are assigned by default: BWPROFILE-0 (read-only)- reserved for the default setting of defined SERV AIDs.
4. Define the following for the profile:
   - **CIR** (Committed Information Rate) - average rate up to which service frames are delivered. All service frames are sent at the UNI speed, e.g., 10Mbps, and not at the CIR, e.g., 2Mbps.
   - **CBS** (Committed Burst Size) - the size up to which service frames may be sent and remain CIR-conformant. Range: Unlimited or up to 16,000 Bytes.
   - **EIR** (Excess Information Rate) - average rate, greater than or equal to the CIR, up to which service frames are delivered without any performance objectives.
   - **EBS** (Excess Burst Size) - the size up to which service frames may be sent and be EIR-conformant. Range: Unlimited or up to 16,000 Bytes.
5. Click **OK**. The new profile will be added to the Bandwidth Profiles list.

EVC Services Definition

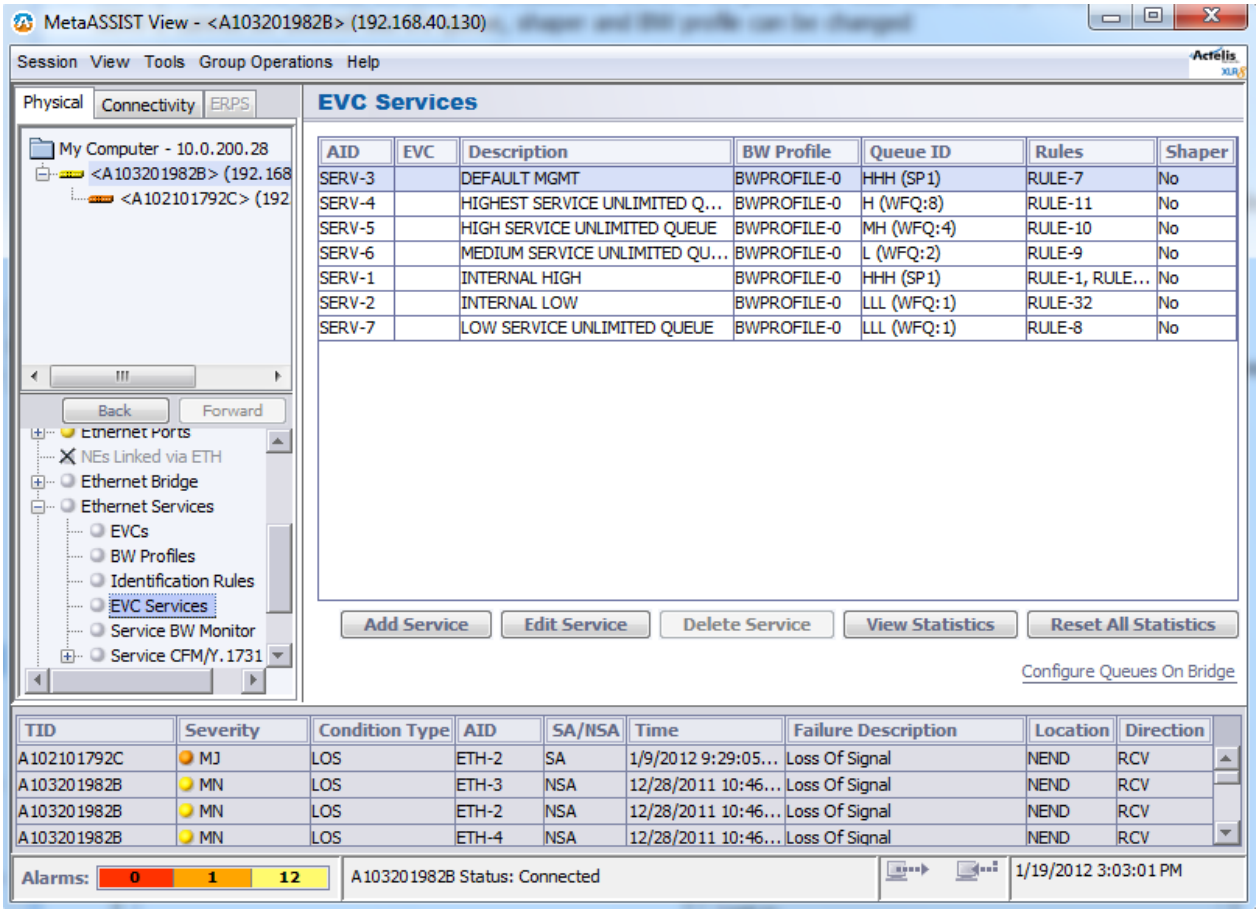
By factory default, ML700 is configured to use these services as follows:

- SERV-1 - for internal purposes, to allow L2CP and CFM features. Traffic of these features is identified using Rules-{1-6}; SERV-1 cannot be deleted but it's queue, shaper and BW profile can be changed
- SERV-2 - to set the default behavior of unclassified traffic to be passed at least with lowest priority. Traffic is identified using Rule-32. SERV-2 cannot be deleted but it's queue, shaper and BW profile can be changed
- SERV-3 – is used for default MGMT traffic and can be deleted and edited.
- SERV-4,5,6,7 – is used for default L2 COS bits classification and can be deleted and edited.

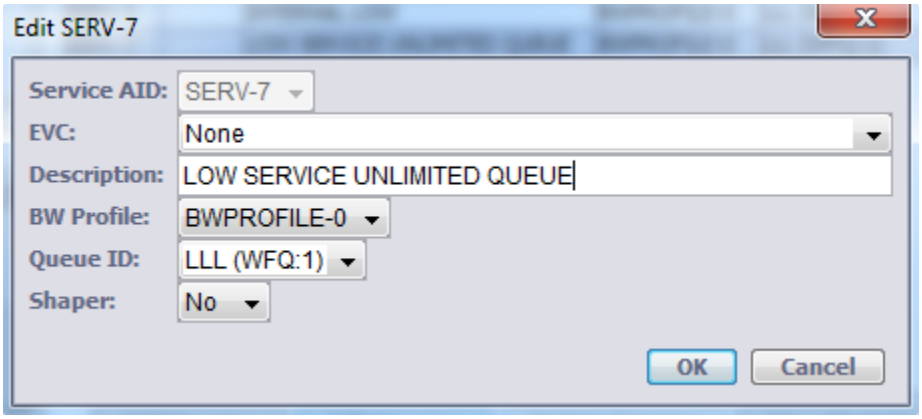
To change the default behavior of the system - i.e. all unclassified traffic – to be dropped or prioritized, use Lower Order Rule (RULE-31 and lower) to define the behavior.

➢ To define an EVC service

1. In the Network Topology tree, under **Ethernet Services** select **EVC Services**. The Services pane appears. The pane lists the currently defined services along with their attributes.



2. To add a Service, Click the **Add Service** button at the bottom of the pane. The Add Service dialog appears.



3. Select from the list of the available **Service IDs**. Up to 8 service IDs are supported (SERV-1 to SERV-8). Only the available service IDs are displayed (i.e. defined services are removed from the list).
4. In the **Description** field, assign the service a meaningful name.
5. Select from the list of predefined BW Profiles. Only defined BW profiles are displayed. If the required BW profile is not available, define it via the BW Profile option and it will be available for the service.
6. Select the **Queue ID.**
7. In the **Shaper** field, configure whether to apply shaper (Yes) or not (No) to the service as the frames egress.
   The Shaper is used to limit data transmit rate and remove data bursts. The shaper is available per queue, and when "Service per Queue" is configured, the shaper becomes a Service Shaper.
   Service Shaper rate limit is calculated automatically as the sum of CIR + EIR (specified in the **BW profile(s)** (on page 10-7) used by the Service(s) as Ingress Meter). For a Service with an enabled Shaper, it is recommended to use a BW profile which doesn't limit the CBS/EBS (should be set to unlimited), otherwise the shaper may work improperly.

   Notes:
   Shaper cannot be enabled for a Service, if the CIR and/or EIR specified in the BW profile(s) used by that Service(s) are unlimited.
   Shaper cannot be enabled for a Service, if the total sum of CIR+EIR specified for that service(s) is greater than theoretically possible on the HSL port of the ML700 model.
8. Click **OK**. The new profile will be added to the Bandwidth Profiles list.

NOTE: The defined service may be modified or deleted by selecting it and clicking the corresponding buttons at the bottom of the pane.

Identification Rules Definition

ML700 supports up to 32 identification rules. Available by factory setup (see **Appendix E - Factory Setup Content** (on page E-1)), default rules on ML700 enable forwarding tunnels for:

- Ethernet packets belong to Layer 2 Control Protocols
- Management LAN (MGMT VID=100) traffic
- Other Traffic classified by Layer 2 COS bits

The first six rules (identify reserved L2CP tunnel MAC addresses) cannot be deleted or modified.
All other rules can be modified or deleted. The last rule identifies unclassified traffic and forwards it with a lowest priority through the system.

To change the default behavior of the system, i.e. drop or prioritize all unclassified traffic, the Lower Order Rule (RULE-31 and less) should be used to define the behavior.

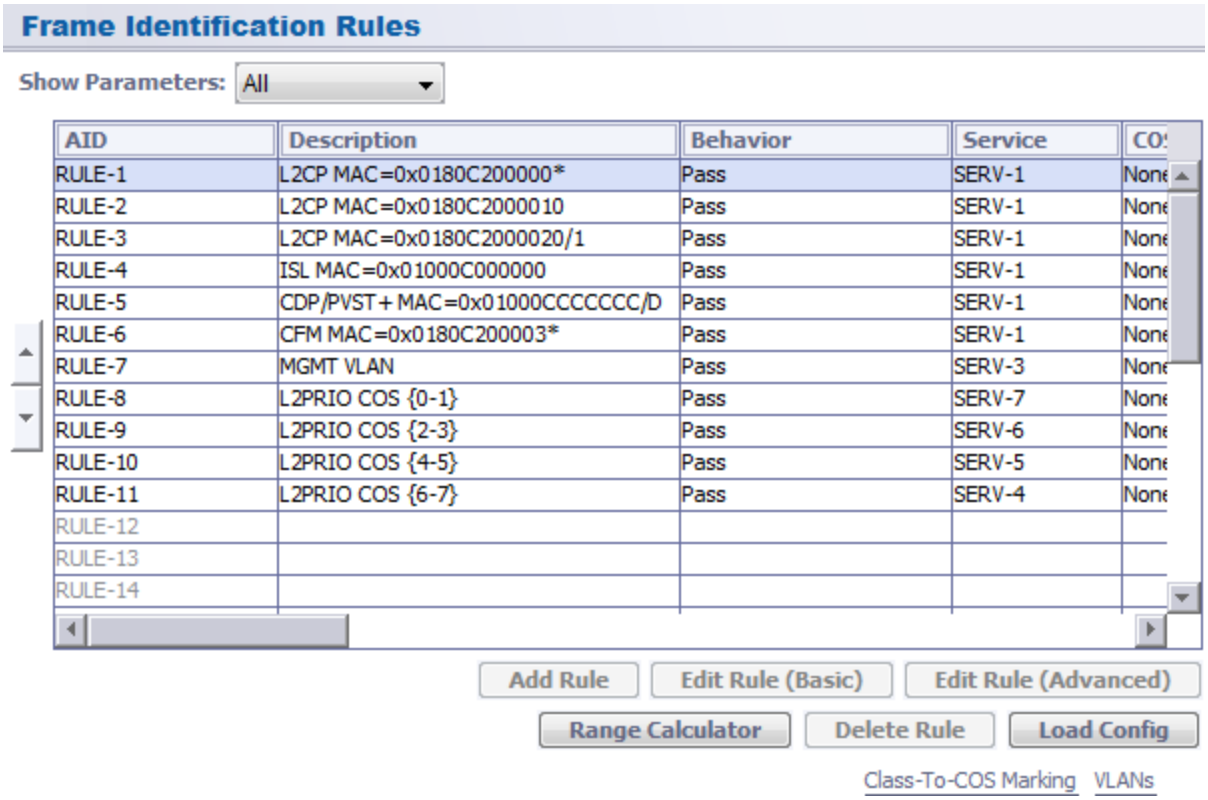
The order of the identification rules is critical due to "First Match" principle implemented for Identification Rules on the ML700 series. A new rule can be added in any of the available rows (the row number corresponds to the order of the rule). The order of configured rules (except for the first six and last rule) can be modified.

NOTE: To change the order of pre-defined rules, use the up and down arrows at the right of the rules table.

Rules can be imported (downloaded) to the ML700 from a text file consisting of TL1 configuration commands.

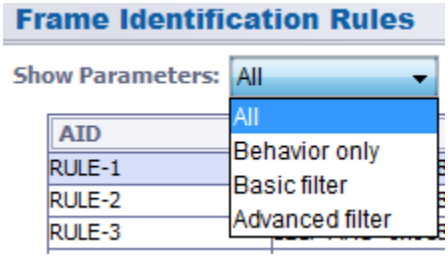
➢ To define an Identification Rule

1. In the Network Topology tree, under **Ethernet Services**, select **Identification Rules**. The Frame Identification Rules pane appears.



The pane lists the currently defined Identification Rules in a table, showing the rules' details according to a user selected filter:

- All - all rules' attributes are displayed
- behavior Only - shows only parameters defining the behavior of the packets (Description, Forwarding, Marking, Used by Services).
- Basic Filter - shows only parameters defining the rule's filters (RXPORT, EXT.VLAN VID, EXT. VLAN COS, IP DSCP/TOS).
- Advanced Filter



The pane also provides access to rule management options via the buttons at the bottom of the pane. The buttons are:

- Add Rule - used for adding a rule. This button is enabled when selecting an unused rule.

- Edit Basic Rule (see **Edit Rule (Basic)** (on page 10-16)) - used to configure the attributes of the selected rule (for rules that are modification protected, this button is grayed-out).
- Edit Complex Rule (see **Edit Rule (Advanced)** (on page 10-18)) - used to configure the attributes of the selected rule (for rules that are modification protected, this button is grayed-out).
- Range Calculator - Opens a dialog for calculating the FROM – TO ranges of an attribute (i.e. VIDs etc.) which cannot be covered by a single RULE, according to the HEX MASK limitations (see **Range Calculator Dialog** (on page 10-23) for details).
- Delete Rule - used for deleting attributes of a selected rule.
- Load Config - used to load a text file of TL1 commands that defines the rule attributes.

2. Select the relevant rule from one of the configurable rules (the **Edit Rule** buttons are enabled when an editable rule is selected).
3. Click the relevant **Edit Rule** button, to display the corresponding dialog appears.
   - **Edit Rule (Basic)** - to display a subset of the rule fields, which are relevant for basic rules (see **Edit Rule (Basic)** (on page 10-16))
   - **Edit Rule (Advanced)** - to display all available rule fields (see **Edit Rule (Advanced)** (on page 10-18))
4. Fill out the Rule fields (see details below) and click **OK**.

Edit Rule (Basic)

This option describes how to display a subset of the rule fields, which are relevant for basic rules.

➢ To Configure Basic Rules

Access the dialog according to instructions in Identification Rules Definition. The Edit Rule dialog appears.

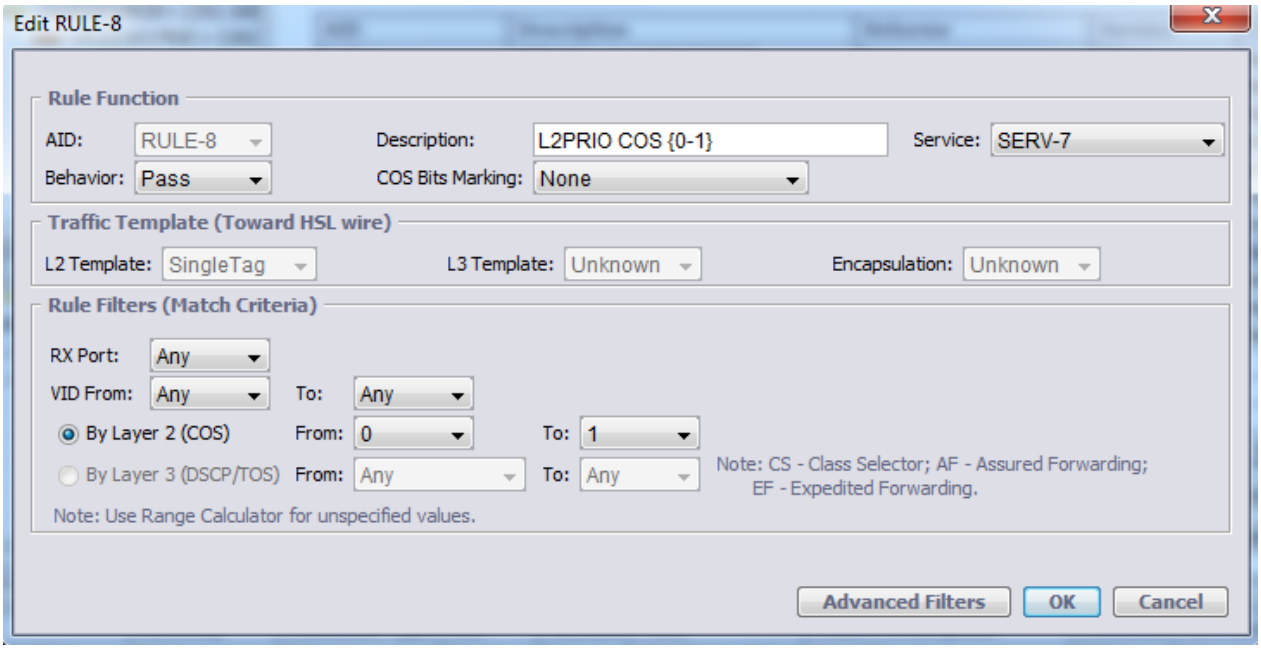


Table 41: Edit Basic Rule dialog areas

Rule Function area	**AID** - Rule AID **Description** - Rule description as it appears in the Rules pane. Can be modified. **Service** - service to which the Rule belongs (from the pool of predefined service IDs). Multiple Rules can belong to the same Service. In this case BW Ingress and Shaper definition are applied on a sum of traffic identified by these rules. *For Rules with Drop behavior - set Service ID to NONE.* **Behavior** - how to handle frames that match this rule. Values = Pass or Drop (not supported on all models) **COS bits marking:** • Class to COS Marking - COS bits of the frame will be set according to the Queue where this frame was assigned (HHH,…LLL). Classification Result (HHH , …,LLL) mapping to COS bits (0 … 7) is configurable per system. • None - no additional marking applied. This means that Original frame priority is kept - when tagged original frame pass through a port with Tagged membership defined on it). Or Port priority is assigned to the original frame - when untagged frame pass through a port with Untagged membership defined on it). Or Original frame Priority is copied to outer tag from inner tag when frame pass through a port with Stacking membership defined.

Traffic template (toward HSL wire) area	Pattern to recognize the traffic. Template *defines the offset* (relative to the frame 1-st bit start) where the traffic should be validated with the parameter values for L2, L3, L4 protocols. For a newly defined basic rule, the template is pre-defined in advance as Layer 2 Template – Single Tag and Layer 3 Template – IPv4. If traffic ingressing the ML device differs from this template (i.e. is double tagged, IPv6, or PPPoE encapsulated), use the **Advanced Rule** dialog. ML700 has some rules pre-defined with hard-coded template (as in the example above, for CESoETH). Traffic Template for such rules will appear grayed-out and cannot be changed in any (basic or advanced) dialog. • **Layer 2 Template** values - Untagged, Single tag, Double tag or unknown. • **Layer 3 Template** values - Unknown, IPv4, IPv6 • **Encapsulation** (between L2 and L3) values - Unknown, None, PPPoE
Rules Filters (Match Criteria) area	Defines the content of the rule. A frame is identified as belonging to the rule if the frame and rule content matches in all specified fields. (Correct offset of fields is determined using the template of the rule). • **Rx Port** - port to which this rule is applied. Only service Ethernet ports are supported (HSL, COLAN and LAG port are not supported). • **VID From** and **To** - Allows to fill in VLAN ID to search for match. Either explicit values or range (using BINARY mask) can be searched for match. See **Calculating the Range Covered by a Rule** (on page 10-21). • **By Layer 2 (COS) From** and **To** - Allows to fill in COS to search for match. Either explicit values or range (using BINARY mask) can be searched for match. See **Calculating the Range Covered by a Rule** (on page 10-21). • **By Layer 3 (DSCP/TOS) From** and **To** - Allows to fill in Tag Type (Eth.Type) to search for match. Either explicit values or range (using BINARY mask) can be searched for match. See **Calculating the Range Covered by a Rule** (on page 10-21). *NOTE: If the FROM and TO fields display ****, you may view the configuration by using TL1 commands, or perform reset via the MAV GUI dialog.*

Edit Rule (Advanced)

This section describes how to edit advanced rules.

➢ **To Configure Advanced Rules**

Access the dialog according to instructions in Identification Rules Definition. The Edit Rule dialog appears.

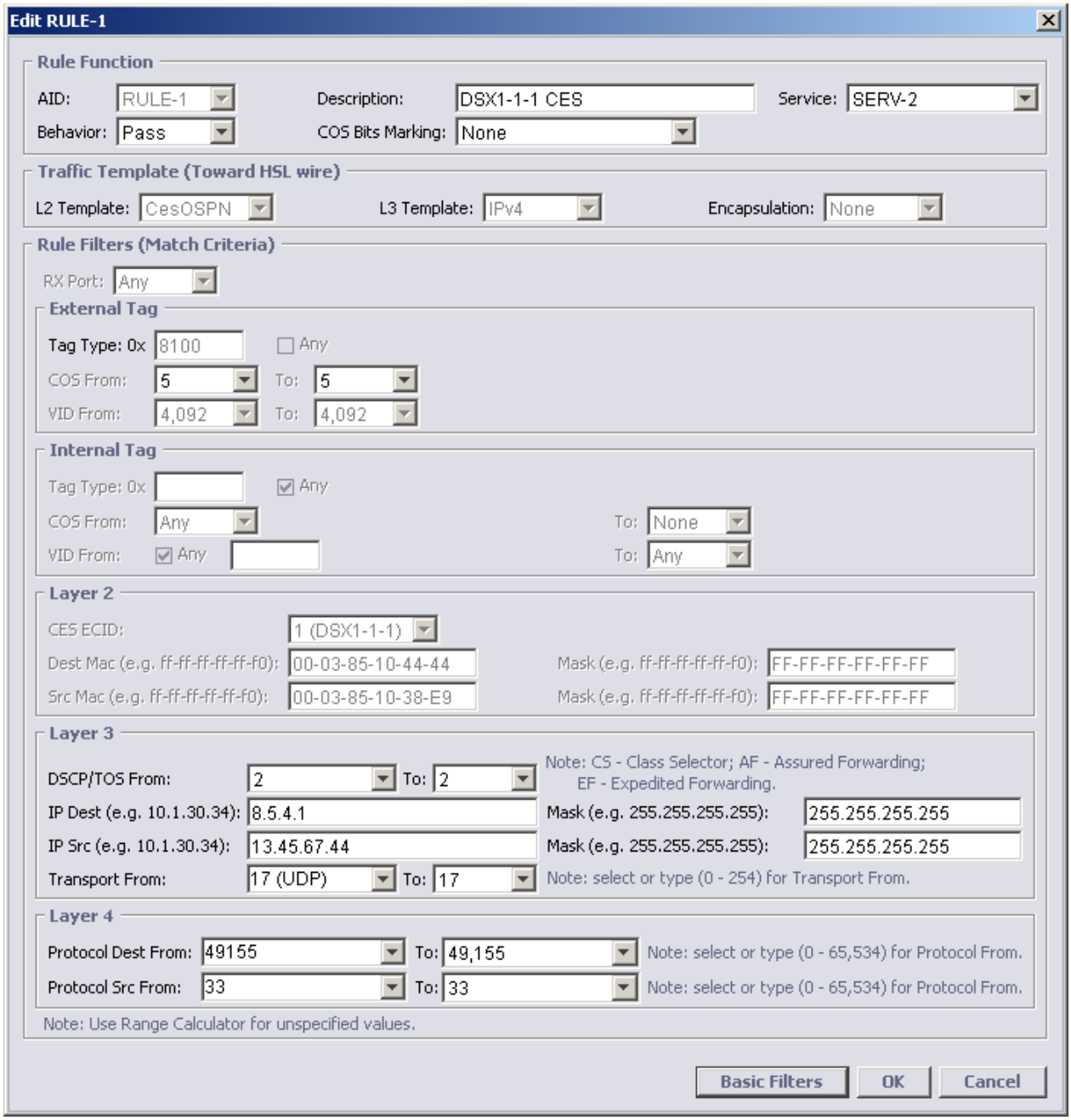


Table 42: Edit Advanced Rule Dialog Areas

Rule Function area	human-readable description and required behavior information of the current rule. The following fields are provided: **AID** - Rule AID **Description** - Rule description as appears in the Rules pane. Can be modified. **Service** - service to which the Rule belongs (from the pool of predefined service IDs). Multiple Rules can belong to the same Service. In this case BW Ingress and Shaper definition are applied on a sum of traffic identified by these rules. *For Rules with Drop behavior - set Service ID to NONE.* **Behavior** - how to handle frames that match this rule. Values = Pass or Drop (not supported on all models) **COS bits marking:** • Class to COS Marking - COS bits of the frame will be set according to the Queue where this frame was assigned (HHH,…LLL). Classification Result (HHH , …,LLL) mapping to COS bits (0 … 7) is configurable per unit. • **CoS Propagation** - no additional marking applied. Which means that Original frame priority is kept - when tagged original frame pass through a port with Tagged membership defined on it). Or Port priority is assigned to the original frame - when untagged frame pass through a port with Untagged membership defined on it). Or Original frame Priority is copied to outer tag from inner tag when frame pass through a port with Stacking membership defined. • None -sets the PBit according to the queue value (1,3,5,7).
Traffic template (toward HSL wire) area	pattern to recognize the traffic. Template *defines the offset* (relative to the frame 1-st bit start) where the traffic should be validated with the parameter values for L2, L3, L4 protocols. In this area, rule pattern is defined according to templates. These should be inspected for match. Deeper frame inspection requires more specific templates to be defined. Each rule can use its own template. For example, in case of mix traffic (expected either single or dual tagged on the same port) 2 rules should be prepared using different templates to catch all required traffic. • **Layer 2 Template** values - Untagged, Single tag, Double tag or unknown. • **Layer 3 Template** values - Unknown, IpV4, IPV6 • **Encapsulation** (between L2 and L3) values - Unknown, None, PPPoE

Rules Filters (Match Criteria) area	(**Port**, **External Tag, Internal Tag, Layer 2, Layer 3,** and **Layer 4**) - Defines the content of the rule. A frame is identified as belonging to the rule if the frame and rule content matches in all specified fields. (Correct offset of fields is determined using the template of the rule). **Rx Port** - port to which this rule is applied. Only service Ethernet ports are supported (HSL, COLAN and LAG port are not supported). • **External Tag** area - outer VLAN tag fields to inspect - available only if the selected template refers to Single or Double tag pattern. When available (depending on the selected template (Pattern)), allows to fill in outer tag VLAN ID, COS or Tag Type (Eth.Type) to search for match. Either explicit values or range (using BINARY mask) can be searched for match. See **Calculating the Range Covered by a Rule** (on page 10-21). • **Internal Tag** area - inner VLAN tag fields to inspect - only available if L2 template refers to **Double tag** pattern. When available (depending on selected template (Pattern), allows to fill in inner tag VLAN ID, COS or Tag Type (Eth.Type) to search for match. Either explicit values or range (using BINARY mask) can be searched for match. See **Calculating the Range Covered by a Rule** (on page 10-21).
Layer 2 area:	*Not supported by all models.* When selecting **CesOEth** in the L2 template field, only the Layer 2 -> **CES ECID** field is available, providing the following options: RULE-1 for DSx1-1-1 port traffic transfer, RULE-2 for DSx1-1-2, RULE-3 for DSx1-1-3, and RULE-4 for DSx1-1-4. For all other L2 templates, the Layer 2 values - Dest MAC and Src MAC fields are available. Define the Dest MAC and Src MAC to search for a match. The values can be explicit or within a HEX range. See **Calculating the Range Covered by a Rule** (on page 10-21).
Layer 3 area	IP protocol fields to inspect. These values are available only if the selected template fully defines L2 and Encapsulation (applied between L2 and L3).
Layer 4 area	Application protocol fields to inspect. These parameters are available only if the selected template fully defines L2, Encapsulation (between applied between L2 and L3), and L3 (IP V4 or IP v6). The Layer 4 area, when available (depending on the pattern selected above), allows to fill in L4 protocol value to match. Either explicit value can be searched or HEX range can be searched (in which case a mask should be specified). *NOTE: If the FROM and TO fields display ****, you may view the configuration by using TL1 commands, or perform reset via the MAV GUI dialog.*

Calculating the Range Covered by a Rule

Adding a mask to an explicit number of any field (COS, VID, TOS, etc.) selection, you can create a rule which covers a RANGE of values.

This section describes how to calculate the range covered by a rule.

NOTE: You may calculate the range using the **Range Calculator Dialog** (on page 10-23).

Note that:

- Mask bit, when set to 0 – allows both 0 and 1 bits in result,
- Mask bit, when set to 1 – requires result bit to be matched with a field value bit.

COS

Note that **COS** bit is provided in Decimal format and **Mask** is in Binary format.

The table below provides an example, how to use/convert formats for COS field

Table 43: COS

Numbering System	Field Value	Mask	Result
DEC	4	7	{4-5}
HEX	0x4	0x7	{0x4 - 0x5}
BINARY	100	110	100 - 101

VID

Note that **VID** is provided in Decimal format and **Mask** is in HEX format.

The table below provides an example, how to use/convert formats for VID field

Table 44: VID

Numbering System	Field Value	Mask	Result
DEC	16	16	{16-31}
HEX	0x10	0x10	-{0x10 - 0x1F}
BINARY	10000	10000	10000 - 11111

TOS/DSCP

Note that both **TOS/DSCP** and **Mask** fields are provided in HEX format.

Note that **TOS/DSCP** field values by DSCP standard are provided in Decimal value (0-63), using 6 bits of 8 bits in a byte (starting from the highest bits of byte). To set **TOS/DSCP** field value using HEX format, the value (e.g. PHB (per-hop-behavior) CS6 (class selector 6), covers DSCP= 48-55) should be translated to BINARY "110000" and extended with "00" (for 2 lowest bits of the byte), the result value (11000000) should be translated to HEX format (0XC0) and typed as a field value.

Table 45: TOS

Numbering System	Field Value	Mask	Result
DEC	192 : PHB = 48 (x 4) – shifted left to 2 bits = 192	224	{48 - 55}
HEX	0xC0	0xE0	-{0xC0 - 0xDF}
BINARY	11000000	11100000	11000000 - 11011111

IP Address

Note that both IP Address field and mask are in Dot Numeric (decimal) format

Table 46: IP

Numbering System	Field Value	Mask	Result
DEC	10.2.17.1	255.255.255.1	10.2.17.{0-255}
BINARY	00001010. 00000010. 00010001. 00000000	11111111. 11111111. 11111111. 00000000	00001010. 00000010. 00010001. {00000000 – 11111111}

MAC

Note that both MAC address field and mask field are in HEX format.

Table 47: MAC

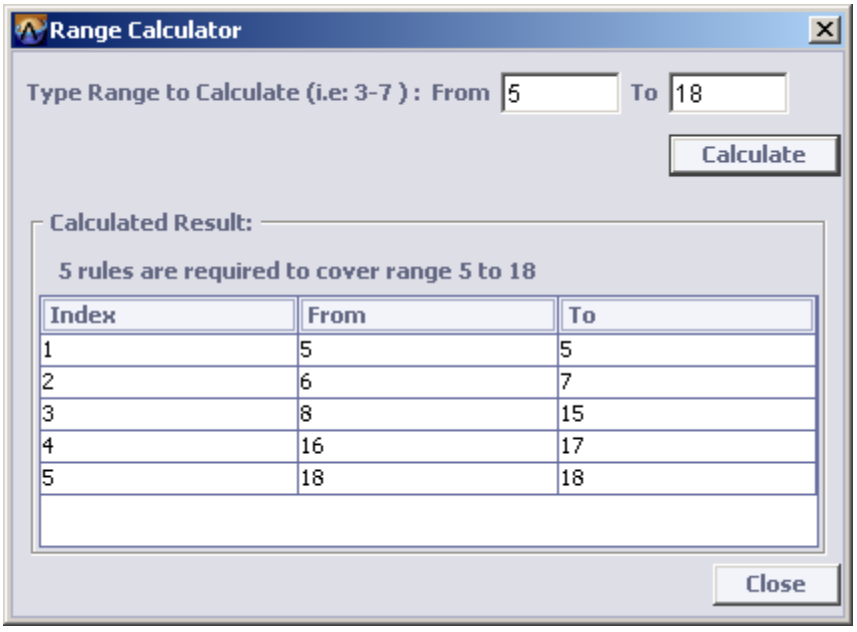
Numbering System	Field Value	Mask	Result
HEX	0x00-03-85-01-01-01	FF-FF-FF-00-00-00	00-03-85-{00-FF}-{00-FF}-{00-FF}
BINARY	00001010. 00000010. 00010001. 00000000	11111111. 11111111. 11111111. 00000000	00001010. 00000010. 00010001. {00000000 – 11111111}

Range Calculator Dialog

In order to ensure a certain range of attributes (i.e. COSs, VIDs etc.) is being covered by the applied rules, the system provides a **Range Calculator** dialog. This dialog allows calculating the FROM – TO ranges which cannot be covered by a single RULE, according to the HEX MASK limitations (see **Calculating the Range Covered by a Rule** (on page 10-21)).

➢ **To Determine the number of Rules required for covering a range of an attribute**

1. In the Network Topology tree, under **Ethernet Services**, in the **Identification Rules** pane, click the **Range Calculator** button. The Range Calculator dialog appears.



2. Type the range to be covered by the rules (In the example above the range 3-7 is being examined).
3. Click the **Calculate** button. The number of required rules, and the range covered by each of them is displayed.
4. Click **Close** to exit the dialog.

Deployment Considerations

Table 48: ML700 Deployment Considerations

Item	Description
Queues Utilization	• It is not recommended to change Management Traffic priority, in order to maintain remote management of the CPE. • The highest queue (even if handled as Strict Priority) cannot guarantee absence of disruption from other queues traffic (see QoS, **Scheduler page** (on page 7-11)). This type of guarantee can be given only if the queue is BUSY all the time, i.e. BW forwarded to this queue is equal to whole HSL BW (calibrated and then, if applicable, egress rate limited). • To reduce Management traffic disruption on TDM services traffic, it can be useful to limit Management Traffic with BW profile consists of CIR=100Kbps (can be more) and CBS=580 bytes (not less). It is recommended to use unlimited BW profile for Management Traffic in maintenance window – otherwise system administration operations (like SW, Configuration, Log files transfer) will be seriously (tens of minutes) prolonged.
BW Profiles	• Burst Size specified in BW profile should be correlated with Rate value of BW profile. Set the burst size to at least a double of max frame size. If you don't know the fame size, you can safely set the burst size to 3000 Bytes. • EIR rate value specified in BW profile is set in addition to CIR value specified (not including CIR value, as available on some network devices). • ML doesn't count IFG (Inter-Frame-Gap) and Preamble bytes as part of Ethernet Service BW. Rates specified in BW profiles are for NET Ethernet traffic (bytes of ETH frames).
Shaper Usage	• Shaper OFF helps for higher quality of traffic which is sensitive to latency and frame delay variation, i.e. the shaper OFF means that there is no additional controller which changes traffic beat pattern. • Shaper ON helps for higher utilization of Ethernet throughput (reduce re-transmission) on traffic with burst nature (like TCP). • If you disable the shaper the UDP traffic will have less delay variation and min latency, but the TCP may not utilize all the available B/W. Some UDP traffic (e.g. video) is not that sensitive to latency and PDV, so I would recommend enabling the shaper in this case (mix of video and TCP). • In configurations, where the same priority queue is used for different (TCP and UDP) Service types, generally it is recommended to set shaper OFF. In case of some UDP traffic (e.g. video) which is not that sensitive to latency and PDV, shaper can be enabled definitely improving TCP session throughput.
Scheduler Usage	• The weights of HSL WFP queues (1..15) are configured individually on each queue. To recalculate this presentation to the % relative ratio between queues (as available on some network devices), consider the following example. • The total sum of all weights is 100% of HSL Egress B/W minus the traffic via SP queues. • If HSL B/W is 10Mbps and traffic via SP queues is rate limited to 2Mbps, this leaves 8Mbps for the WFQ queues. In Factory Default configuration the weights of the queues are distributed as 1:1:2:2:4:8. The sum of weights is 1+1+2+2+4+8=18, which constitutes 100% of 8Mbps, making the weights in % as: 5.6% : 5.6% : 11.1% : 11.1% : 22.2% : 44.4%.

11 Ethernet Operation, Administration and Management

Actelis ML systems support Ethernet OAM (operations, administration and management) capabilities as implemented by standards *802.1ag* and *Y.1731*. Only one of the standards can be activated at a time, where each of the standards supports different types of capabilities: 802.1ag and Y.1731 standards are both used to confirm and isolate faults at the port level, EVC and application level. In addition, to all 802.1ag capabilities, Y.1731 monitoring and performance standard provides QoS monitoring for key service level agreements criteria including jitter, latency and packet loss.

This section provides a brief description of how each of the standards is implemented in the ML, how it is configured and the monitoring options. 802.3ah Link Layer OAM descriptions are provided in 802.3ah Ethernet OAM Tools.

In This Chapter

802.1ag CFM

The connectivity fault management (CFM) functionality of the end-to-end network is divided into hierarchical management spaces referred to as **Maintenance Domains.** There are three Maintenance Domain levels: Operator, Service Provider and Customer. The hierarchical relationship is based on numerically assigned values from 0 to 7 that correspond to the levels - Operator level being the lowest (lower numbers) and Customer being the highest. The operator domain usually refers to a partner carrier network accommodating end-to-end links that involve a number of intermediate service providers for transport.

Domains are demarcated by Maintenance End Points (**MEPs)**. These generate and manage end-to-end sessions. The MEPs receive OAM information via Maintenance Intermediate Points (**MIPs**). MIPs also provide troubleshooting information for fault isolation. All MEPs belonging to a common service or provider are grouped under common entity: Maintenance Association (**MA**).

802.1ag OAM Configuration Overview

All NEs should be configured to operate using the same standard (802.1ag or Y.1731).

➢ **To configure the NE performing by 802.1ag standard perform the following procedure:**

1. Enable the 802.1ag OAM option on the ML unit.
2. Configure the Maintenance Domains.
3. Allocate the MIPs that comprise each Maintenance Domain.
4. Select the Maintenance Associations in each domain.
5. For each Maintenance Association, configure the defining MEPs.

Setting ML to Operate with 802.1ag

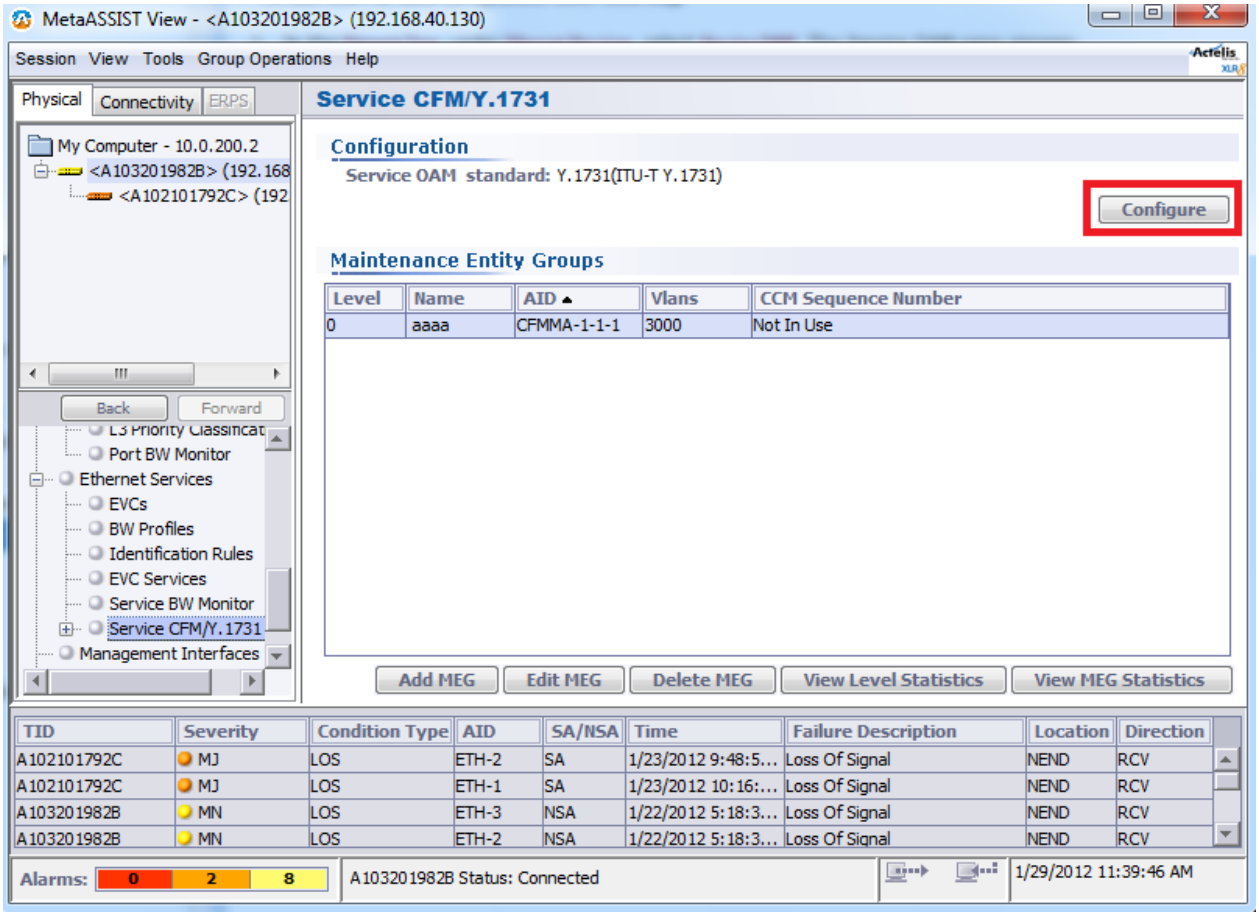
Begin by setting the ML unit to operate with the 802.1ag standard. All the relevant options will become available.

NOTE: Refer to **802.1ag OAM Configuration Overview** (on page 11-2) for an overview of the complete configuration procedure.

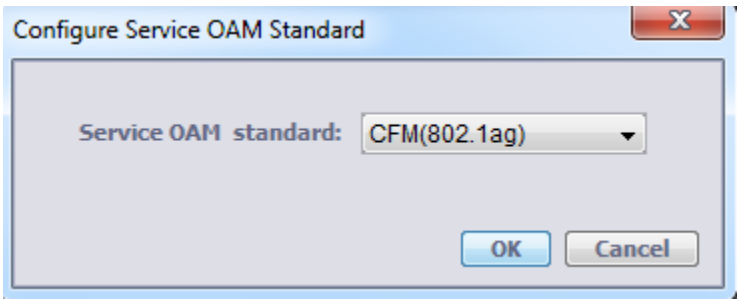
➢ **To set the ML unit to operate with 802.1ag**

1. In the **Element Tree,** under **Ethernet Services**, select **Service CFM.** The Service CFM pane appears.

2. Under **Service OAM Standard,** click the **Configuration** button. The Ethernet OAM Standard dialog appears.



3. Select **CFM (802.1ag)** and click **OK**. The relevant options will be available.



802.1ag Domain Definition

A CFM maintenance domain is a management space defined by a set of ports that make up the internal boundary of the domain (MEPs). Each domain is owned and managed by a single entity (single service provider or network operator).

Labeling domains:

Domains are labeled by their name and categorized by one of eight (0 to 7) maintenance levels.

The maintenance levels usually correspond to their relative size and hierarchy (higher level for larger domains). Core Network operator, for example, may have smaller domains - labeled 0 to 4, while service providers (responsible for Peripheral Network - Access and Concentrator devices beyond the Core Network) usually have larger domains - labeled 5 to 7.

ML devices currently allow up to four different domains sizes to be used. Domains with the same (lower - i.e. Level 2) level can be nested in a single (higher level - i.e. 4) domain and monitored as a group. This can be used by service providers to monitor a number of smaller operators under their contract

Domain structure:

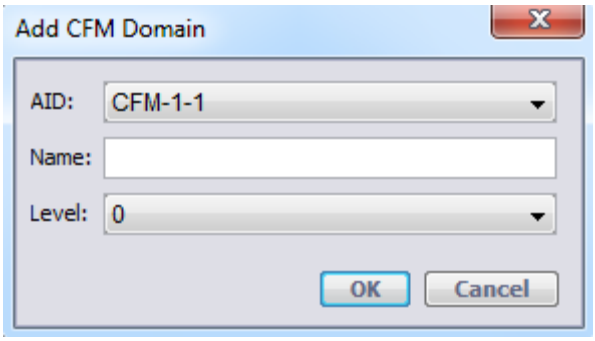
Since each domain can only be managed by a single entity, domains cannot intersect or overlap. Domains can touch and nest. When touching, the relay side (Switch) of an ML device link may belong to one domain while the wired side (Port) can belong to another domain. Nesting domains, enables a larger (i.e. service provider) domain to include smaller domains (i.e. several service operators that have a contract with the same provider).

Note the following:

- The numbers of domains per system may vary according to the ML models.
- CFM Domain Instance Names/Level cannot be edited, DLT/ENT should be used instead. All associated data should be deleted prior to Delete.

➢ To create management domains

1. In the **Network Element** tree, select **Service CFM** and in the **Domains** area of the displayed pane, click **Add Domain.** The following dialog appears.



2. In the **AID** field, select the corresponding CFM AID.
3. In the **Name** field, type the name assigned to the domain.
4. Select the domain **Level.**

5. Click **OK**. The domain will be listed in the CFM Domain pane and in the Network Element tree under Service OAM.
6. Define Domain MIPs and MEPs according to the following section.

802.1ag MIP Definitions

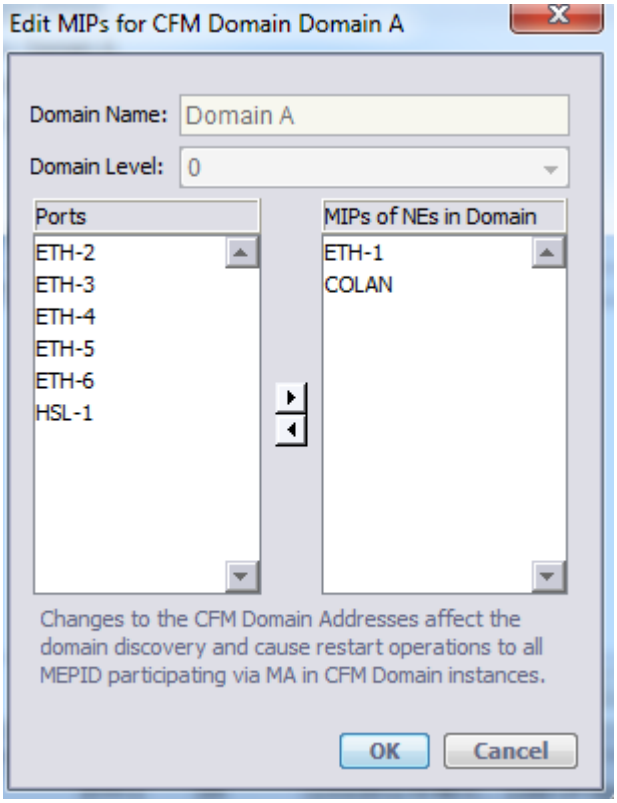
CFM Maintenance Intermediate Point (MIP) is a port which forwards CFM frames identified by an equal or higher level and drops lower level, regardless of whether they are received from the relay (Switch) or wire (Port) side.

MIP responds to CFM Loopback (unicast) and CFM Link Trace (multicast) messages of the CFM Domain to which MIP belongs (identified by domain name and level in a message).

If MIPs are not configured on a device, CFM frames are forwarded on port according to VLAN rules.

➢ To define the domain MIPs

1. Invoke the pane of the domain whose MIPs are to be defined by doing one of the following:
   - In the **Network Element** tree, under **Service CFM,** select the relevant domain.
   - In the **Network Element** tree, select **Service CFM** and double-click on the defined domain.
2. In the **CFM Domain** pane, Configuration area, the currently defined MIPs for the selected domain are displayed (e.g. ETH-1, COLAN etc.). To add or modify the defined MIPs, click the **Edit MIPs** button. The following dialog appears.



3. Under **Ports,** select the MIPs (or MIPs) participating in the domain and use the arrows to allocated them to the domain or remove them from this domain.
4. Click **OK**. The new definitions appears in the CFM Domain pane, MIPs area.
5. Define MAs according to the following section.

802.1ag MA Definitions

A Maintenance Association (MA) accounts for all MEPs from a common service or provider. An MA can be defined according to a user assigned name (string of characters) or by selecting a VLAN ID.

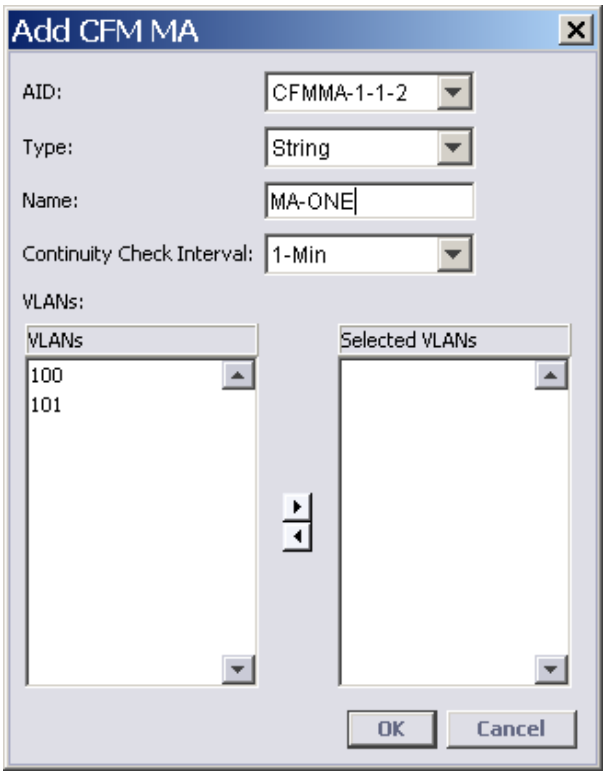
Note the following:

- Each CFM Domain Instance allows configuration of up to 256 Maintenance Associations.
- Each Maintenance Association allows a list of up to 16 VLANs in MA.
- Up to 64 MA can be monitored using a one sec CCM interval (minimal). Other MEPs can be monitored as part of a 10 sec interval.
- CFM Maintenance Association content cannot be edited, DLT/ENT should be used instead. All associated data should be deleted prior to Delete.
- Up to 256 Maintenance Associations can be configured for each domain.

➢ To define a CFM Maintenance Association

1. Invoke the pane of the domain whose MAs are to be defined by doing one of the following:
   - In the **Network Element** tree, under **Service CFM,** select the relevant domain.
   - In the **Network Element** tree, select **Service CFM** and double-click on the defined domain.

2. In the **CFM Domain** pane, **Associated MAs** area, click **Add MA.** The following dialog appears.



3. Select the **Type** as one of the following:
   - String - and assign a user defined name
   - PVID - enter the VLAN ID
4. In the **Name** field, enter a recognizable CFM MA name. The MA name is a VLAN number that should represent the group of services (VLANs).
5. Select the **Continuity Check Interval** from the drop-down list. CCM is multicast heartbeat messages exchanged periodically between MEPs that allow MEPs to discover other MEPs within a domain and allow MIPs to discover MEPs.

   Choose the interval according to the following criteria:
   - A lower interval takes up more bandwidth resources on one hand and reduces monitoring feedback on the other. Choose a value that will not overload your band while providing the required monitoring.
   - Up to 64 MA can be configured with 1 sec interval, the remaining MAs (up to 256 MAs per domain) can be configured with 10 or 60 sec intervals.
6. Assign the NEs by selecting an NE from the **Available NEs** list and clicking the > (right arrow) button. The NE will be displayed under the **Participating NEs** list.

   NOTE: To remove an NE from the Participating NEs list, select the NE and click the < (left-arrow) button.
7. Click **OK**. The CFM MA will be displayed under the applicable Domain in the CFM Navigation tree.

802.1ag MEP Definitions

Maintenance End Points (MEPs) define the boundaries of the corresponding MA. MEPs are specific ports interfaces located on the wired side of the domain. Each MEP is identified by its NE, VLAN and, Port, direction and assigned attributes. Each MEP is configured by defining its boundaries. (The MEP CCM messages can be configured as well).

After configuring a MEP, it is added to the CFM navigation tree. Selecting the item invokes a graphical display showing the MEP connections and providing access to additional tabs showing MEP parameters.

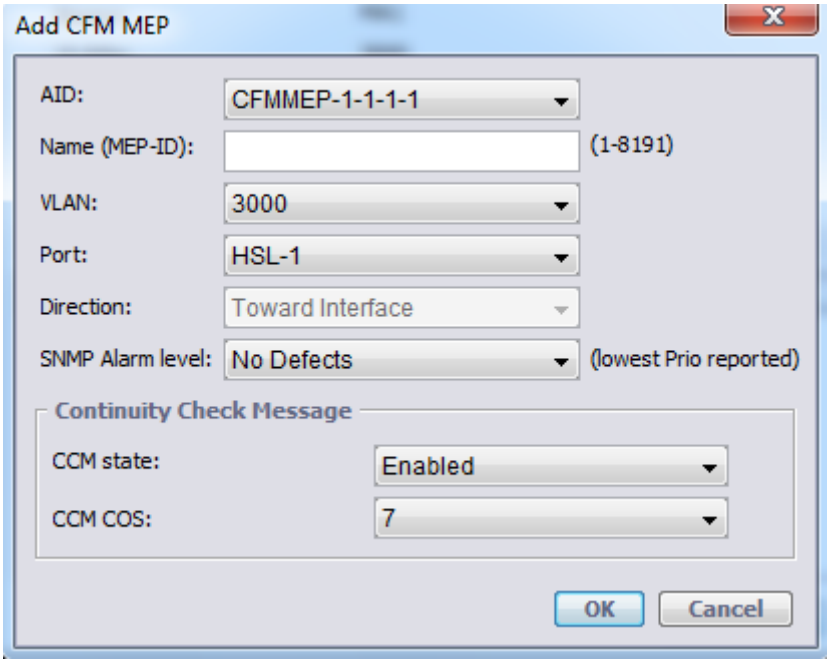
Note the following:

- Up to 16 VLANs and up to 512 MEP IDs can be configured per Maintenance Association.
- Maximum number of MEPs per NE (not per CFM Domain): SDU-400 = 512 MEPs max; ML700 = 64 MEPs max
- MEP is supported only on tagged/untagged ports (not stacked) in Down (towards wire) direction only.
- MEP cannot be set on a LAG.
- A maximal number of 5 Remote MEPs can be registered per MEP on each NE. Discovered RMEPs are not aged (i.e. when 5 RMEP are registered by MEP, newly discovered in network RMEP will be invisible.
- To refresh the data, MEP should be restarted (not service affecting).

➢ To add a MEP to a defined MA

1. In the **Network Element** tree, under **CFM**, select the relevant *Domain Name,* and choose the relevant *MA.* The corresponding pane is invoked.

2. In the **Maintenance Association (MA)** pane, **Associated MEPs** area, click **Add MEPs.** The **Add CFM MEP** dialog appears.



3. Assign the MEP ID: Range = 1 to 8191
4. Specify the MEP as follows:
   - Select the relevant VLAN from the **Primary VID** drop-down list. The ports associated with the selected VLAN will be listed in the Port drop-down list.
   - Select the port (on the wired - external side) to be associated with the defined MEP. The Direction will be displayed.
5. Select the **Lowest Priority Alarms -** the lowest priority level that will be assigned to a message processed by this MEP. Default: No defects
6. To enable Continuity Check Messages for the MEP:
   - Set the **CCM (Continuity Check) State** to **Active**.
   - Select the **CCM COS Priority** (0 to 7) assigned to CCM packets in the MEP.
7. Click **OK** to end the procedure.

CFM MEP Monitoring and Analysis Tools

ML devices support several EFM mechanisms used for locating the source and cause of network failures. These mechanisms operate using the capabilities provided by VLAN endpoints **configured as MEPs** (on page 11-8) (required part of the provisioning procedure). MEPs are able to originate ping (loopback) trace packets, and support continuity-check and cross-check functionalities. These Layer-2 mechanisms are used for troubleshooting faults of a customer service level.

The *continuity-check mechanism* can be used to determine which EVCs are impacted so the service provider can identify the downed customer services. The operator can verify the loss of connectivity using *CFM loopback (on page 11-12) (ping),* and locate the connection failure using *CFM link trace* (on page 11-14). The problem can then be further diagnosed and remedied. Finally, *CFM loopback* may be used to verify that the remedial action has succeeded and that the service has been re-established.

The test options are available on the **MEP Pane** (on page 11-11). This section describes the 802.1ag analysis tools. Note the list of limitations that should be taken into account for various types of MLs.

➢ **802.1ag supports the following analysis tools**

NOTE: CFM MIB SNMP notifications are sent in a regular “SNMPv2 over UDP over IP over ETH” way, a new transport “SNMP over ETH”, defined in IEEE802.1ag, is unsupported.

- **Continuity Check Messages (CCM) -** these are Multicast heartbeat message(s) that are exchanged periodically between MEPs. CCM enables MEP to discover other (remote) MEPs within a (CFM) domain. In addition, CCMs allow detection of configuration mismatch in an MA (802.1ag) or MEG (Y.1731) and remote MEP defect indication (RDI).

  An RDI signal is sent by MEPs that do not receive a CCM from a discovered Remote MEP during "RMEP self-defined interval" x 3.5. The RDI signal received from the Remote MEP is immediately reported (by the ML) as a RDI alarm on MEP AID via TL1 or as dot1cfmFaultAlarm trap via SNMP.
- **Linktrace messages** (on page 11-14)
- **Loopback Messages** (on page 11-12)

Limitations

- ML aggregated switch specific: CFM Traffic is dropped when passing through Ethernet Ports configured with stacked membership. In such deployments, in order to pass the ML230/ML2300 device transparently, no CFM domains shall be configured on the NE.
- ML50 specific: When configured as CPE, ML50 passes transparently CFM PDU received on the port only if Stacked VLAN is configured on this port. In all other configurations CFM PDU received on a port will be dropped if found as not matching to ETH type configured by ED-BRIDGE on ML50.

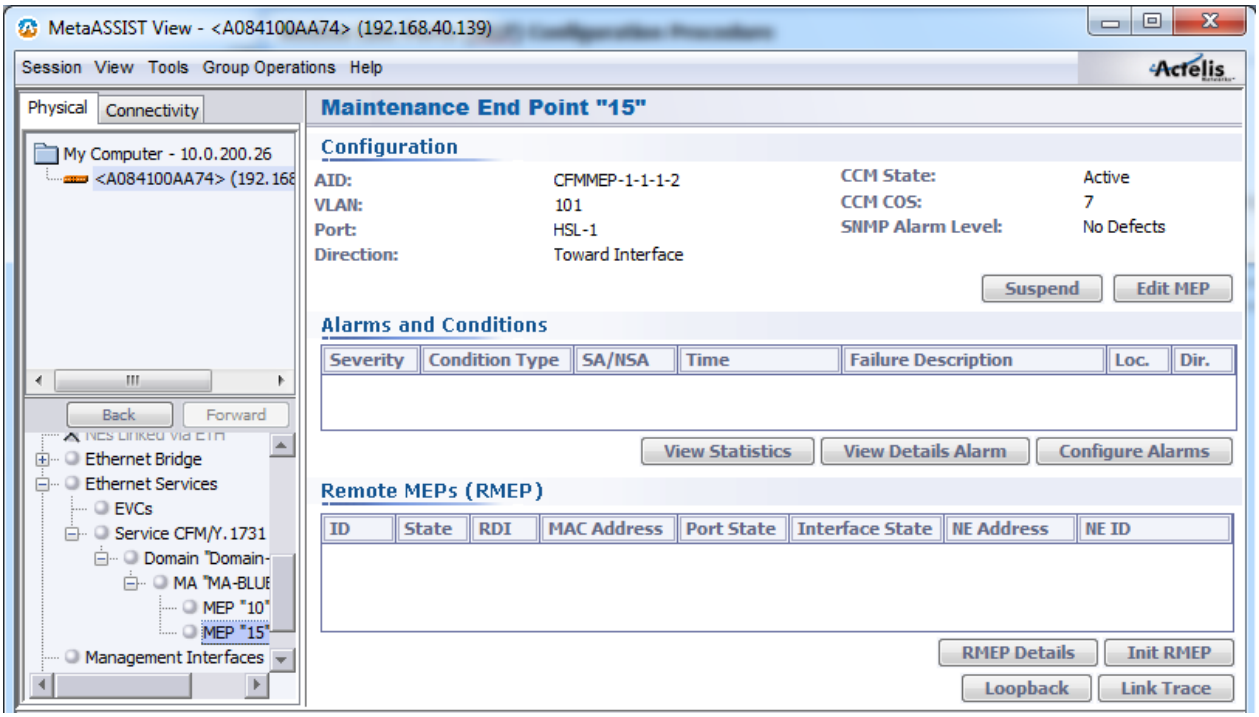
- ML700 specific: CFM Traffic of a layer lower than the lowest CFM Domain defined on NE is not dropped (as required by the standard) but behaves as a regular service traffic (dropped or passed as is or passed with VLAN encapsulation) depending on Port VLAN membership where CFM traffic appears.

CFM MEP Pane

The MEP pane provides general information, analysis and troubleshooting options relevant for the selected MEP.

➢ To invoke the MEP Pane

In the **Network Element** tree, under **Service CFM,** select the relevant MEP. The MEP pane is invoked. The MEP pane provides the MEP configuration and analysis options.



The pane is divided and pane contains the following areas:

- Configuration - shows the current parameter definitions and provides access to suspending the MEP operation (**Suspend**) and editing the MEP Configuration dialog (**Edit MEP)** (on page 11-22).
- Alarms and Conditions - shows the current alarms for the MEP and provides access to the following options:
  - View Statistics - displays the PDU Tx and Rx frame statistics.
  - View Details Alarm - displays information on alarms if such appear.
  - **Configure Alarms** (on page 13-9) - used to modify severity levels of individual alarms or to disable alarms.

- RMEPs - a list of up to *five remote* MEPs (in the MA) is displayed. Basic information on each MEP is provided in the displayed table.

Table 49: RMEP Control options

Click...	To...
RMEP Details	Show more information on a selected RMEP.
Init RMEP	Refresh the RMEP discovery process.
Loopback	Ping a selected RMEP according to the parameters defined in the invoked dialog.
Link Trace	Trace the path to a selected RMEP according to the parameters defined in the invoked dialog.

CFM Loopback

CFM loopback can be used by the operator to verify connectivity (ping). The test consists of Unicast frames transmitted by a MEP at administrator request to verify connectivity to a particular maintenance point, indicating if a destination is reachable.

A CFM loopback message is similar to an Internet Control Message Protocol (ICMP) ping message; however, the CFM loopback message cannot pass through L3 switching (Routers) devices, making the operation relevant only for L2 switching (Bridges) network.

NOTE: CFM loopback is dedicated for connectivity fault isolation and for SLA performance monitoring

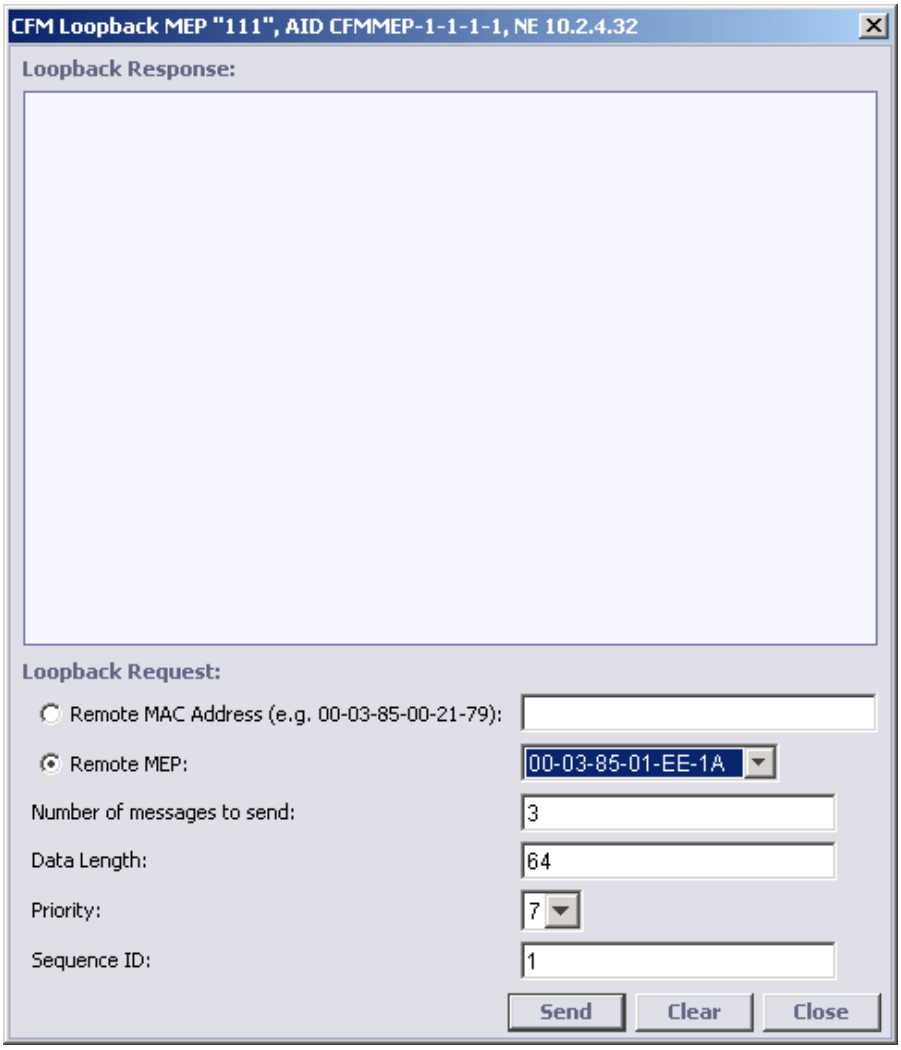
The Waiting interval between two loopback messages transmitted in series is set to 1 sec and the timeout to report loopback failure is set to 5 sec. These options are *not* configurable. Other attributes such as number of messages sequentially sent, length of data, etc. are user configurable.

A total of 10 Loopback operations can be simultaneously executed from the same NE.

➢ To configure and run CFM Loopback

1. In the **Network Element** tree, under **Service CFM,** select the relevant MEP. The MEP pane is invoked.

2. Under **Remote MEPs (RMEP),** select **Loopback. The** following dialog appears.



3. Set the MAC address to which the loopback will be performed - this is the unicast address of the remote device. Set the address using one of the following options:
   - Remote MAC Address - type the address
   - Remote MEP - select from the list of addresses discovered during CCM remote MEP.
4. Define the attributes of the data to be sent:
   - Number of messages to send - number of CFM LPBK frames to be sent in series. Range 1 to 100
   - Data length - CFM Loopback Message Frame Payload (without CFM header). Range 1 to 1500
   - Priority - L2 COS bits of CFM LPBK frame to send. Range 0 to 8
   - Sequence ID - number applied to each CFM LPBK frame. Uniquely identifies the series.

NOTE: Click **Clear** to clear the configured definitions.

5. Click **Send**. If connectivity is available (at some level), the returned message will be displayed. The quality of the message can be induced from the response.

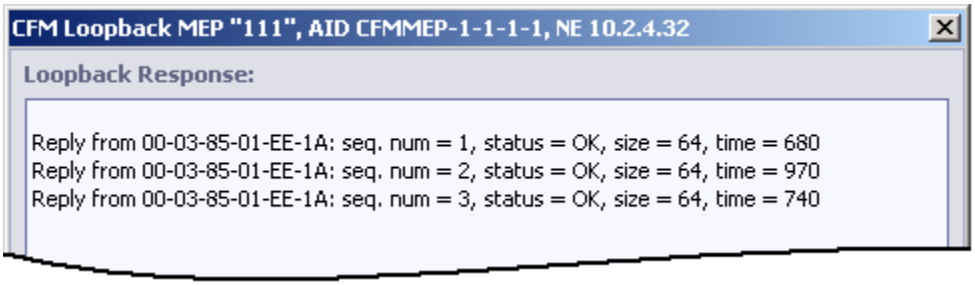


Table 50: Loopback Tab buttons

Click...	To...
Clear	clear currently displayed data.
Save As...	save the test results to a user defined text file
Stop	stop the test
Close	close the tab

CFM Link Trace

Link trace is used to locate a connection failure by following a path (tracing a link) between the local MEP and a destination MEP (or any other Unicast destination). This is implemented by the CFM link trace message - a multicast message which requests all CFM domain participants (MEP and all MIPs along the path) to respond and forward (re-build) the request. The report used for analyzing the connectivity for the path includes a list of all the domains through which a message would need to pass, along with their current status, link type, address, etc. The messages are forwarded only through the active topology (on ETH ports which are considered as Traffic Forwarding by STP/RSTP, when enabled).

Timeout of error messages is not displayed; the successful result should be found manually by analyzing the Terminal MEP = MEP and Rx Flag = 0 (which means the MEP destination was achieved) or by Rx Flag = 0 only (which means the addressed MIP destination was achieved).

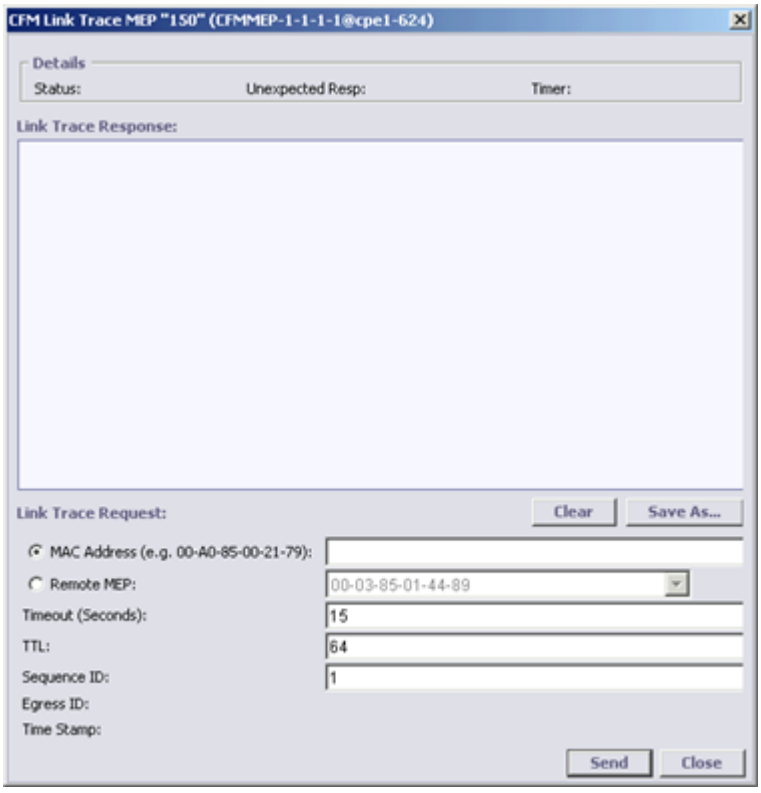
A linktrace message is terminated (dropped) on an NE whose level is higher than that of the CFM level defined in a message. For example, a CFM domain of level=4 will only answer and forward messages of equal and higher levels (4, 5, 6, 7), dropping level 1, 2, 3 messages that are out of boundaries of allowed CFM domain. *Up to total of 10 LinkTrace operations can be applied at the same time on NE.*

NOTE: The display can be saved to a text file.

➢ To run link trace between two MEPs

1. In the **Network Element** tree, under **Service CFM, select** the relevant MEP. The MEP pane is invoked.

2. Under **Remote MEPs (RMEP),** select **Link Trace.** The following dialog appears.

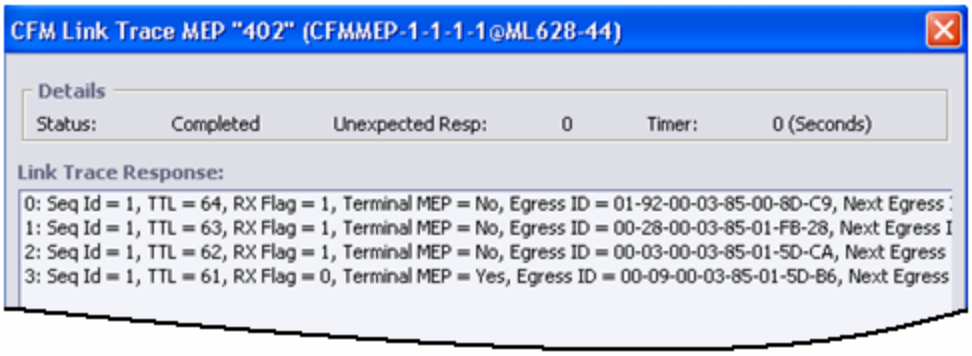


3. Set the MAC address (unicast address) of the remote device to which the link trace will be performed, using one of the following methods:
   - Remote MAC Address - type the address
   - Remote MEP - select from the list of addresses
4. Define the attributes of the data to be sent:
   - Timeout - Number of seconds before the Link Trace request is transmitted.
   - TTL (Time To Live) – Period of time a data unit can exist in the network. Used to prevent packets that have not reached their destination from loading the network.
   - Sequence ID – user defined ID assigned to the link trace sequence. Used to identify and analyze the link trace messages.

   For Y.1731 mode only:
   - Egress ID – *after the test is run*, shows the ID of the port on which the link trace packet egressed.
   - Time Stamp – Index showing when the Link Trace test was run (*shown after the test is run*).
5. Click Send. If connectivity is available (at some level), the returned message will be displayed.

   The message (e.g. illustrated below) shows the Seq ID (i.e. 5), other configured parameters (i.e. TTL = 64) and link trace information.

NOTE: Use the scroll bar at the bottom of the window to show display additional information.



For more explanations about the messages in this window, see **Link Trace Result Example** (on page 11-17).

The Link Trace tab buttons can be used to control the test and save results:

Table 51: Link Trace Tab buttons

Click...	To...
Save As...	save the test results to a user defined text file
Stop	stop the test
Close	close the tab

Each CFM Link Trace response includes the following information.

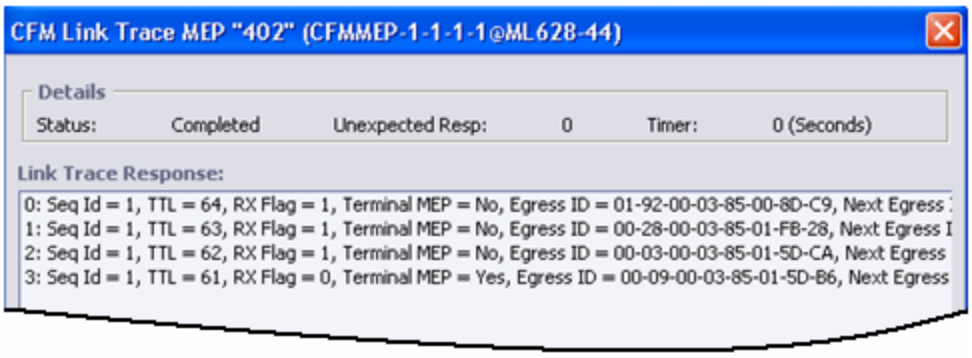
Table 52: CFM Link Trace Response Information

Message Info	Description
Seq ID	Sequence ID. The identification which communicates Link Trace Request and Response messages (the ID is equal). This identification is used to identify own Link Trace Request (and it's responses) in multiple management environment.
TTL	Time-to-live. Provided in Link Trace Request/Response Message. Each NE answering to the CFM Link Trace message, decreases (-1) the TTL forwarded in the CFM Link trace Request. This is used to identify the number of hops that participated in the link trace.
Rx Flag	Shows if CFM Link Trace message was re-build and forwarded.
Terminal MEP	Identifies the responder as a MIP (intermediate point) or MEP (end point)
Egress ID and Next Egress ID	Re-built by each hop when the CFM Link trace message is re-sent. Used view directly communicating hops (as chain): • Two NEs are considered as connected if Next Egress ID of one of them appears as (Last) Ingress ID on another (see example). • Egress ID format includes: Shared MAC (of Bridge) provided in the low-order six octets, and internally used (MEP + PORT) unique NE identification in the high-order two octets.

Message Info	Description
Relay	Specifies which forwarding table is used (MIP/MEP FRWDB or Traffic FRWDB). On ML NE only MIP/MEP FRWDB is used for CFM forwarding.
CHS ID Type, CHS ID, Mang.Address	Identifies NE (chassis) type, TID/SID configured on ML NE, and NE Management Address (IP V4 format)
Ingress, Ingress MAC, Ingress Port ID	Reports Ingress Port Status, Address and Local Name of the Port on which the CFM Linktrace Request message was received (come in). NOTE: CFM Link Trace Response is sent backward through the port specified as ingress.
Egress, Egress MAC, Egress Port ID	Reports Egress Port Status, Address and Local Name of the Port on which the CFM Linktrace Request message was forwarded (come out).
ORG TLV	Organization Specific TLV. ML NE doesn't provide this parameter. If any other device will provide, ML will print out this parameter in HEX form.

Link Trace Result Example

In this example you can see a fragment of CFM Linktrace response collected in Link Trace dialog:



By scrolling the pane to the right, this text is revealed:

1st line: Seq Id = 1, TTL = 64, RX Flag = 1, Terminal MEP = No,

Egress ID = 01-92-00-03-85-00-8D-C9, Next Egress ID = 00-05-00-03-85-00-28-C6, Relay = MIP Forward DB,

CHS ID Type = ENTPHNAME, CHS ID = Z0525G40008, Mang. Addr = 10.1.4.1 (IPV4), Ingress = Ok, Ingress MAC = 00-03-85-00-28-C6, Ingress Port ID = ETH-6 (LOCAL), Egress = Ok, Egress MAC = 00-03-85-00-28-C6, Egress Port ID = ETH-4 (LOCAL), ORG TLV = null

2nd line: Seq Id = 1, TTL = 63, RX Flag = 1, Terminal MEP = No,
Egress ID = 00-05-00-03-85-00-28-C6, Next Egress ID = 00-03-00-03-85-01-5D-CA, Relay = MIP Forward DB,
CHS ID Type = ENTPHNAME, CHS ID = ML648-64, Mang. Addr = 10.1.6.7 (IPV4), Ingress = Ok, Ingress MAC = 00-03-85-01-5D-CA, Ingress Port ID = ETH-4 (LOCAL), Egress = Ok, Egress MAC = 00-03-85-01-5D-CA, Egress Port ID = ETH-2 (LOCAL), ORG TLV = null

3rd line: Seq Id = 1, TTL = 62, RX Flag = 1, Terminal MEP = No,
Egress ID = 00-03-00-03-85-01-5D-CA, Next Egress ID = 00-09-00-03-85-01-5D-B6, Relay = MIP Forward DB,
CHS ID Type = ENTPHNAME, CHS ID = ML648-CO, Mang. Addr = 10.1.6.15 (IPV4), Ingress = Ok, Ingress MAC = 00-03-85-01-5D-B6, Ingress Port ID = ETH-2 (LOCAL), Egress = Ok, Egress MAC = 00-03-85-01-5D-B6, Egress Port ID = HSL-1 (LOCAL),

ORG TLV = null

Explanation:

In this fragment CFM Link Trace Request passed through NE with TID="Z0525G40008", then through NE with TID="ML648-64" and then through NE with TID="ML648-CO".

It is clear that this is a "chain" connectivity (and not "star"):
The Next Egress ID=00-05-00-03-85-00-28-C6 of 1st response (first line) is equal to Egress ID=00-05-00-03-85-00-28-C6 from 2nd response (2nd line) and Next Egress ID=00-03-00-03-85-01-5D-CA from 2nd response is equal to Egress ID=00-03-00-03-85-01-5D-CA from 3rd response (3rd).

Y.1731 Ethernet OAM

Y.1731 Ethernet OAM standard provides superset of functionalities provided in CFM and additional performance monitoring functionality. Y.1731 performance monitoring functions enable continuous control of Service Level Agreement objectives.

The connectivity fault management functionality of the end-to-end network is divided into hierarchical management spaces referred to as **Maintenance Entity Groups (MEGs)** There are three Maintenance Domain levels: Operator, Service Provider and Customer. The hierarchical relationship is based on numerically assigned values from 0 to 7 that correspond to the levels.

MEGs are demarcated by Maintenance End Points (MEPs) belonging to a common service or provider. These objects generate and manage end-to-end sessions and it is *required* to configure them in order to provide connectivity control, fault isolation and SLA monitoring. In addition (and optionally) Maintenance Intermediate Points (MIPs) can be configured, in order to provide additional information for fault isolation.

➢ To configure Y.1731

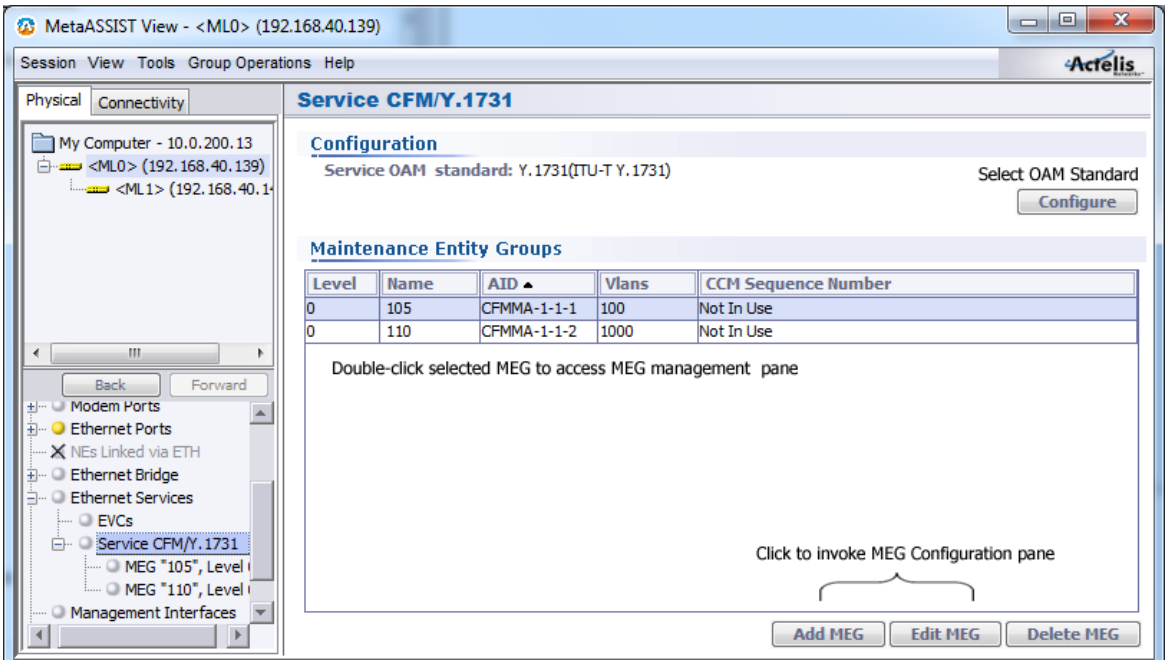
1. Enable the Y.1731 OAM option on the ML unit.
2. Configure the MEGs.
3. Allocate MEPs per each MEG which has end-points on the ML unit.
4. Allocate MIPs if no MEP of this MEG planned on the ML unit.
5. Allocate Remote MEPs (RMEPs).

Setting ML to Operate with Y.1731

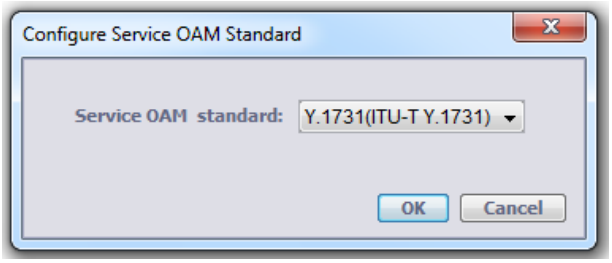
Begin by setting the ML unit to operate with the Y.1731 standard. All the relevant options will become available.

➢ **To set the ML unit to operate with Y.1731**

1. In the **Element Tree,** under **Ethernet Services**, select **Service CFM.** The Service CFM pane appears.



2. Under **Ethernet OAM Standard,** click the **Configure** button. The Ethernet OAM Standard dialog appears.



3. Select **Y.1731** and click **OK**. The relevant options will be displayed in the Service OAM pane:
   - Ethernet OAM Standard - shows the currently operating OAM standard Y.1731.
   - Maintenance Entity Groups - shows the currently defined MEGs and provides access to the MEG management options using the buttons and by double-clicking on the selected MEG.

     Note that different options are available when double-clicking a selected MEG or clicking the Edit MEG button

Y.1731 MEG Definition

A Maintenance Entity Group (MEG) accounts for all MEPs from a common service or provider. A MEG is defined according to a user assigned name (string of characters) and VLANs comprising the MEGs.

Y.1731 MIP Definitions

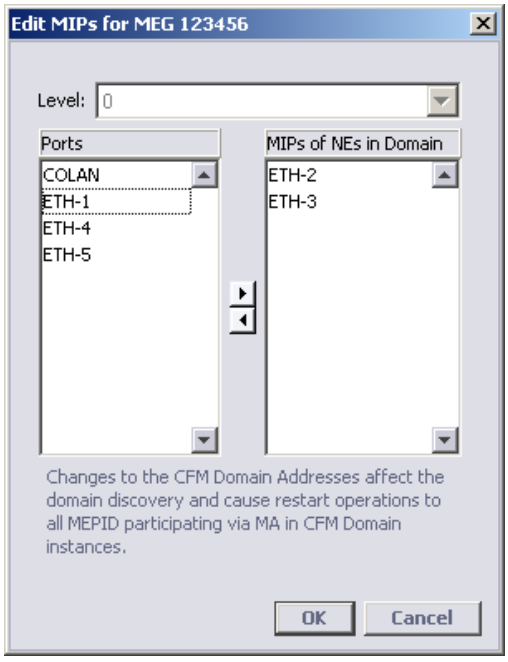
A CFM Maintenance Intermediate Point (MIP) is a port which forwards CFM frames identified by an equal or higher level and drops lower level, regardless of whether they are received from the relay (Switch) or wire (Port) side.

MIP responds to CFM Loopback (unicast) and CFM Link Trace (multicast) messages of the CFM Domain to which MIP belongs (identified by domain name and level in a message).

If MIPs are not configured on a device, CFM frames are forwarded on port according to VLAN rules.

➢ **To define the domain MIPs**

1. Invoke the pane of the domain whose MIPs are to be defined by doing one of the following:
   - In the **Network Element** tree, under **Service CFM,** select the relevant MEG.
   - In the **Network Element** tree, select **Service CFM** and double-click on the defined MEG.
2. In the **MEG** pane, MIPs area, the currently defined MIPs for the selected domain are displayed. To add or modify the defined MIPs, click the **Edit MIPs** button. The following dialog appears.



3. Under **Ports,** select the MIPs (or MIPs) participating in the domain and use the arrows to allocate them to the MEG or remove them from the MEG.
4. Click **OK**. The new definitions will be applied to the MEG. .

Y.1731 MEP Definitions and Management

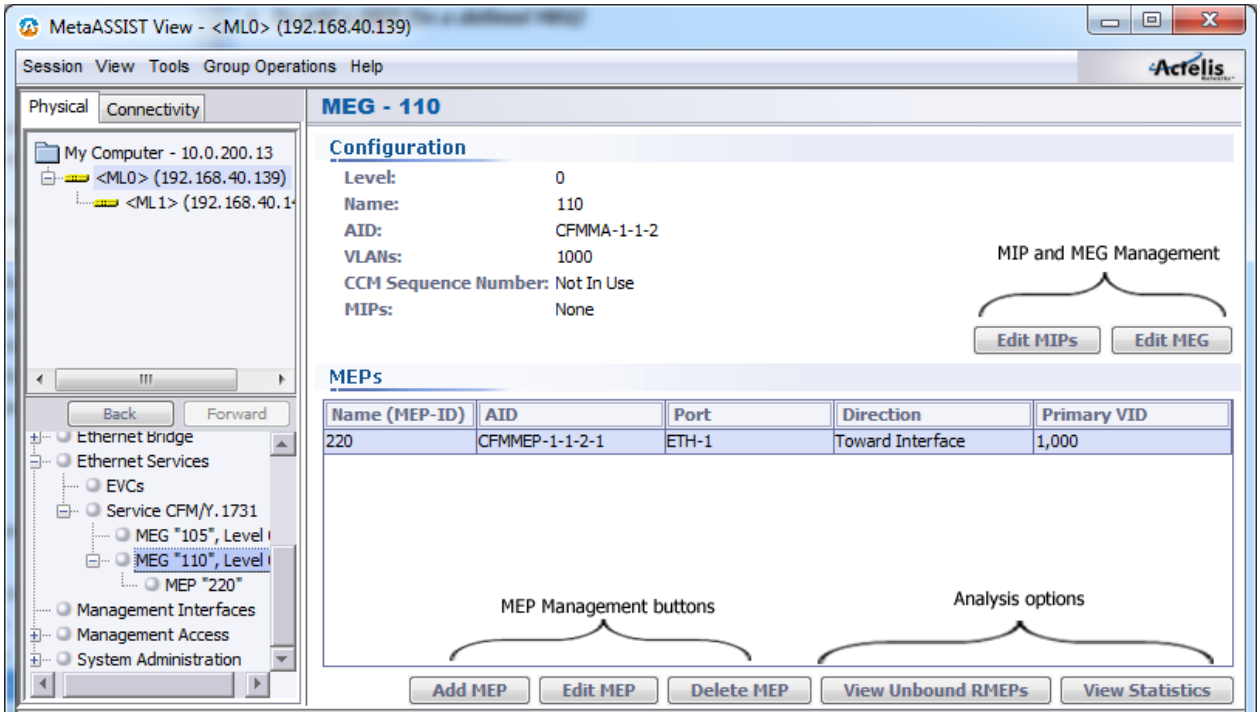
Maintenance End Points (MEPs) define the boundaries of the corresponding MEG. MEP in a network is identified uniquely by MEG (Name, level), MEP ID , VLAN tag VID and COS bits value provided in each frame. To provide this uniqueness , MEP is configured on ML unit using Port , Direction (always toward wire), VID, MEPID.

In addition, MEP connectivity control and performance monitor parameters can be configured.

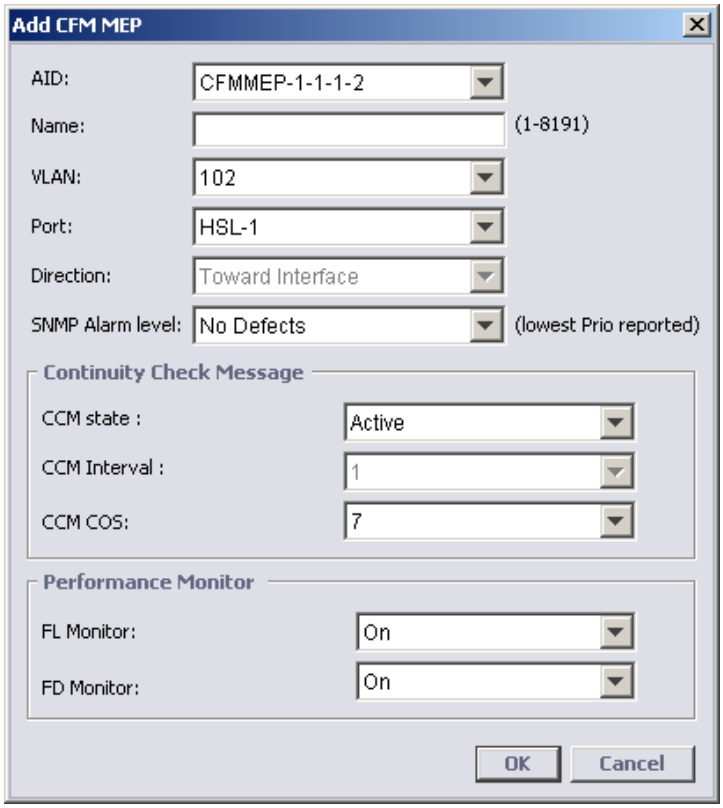
Note that *each MEG allows up to 8 MEPs,* where the *maximum number of MEPs* supported by each system may vary according to the ML model.

➢ **To add a MEP (to a defined MEG)**

1. In the **Network Element** tree, select **Service CFM** and click on the MEG to which MEPs will be allocated. The dedicated MEG pane appears.



2. In the **MEG** pane, **MEPs** area, click **Add MEPs.** The **Add MEP** dialog appears.



3. MEP AID appears automatically. It is an internal identifier used to locally identify the MEP. SIGFLT or RDI alarms are raised against this AID.
4. In the **Name** field, assign the MEP ID. It is a part of unique identification of the MEP frames in the network.

   Range = 1 to 8191.
5. Select the VLAN ID from the list of specified in MEG VLANs (will be part of unique identification of the MEP frames in the network).
6. Select the Port on which the MEP is located on the NE. The MEP can be configured only on tagged/untagged (not stacked) ports (not LAGs).

NOTE: Only Towards Interface direction is supported (cannot be modified).

7. Select SNMP Alarm Level - the lowest priority level to be reported as a SNMP notification by this MEP. Default: No defects
8. To enable Continuity Check Messages for the MEP:
   - Set the CCM State to Active.
   - CCM Interval is set to 1 sec and cannot be changed.
   - Select the COS Priority (0 to 7) assigned to of CCM packets to be sent by the MEP.
9. Set performance monitoring as follows:
   - FL Monitor is enabled by default. Set Off to disable. Control ETH-CC multicast messages arrived in the same MEG to make Frame Loss (FL)/Frame Loss Ratio (FLR) calculations.

- FD Monitor is enabled by default. Set Off to disable. Originate unicast ETH-DM messages and control ETH-DMR messages replied to make Frame Delay (FD) and Frame Delay Variation (FDV) calculations.

10. Click **OK** to complete the procedure. The MEP is added under the relevant MEG. If the MEP item is selected in the tree, the dedicated MEP pane appears.

Y.1731 RMEP Configuration

To complete Ethernet OAM configuration, create MEPs on at least two points of Ethernet connection to two neighbor NEs. Each MEP configured on a *neighbor* NE is considered a Remote MEP (RMEP) by the MEP of the NE.

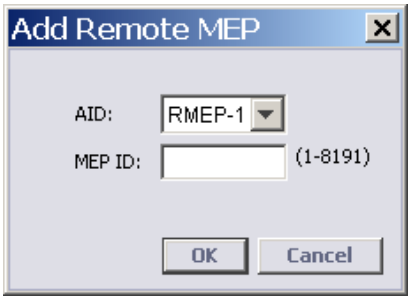
In Y.1731 mode, RMEPs are manually specified for each configured local MEP. The procedure is used to control NE monitoring resources (do not allocate them for any discovered RMEP, but to RMEP committed to be controlled).

RMEPs can be manually defined or auto-discovered.

Manually Defining RMEPs

➢ **To manually define RMEPs**

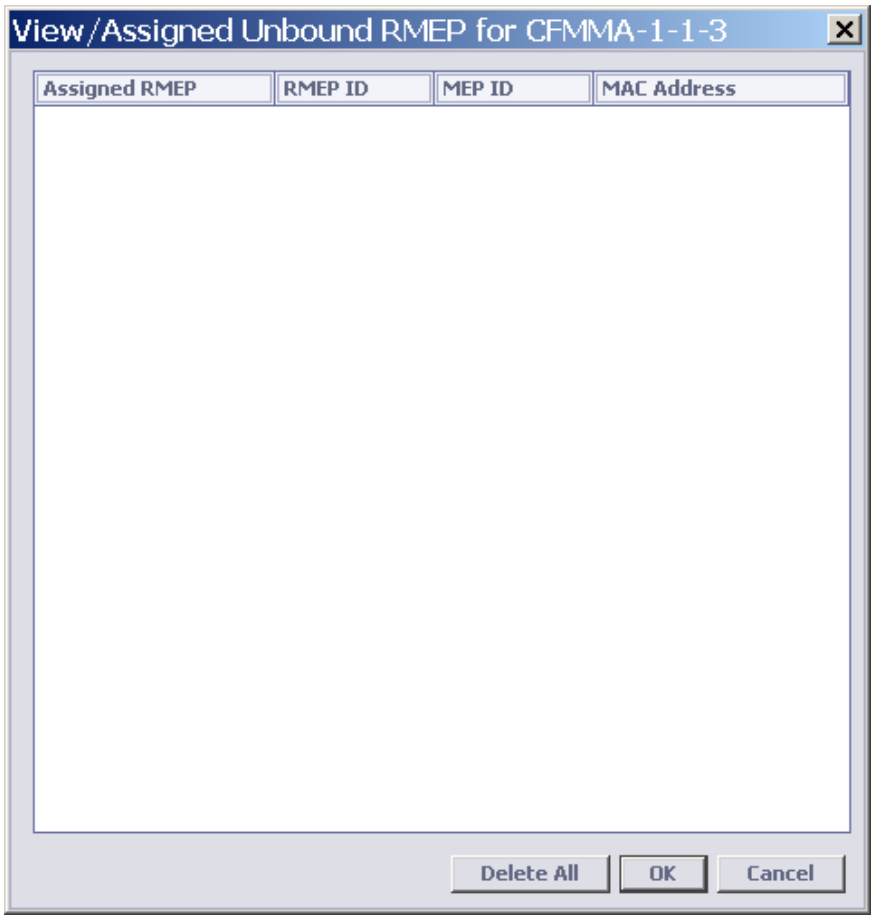
1. In the **MEP Pane**, click the **Add RMEP** button. The Add Remote MEP dialog appears.



2. Enter the **MEP ID** - a unique network identification of remote MEP.

   The MEG ID, MEG level and VID of the RMEP should match that of the MEP. These parameters are configured on the remote NE on which the remote MEP is created.

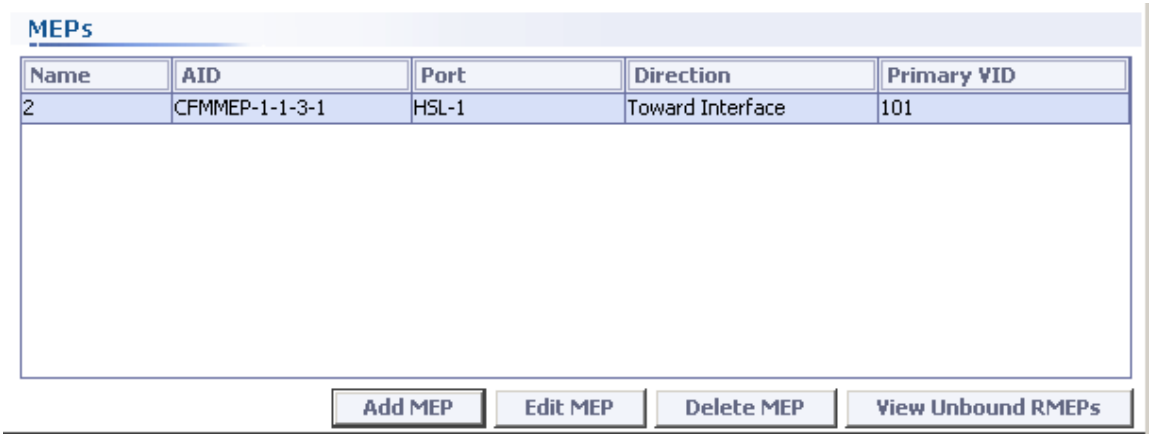
To simplify the process of MEP and RMEP assignment, a list of unbound auto-discovered RMEPs on a MEG level are provided.



Viewing Auto-discovered MEPs

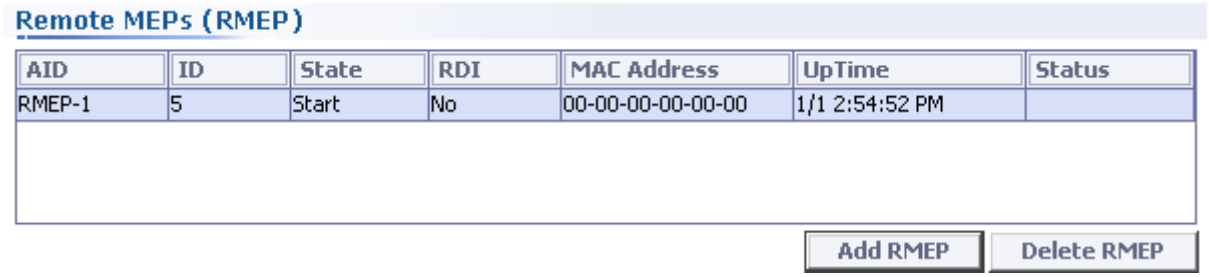
- **To view auto-discovered RMEPs**

  In the MEP area, RMEML NE provides list of unbound auto-discovered RMEPs on a MEG level .



- Click the **View Unbound RMEPs** button to view discovered in the same MEG MEPs on other NEs.
- Up to 20 MEPs can be shown, records are not aged.
- To refresh information (addition /removal of MEP on neighbor NEs) , click **Delete All** inside the dialog.

State and Status of RMEP is monitored in a table:



Y.1731 Tools

There are two main areas of OAM: *connectivity fault management* and *service performance monitoring*. Connectivity Fault management functionalities of Y.1731 and CFM 802.1ag modes are equal. See **CFM MEP Monitoring and Analysis Tools** (on page 11-10).

Y.1731, additionally provides Performance Monitoring functionality implemented on ML NE as defined below.

ML units provide raw counters for the following:

- Current 15min and 1-day intervals (start of PM counters can be set per system)
- Previous 8 hours (15min x 36 intervals)
- Previous 1-day interval

See Performance Monitoring. Y.1731 Performance data is available via MAV GUI, TL1 and SNMP (proprietary Actelis MIB). The following counter types are available:

- **Frame Loss** - is implemented using CCM representative traffic. Standard CCM with Sequence Number that is not in use (i.e. permanently set to 0) utilizes TX/RX counter fields to count CCM frames lost - suitable for point-to-point (E-Line) deployment only. Sequence Number incremented within each CCM sent by each MEP (non-standard solution) allows frame lost monitoring per each Remote MEP individually – which is suitable for all point-to-multipoint deployments.
- **Frame Loss Ratio** – is implemented using Frame Loss counters (see above) , being calculated and updated each 1-minute. To calculate FLR over an interval (1-minute, 15-min or 1-day), total FL is divided to Total number of Rx Frames arrived during the interval.
- **Round Trip Frame Delay** – is implemented using ETH-DM/DMR unicast messages, as an average delay measured during the interval, monitored per each MEP-to-RMEP connection individually. Provided in microsec units.

- **Round Trip Frame Delay Variation** – is implemented using Frame Delay measurement, being calculated as the difference between minimal and average (updated each 1-minute using 60 samples collected in the minute) result. Provided in microsec units.

For TL1 only - ML units supports configurable thresholds per each type of counter, causes notification to be sent when any threshold is crossed.

For SNMP only - in addition to raw data of Y.1731 counters, ML units provides additional Service Availability parameter (MEF10.2) reported for current and previous day, using configurable via SNMP Service Availability and Unavailability criteria (by FLR %). Service Availability result (as per MEF10.2) is normalized to configurable via SNMP Service Availability Objective (by FLR %) criteria.

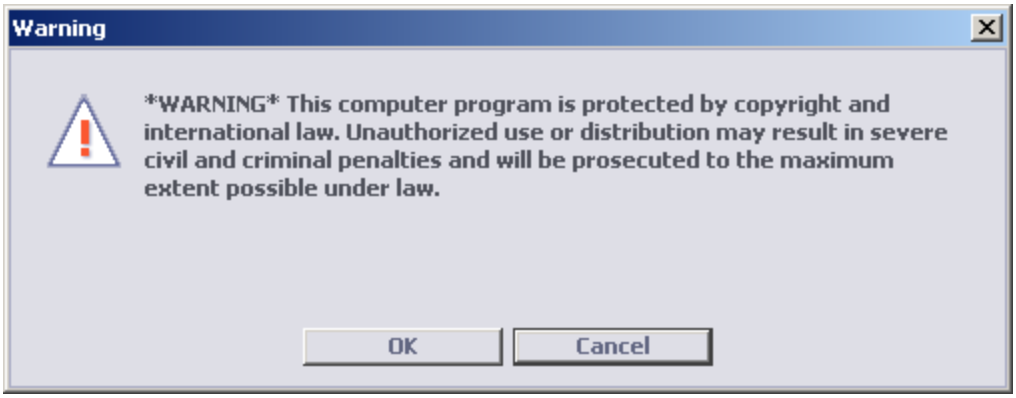
12 Security Management

This chapter describes the options available for managing security on an ML device.

In This Chapter

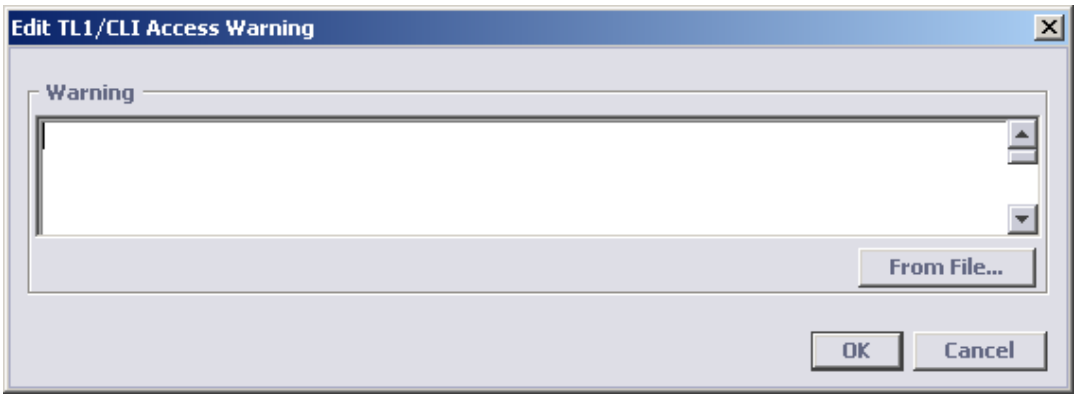
Configuring Session Access Warning Text

The system administrator can configure a security message to appear each time a new CLI, TL1 or MetaASSIST View session is opened. This is done by configuring the warning text, according to the site security needs or regional requirements. If text is not configured, the message will not appear, and the session will be directly accessed. The warning session appears in the following format:



➢ To configure the session access warning

1. In the **Network Element** tree, choose **Management Access** and press the **Edit Warning** button. The Edit Warning dialog appears.



2. Enter the warning text by either:
   - Using the dialog to type the text (use <Enter> for new line) .
   - Selecting the text from a file by clicking the **From File** button to attach a file with Warning text (in ASCII format) prepared in advance.
3. Click **OK**. The Warning text will now be displayed in the **Management Access** screen under the TL1/CLI Access Warning. The warning will now be displayed whenever a user opens a session.

Managing User Accounts

ML systems are factory set with three **default user accounts** (on page 12-5) with varying privilege levels (Admin, Read, Write). The set of default privileges cannot be modified; however, *five* additional (customizable) sets of privileges may be defined, based on templates of the default sets. Thus, a total of *eight privileges* are available per ML: three default and up to five more user definable privileges.

➢ To manage user accounts

1. Are the default user accounts privileges sufficient?
2. If the default user accounts privileges are not sufficient, enter as Admin level user and define additional privileges. Up to five additional privileges can be defined.
3. Add user accounts and assign each new user one of the default or customized privileges. Up to 100 users can be defined per ML system.

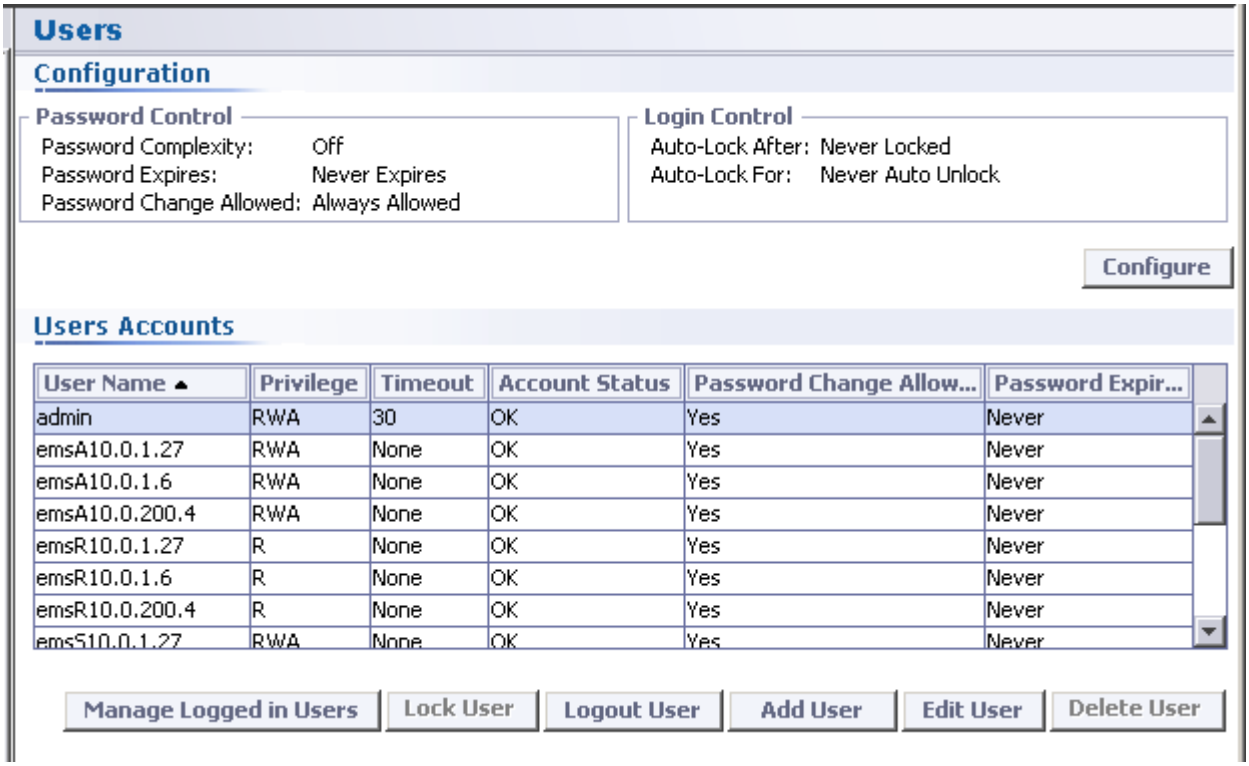
NOTE: Refer to **Default User Accounts and Privileges** (on page 12-5) for more information about the available privileges and specifically privileges of the Admin level user.

The User Accounts Pane

This Users pane provides access to all the user account management options.

➢ **To invoke the Users pane**

In the **Network Element** tree, expand **Management Access** and click **Users**. The corresponding pane appears. The pane is divided into two main areas where operation buttons are located at the bottom of the pane.



Users' pane areas:

- Configuration area - summarizes the global password and login characteristics and behavior and provides access to the corresponding configuration options via the **Configure** button.
- User Accounts area - shows the default users (admin, read, write) and any other defined users along with configuration and status of each password.

The buttons at the bottom of the pane provide access to various operations as described below.

Table 53: User Accounts pane operations

Button	Description
Manage Logged in Users	Displays the users that are currently logged onto this NE and enables an Admin level user to disconnect any user.
Lock Users	Locks out a selected user. This does not delete the user account.
Logout User	Logs out the selected user.

Button	Description
Add User	Accesses a user account definition dialog.
Edit User	Accesses the user account definitions dialog for the selected user.
Delete User	Removes the selected user from the list (after a verification prompt).

Default User Accounts and Privileges

The following table details the available default user accounts:

Table 54: Default User Accounts

User name	Password	Privilege Rights
read	read	Monitoring of insecure data
write	write	Monitoring and configuring of insecure data
admin	admin	Monitoring, configuring and security administration. Service critical operations.

NOTE: An administrator level user can **lock out a user** (on page 12-11) without deleting the account.

All User Account management operations are performed via the **User (accounts)** (on page 12-4) pane.

When managing the user accounts list:

- Up to 100 users can be defined.
- The user name **admin** cannot be deleted.
- Account passwords can be modified by the System Administrator at any time.

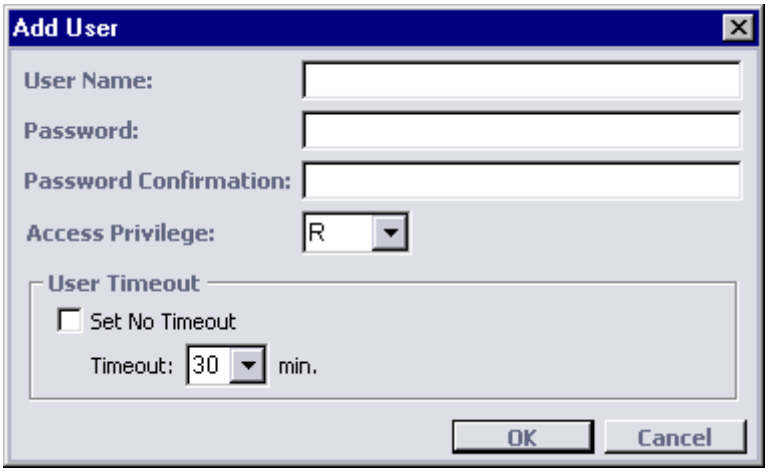
Adding a User Account

Up to 100 user accounts may be defined.

➢ **To add a user account**

1. In the **Network Element** tree, expand **Management Access** and click **Users**. The corresponding pane appears.

At the bottom of the pane, click **Add Users**. The **Add User** dialog appears.



NOTE: For group operations, open the **Add User** dialog box via the menu bar: **Group Operations**, **Users**, **Add**.

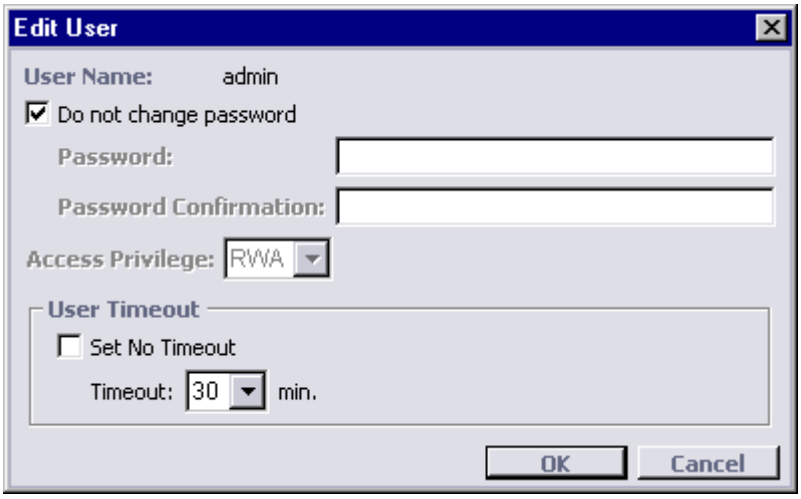
2. Add an account as follows:
   - Type the new **User Name.**
   - In the **Password** box, type in the password.
   - In the **Password Confirmation** box, re-type the password.
   - In the **Access Privilege** box, select the access privilege right (R-read, RW-write, RWA-admin).
3. You may define the account to timeout after a defined time period. To define timeout, in the **Timeout** list box, select the timeout in minutes. Range = 5 to 99 minutes.
4. To set no timeout, select the **Set No Timeout** check box. The **Timeout** box is grayed out.
5. Click **OK**. The **Add User** dialog box closes and the user is added to the list.

Editing User Account

➢ **To edit a user account**

1. In the **Network Element** tree, expand **Management Access** and click **Users**. The corresponding pane appears.

In the **Users** pane, select a user from the table and click **Edit User**. The **Edit User** dialog appears.



2. To modify the password, clear the **Do not change password** check box.
3. Modify the details as necessary (see steps 3 to 8 in **Adding a User Account** (on page 12-5)).
4. Click **OK**. The **Edit User** dialog box closes.

Deleting a User Account

Only users with admin privileges can delete a user account.

➢ **To delete a user account:**

1. In the **Network Element** tree, expand **Management Access** and click **Users**. The corresponding pane appears.
2. In the **Users** pane, select the user to be deleted and click **Delete User**. A warning message appears.
3. To delete the user, click **Yes**. The user is deleted from the list.

NOTE: Users with admin privilege can delete their own user account via the on-going session opened using this user account. No special notification is given, except for the regular warning window.

Password Control

The general characteristics (complexity, etc.) of a password are defined on a system (global) level. In addition, each of the users can change their own password in an ongoing session.

System Wide User Settings

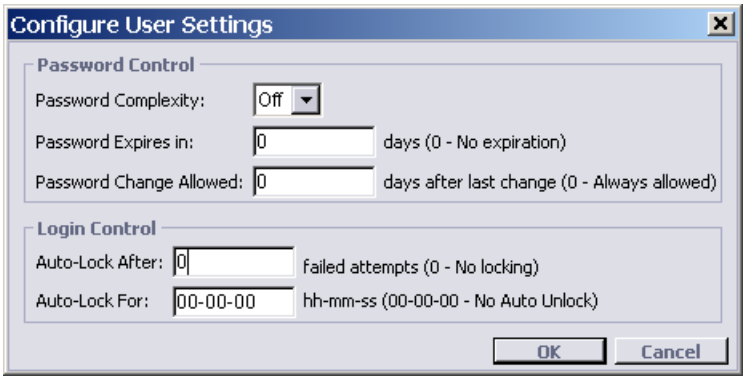
Note the following:

- Only users with **admin** privileges can configure password control parameters.
- The ML device Date/Time changes affect the remaining Password Expiration Time and Time Between Password Changes. Each user accounts is updated according to the following:
  - Date and/or Time are set forward before original expiration time: the times are reduced accordingly so expiration would take place at the original date and hour.
  - Date and/or Time are set forward beyond original expiration time: the expiration would take place immediately.
  - Date is set backward: the times are reset to the start (with time 00:00) so expiration would take place as if the password was created today at 00:00.
  - Time is set backward (no date change): the times are unchanged, expiration would take place after the remaining time.

➢ To configure global password settings

1. From the **Network Element** tree, expand **Management Access** and choose **Users**.
2. In the invoked pane, click **Configure**. The **Configure User Settings** dialog appears.

NOTE: For group operations, open the **Configure User Settings** dialog box via the menu bar: **Group Operations, Users, Configure**.



3. Set **Password Complexity**:
   - Off - any number of characters can be used (1 to 20)
   - On - passwords must consist of at least 8 characters (maximum 20) including at least 2 letters and 2 numbers but no more than 20 characters.

NOTE: When Password Complexity is enabled, you can continue using your original non-complex password. However, it is recommended to change your own password to a complex one.

4. Set the **Password Expires -** this is the duration for each valid password before it expires. By default, password expiration is disabled.

   The user session is discontinued immediately after expiration of the password from the attached system. MetaASSIST View and the ML device allows the user to log in with the expired password but immediately displays a dialog box requiring the user to define a new password before running the session. Expiration can be enabled/disabled by the System Administrator only.

   It is recommended to immediately change the password the first time after new password setting by the administrator.

   NOTE: Password expiration global change is not applied immediately on each user account, but upon next change of the password, except when password expiration is disabled/enabled (changed from/to No expiration).

   About password history: When password complexity is enabled, then six previously used passwords cannot be reused. This implies that after the expiration period has passed and the user needs to enter a new password, the user cannot use the same password or any earlier password (up to 6 passwords) as a new password. Password History size (6) is not configurable. Password History control can be disable together with Password complexity.

5. In the **Password Change Allowed** box, type the minimum amount of time in which a password cannot be changed (0 - always allowed).

   NOTE: When configuring the password, MetaASSIST View verifies that the password Change Not Allowed value is smaller than the password Expires After value.

Editing Password in Session

Each of the users can change their own password in an ongoing session. After changing the password you must login with the new password.

Notes:
1. If the password expires during the ongoing session, an **Edit Password** dialog opens with an instructional note to change the password.
2. If you try to change the password before the Password Change Allowed time has elapsed, an error message is displayed.

➢ **To Edit Password in ongoing Session:**

From the **Session** menu, select **Edit Password**. The **Edit Password for User** dialog appears.

1. In the **Type Current Password** box, type the current password.
2. In the **Type New Password** box, type your new password.
3. In the **Retype New Password** box, retype your new password.
4. Click **OK**.

Locking Out Users

Individual users can be locked out. The time and behavior of the lockout are determined on a global level.

Lock a User Account

The System Administrator can lock out a selected user from future sessions from the users accounts without deleting the account.

➢ **To lockout a user:**

1. In the **Network Element** tree, expand **Management Access** and click **Users**. The corresponding pane appears.
2. From the table, select a user to lockout.
3. Click **Lock User**. A warning message appears.
4. Click **Yes**. The user status is displayed as locked out by admin in the list.

➢ **To unlock a user:**

1. In the **Network Element** tree, expand **Management Access** and click **Users**. The corresponding pane appears.
2. To unlock a user, select the user and click **Unlock User**. A warning message appears.
3. Click **Yes**. The user status is cleared.

System Wide Lockout Behavior

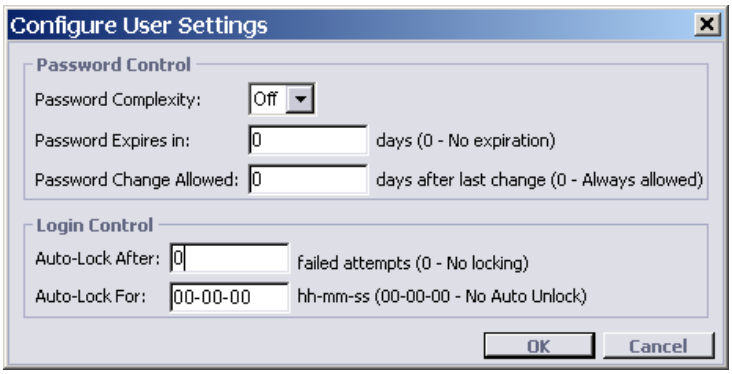
Note the following:

- The ML device Date/Time change does not affect actual count of Failed Login Attempts and account Locking Period.
- NOTE: The features described below are applied to all user accounts.
- Only users with **admin** privileges can configure lockout control parameters as follows.

➢ **To configure account locking**

1. From the **Network Element** tree, expand **Management Access** and choose **Users**.
2. In the invoked pane, click **Configure**. The **Configure User Settings** dialog appears.

NOTE: For group operations, open the **Configure User Settings** dialog box via the menu bar: **Group Operations, Users, Configure**.



3. Set the lockout behavior as follows: Under **Login Control** set:
   - **Auto-Lock After:** The system can automatically lock users after a certain amount of failed attempts. Locked users cannot log in to the system via MetaASSIST View, a TL1 session or the support page for a configured amount of time. Both the number of allowed incorrect attempts and the time for account locking are configurable as a system-wide parameter controlled by the administrator only.
   - **Auto-Lock for:** By default, the lock out time period is 0 (no automatic unlock). In this case, only a user with **admin** privileges can unlock the account before it can be used again.

Managing Sessions

Each of the users can view his own session information including password expiration and change status in the **Session.**

In addition, an Admin level user can view all the currently connected sessions and disconnect any session.

User Session Information

Each of the users can view his own session information including password expiration and change status in the **Session Information** box.

When managing the sessions, consider the following:

- The ML device system can support up to 20 concurrent management sessions (19 remotely (via LAN) and 1 locally (via craft port) connected management hosts);
- The ML device supports up to three SSH sessions.

➢ **To view Session Information:**

From the Menu bar, click **Session - Session Information**. The **Session Information** dialog appears.

Viewing and Managing Current Logged in Sessions

➢ **To view current logged in sessions:**

1. In the **Network Element** tree, expand **Management Access** and click **Users**. The corresponding pane appears.
2. Click **Managed Logged in Users**. The **Logged in Users** dialog appears showing the currently logged in users and the IP from which the session is connected.

NOTE: If more than one session is opened from the same IP, each *additional* session is indicated by a letter. The example below shows three sessions opened from the same IP: the first session is not marked by a letter, while each of the other sessions is assigned a letter (A, B, etc.).

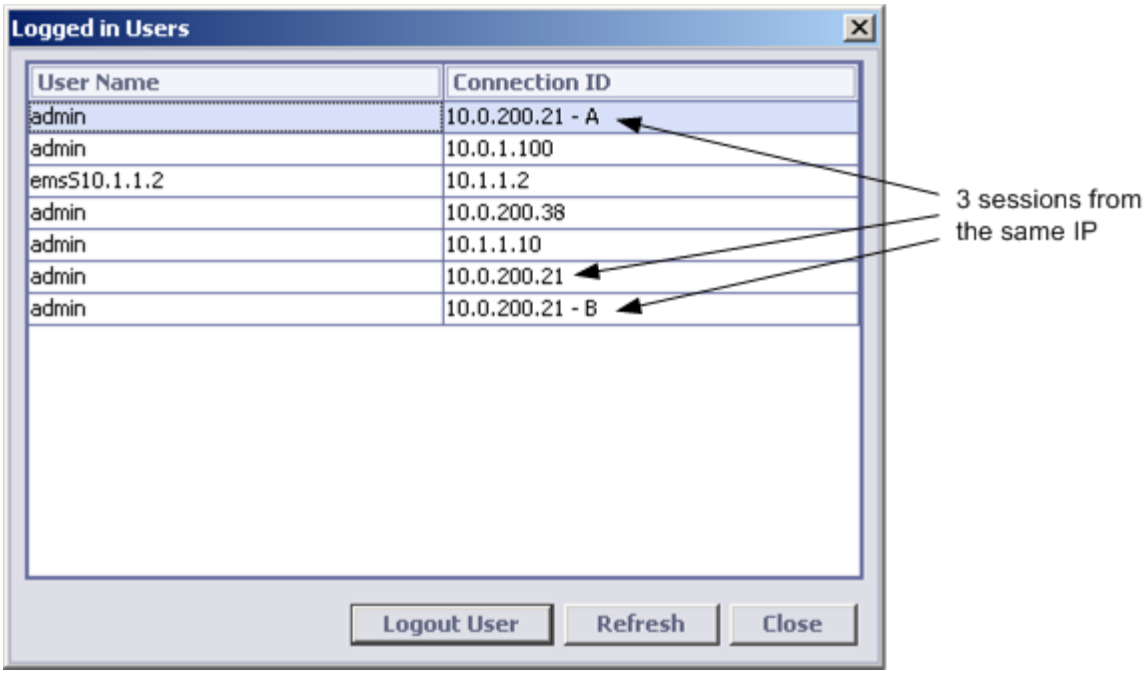


Table 55: Additional operations

Click..	To do this
Logout User	Forcible logout a selected user according to characteristics defined in **System Wide Lockout Behavior** (on page 12-11). (Only for Admin level users).
Refresh	Refresh the display readings.
Close	To return to the User's pane.

3. To refresh the display, click **Refresh**.
4. To logout a user,
5. To close the dialog box, click **Close**.

NOTE: Sessions aborted due to Access Control enabling may be listed for a few minutes after they were disconnected.

You can forcibly logout a selected user from the users accounts to terminate the user ongoing session.

➢ **To log out a user:**

1. From the table, select a user to log out.
2. Click **Logout User**. A warning message appears.
3. Click **Yes**.
4. The user status is displayed as logged out in the list.

RADIUS

Remote Authentication Dial-In User Service (RADIUS) is a distributed client/server system that centralizes control of device access. If RADIUS is used, all user profiles and access limits to the ML devices can be managed via the RADIUS server. The ML devices serve as clients which send authentication requests to a central RADIUS server.

NOTE: The Radius option can be configured on an ML level (as described in this section) or for all selected MLs through the **Group** menu, **Radius** option.

It is recommended to use RADIUS in the following network environments:

- Networks with multiple-vendor access servers
- Networks already using RADIUS
- Networks in which a user must only access a single service
- Networks that require resource accounting
- Networks with dynamic group of users (no need to set changes in the group on all NEs but only in one location)

From R6.0 and higher, RADIUS on ML supports:

- PAP (Password Authentication Protocol). (CHAP (Challenge Handshake Authentication Protocol) is not supported, where CHAP messages are discarded by the system.)
- Authentication only (RFC 2865). All account messages (supported in RFC2866) are discarded by the system.

Configuring for RADIUS Operation

In order for the ML to be secured with the RADIUS server, two types of operations are required:

- Configure the ML NE (as a Radius client) with the RADIUS server address and with the relevant communication parameters. See **Configuring RADIUS on ML** (on page 12-16).
- Configure the Radius Server to respond with a **Message** (on page 12-18) which provides **Service-Type** (on page 12-19) (Parameter ID #6) with values 1, 7 or 6 - for read, write and admin user accordingly.

Authentication of user upon TL1 login is processed by checking for:

- record availability for specified UserID (name);
- matching of typed and registered (stored encrypted) password;
- checking for the UserID privileges (read only, read-write, or full admin access)
- idle session timeout (to close the session between ML and TL1 (MAV) agent automatically if no activities detected).

With the introduction of the RADIUS Client on ML, there are three ways to authenticate user account during TL1 login to ML:

- Using Local ML device user accounts records only (default configuration of ML device) - In this case queries to Radius Server for user account authentication are not issued.
- Using Radius Server and then Local DB for user account records query:
  - If the Server did not answer during defined period of time (Timeout Period x Number of Retries), then Backup Server is queried (if configured).
  - If the Backup Server did not answer during the defined period of time (Timeout Period x Number of Retries), then local ML device user account records are checked.
  - If the Server replies with reject (no user account found), Local ML device user account records are queried.
  - Each new attempt of login always passes through the "Server->Backup Server->Local DB" flow, which means that if the Primary Server is down, it takes (Timeout Period x Number of Retries) time to access the Backup Server each time, where improper configuration queries to the RADIUS may seriously slow down the login of TL1-based management applications (MetaASSIST View, MetaASSIST EMS, etc.).
- Using only RADIUS - this provides a very high level of security in which access to ML device is available only through Radius authentication. In cases where both the RADIUS Server and Backup Server are unreachable (connection on ML is configured improperly or Servers are down), connection can be restored as follows:
  - Factory Restart - may restore the remote connection to the ML device.
  - Local Craft access - (using "Radius then Local"), using local ADMIN user account (which can be modified but not deleted).

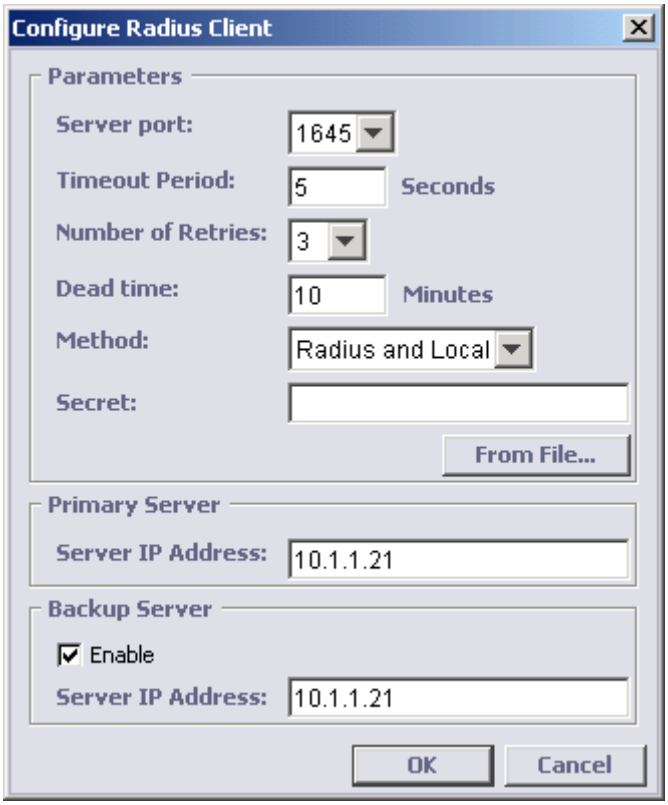
Configuring RADIUS on ML

NOTE: RADIUS can also be configured on groups of selected ML devices (and their NEs) through the **Group** menu, **RADIUS** option.

➢ To configure Radius on the ML device

1. From the **Network Element tree**, under **Management Access**, choose **Radius**. The Radius client pane appears.

2. To define the Radius Server click the **Configure** button. The Configure Radius Client pane is invoked.



3. Configure the Radius server host Parameters:
   - Under Primary Server, in the **Server IP Address** field - enter the IP the Radius application server (0.0.0.0, by default).
   - **Server Port** – the authentication destination port that is configured on the RADIUS server. Options: 1645, 1812. (Default = port 1812)
   - **Timeout Period** – Number of seconds the ML waits for a reply before retransmitting the request to the Radius server (Default = 60 sec).
   - **Number of Retries** – Maximum number of times the ML transmits each RADIUS request to the server (Default = 3).
   - **Dead Time** – Maximum time a client should wait before attempting to contact the server again after the "Timeout period x Number of Retries" expired (default = 10 min).
   - **Secret** – A key string shared between the ML and a RADIUS server. The secret must match the encryption key used on the RADIUS server and CANNOT be empty.

NOTE: The Secret is configured once per ML, and thus is used the same for both Primary and Secondary Server (assuming the Secondary Server usually is a full replica of Primary Server, with another IP address only).

4. Define the **Method** of access to the ML device:
   - Local (ML factory default) - access is verified according to the user information stored in the ML device.
   - Radius and Local - the Radius server (including backup Server) and then locally stored on ML user information is queried for authentication.
   - Radius - only the Radius can authenticate access. If the Radius is not available, then access the ML is not allowed.
5. If a backup Radius Server exists, under **Backup Server**:
   - Check-mark the **Enable** option
   - Enter the IP address of the backup Radius Server.

   NOTE: If a backup server is not defined (0.0.0.0 by default) query is skipped. If both Servers are configured with the same IP, queries will be sent twice (if no reply from Primary Server).
6. Click **OK**.

RADIUS Message Parameters Supported by ML

From R6.0 and higher, RADIUS on ML supports:

- PAP (Password Authentication Protocol). (CHAP (Challenge Handshake Authentication Protocol) is not supported, where CHAP messages are discarded by the system.)
- Authentication only (RFC 2865). All account messages (supported in RFC2866) are discarded by the system.

ML devices support either group of the Message Parameters

Table 56: Group I - Message Parameters Supported by ML

Type	Name	Length	Description	Message(s)
1	User-Name	3-63 chars	the name of the user to be authenticated	Access-Request/ Access-Accept
2	User-Password	16-128 chars	the password of the user to be authenticated	Access-Request
4	NAS-IP-Address		IP Address of the ML (MUST be used to select the shared secret)	Access-Request
5	NAS-Port		Indicates the physical port number of the NAS, which is authenticating the user.	Access-Request

Table 57: Group II - Message Parameters Supported by ML

Type	Name	Length	Description	Message(s)
61	NAS-Port-Type		The type of the physical port: 15 - Ethernet 16 - xDSL - Digital Subscriber Line of unknown type	

Type	Name	Length	Description	Message(s)
6	Service-Type		The type of service the user has.	Access-Request/ Access-Accept
18	Reply-Message		Indicates text, which should be displayed to the user. When used in an Access-Accept, it is the success message. When used in an Access-Reject, it is the failure message.	Access-Accept / Access-Reject
28	Idle-Timeout		Maximum number of consecutive seconds of idle time this user should be permitted before being disconnected by the ML.	Access-Accept

RADIUS Service Type Parameters Supported by ML

Table 58: RADIUS Service Type Parameters

Value	Type	Description	Notes.
1	Login	The user should be connected to a host.	ML Users with “Read” access privilege.
6	Administrative	The user should be granted access to the administrative interface to the NAS from which privileged commands can be executed.	ML Users with “Admin” access privilege.
7	NAS Prompt	The user should be provided a command prompt on the NAS from which non-privileged commands can be executed.	ML Users with “Write” access privilege.

Radius Server Configuration for ML Versions

Table 59: Radius server configuration for various ML versions

ML SW Version	You will need this for configuration....
Before R7.1 **Can be used also with R7.1 or higher)	Acquire from the radius server the "users" file with records for ML units access: <name> Cleartext-Password:= "<password>" Login-Service=Telnet User-Service-Type=Login-User/NAS-Prompt-User/Administrative-User, Idle-Timeout = <value of timeout in sec>
R7.1 and higher only	Vendor Specific attributes: ATTRIBUTE NAS-Identifier 32 string ATTRIBUTE Vendor-Specific 26 string VENDORATTR 5468 Actelis-Privilege 1 string Radius Server "dictionary" file entry: $INCLUDE dictionary.actelis Actelis dictionary file for "dictionary.actelis": # For Actelis # # Id # VENDOR Actelis 5468 BEGIN-VENDOR Actelis ATTRIBUTE Actelis-Privilege 1 string END-VENDOR Actelis Radius Server "users" file should be updated with the following records: <name> Cleartext-Password:= "<password>" NAS-Identifier=5468, User-Service-Type=Login-User, Login-Service=Telnet, Actelis-Privilege= "RWA"/"RW"/"RO" Idle-Timeout = <value of timeout in sec>

IP Access Control List (ACL)

The ML provides a secured-session-access mechanism, which allows defining a list of up to 100 allowed IP addresses (or range of addresses, using a subnet mask)), and their allowed access protocols. Range of IP addresses is supported on ML700 and ML2300 (SDU-400) systems

The ML NE management access can be controlled via the following protocols:

- **Telnet-TL1** (MetaASSIST View and TL1)
- **Telnet-CLI**
- **SSH** (MetaASSIST View and TL1 over SSH)
- **SNMP**
- **HTTP**

In addition to TCP/UDP ports operated for ML NE management, there are some other opened TCP/UDP ports which can be controlled as follows:

- When ACL is enabled, TCP 1112 (msql service port), 49155 (vxworks debug port) and UDP 2601 (netmount port) are automatically closed.
- Port UDP 123 (SNTP) can be enabled or disabled on application level, unaffected by ACL.
- Port UDP 3087 (Actelis Discovery Protocol) cannot be disabled, unaffected by ACL.

IP Access Control List (ACL) is managed by System Administrator with admin privilege, who can enable the ACL mechanism (not enabled by default) and update the list of allowed clients and their protocols.

ML devices are always accessible via craft port, regardless Access Control mechanism setting and ACL content.

If ACL is enabled and no client with permitted Telnet access protocol is defined, then ML device cannot be configured and monitored remotely via Telnet but via the craft port only.

Managing the IP Access Control List (ACL)

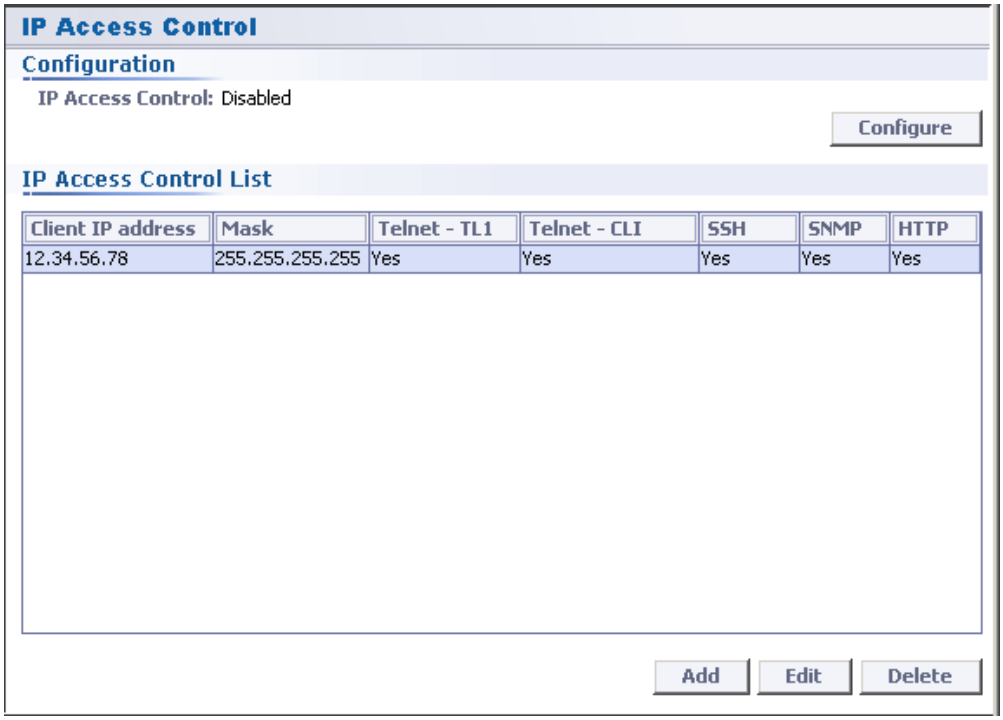
The **IP Access Control** pane provides the following capabilities:

- Enable/Disable the IP Access Control mechanism.
- Manage (add/delete,..) client IP addresses listed in the IP Access Control List (ACL), along with their permitted connection protocols.

NOTE: For group operations of Adding or configuring the IP Access Control, open the **IP Access Control** dialog box via the menu bar: **Group Operations, IP Access Control, Add** or **Configure**.

➢ To open the IP Access Control pane:

1. In the Network Element tree, expand the **Management Access** and choose **IP Access Control**. The IP Access Control pane opens in the work area.



The screen provides a table listing the allowed IP addresses and configured attributes:

- Subnet Mask IP address
- Allowed/Blocked protocols for each IP entry (CLI, TL1, SSH, SNMP, HTTP)

2. The following operation buttons are available:
   - **Configure** - enable/disable the IP Access Control mechanism. When IP Access Control is enabled, all open management sessions running on IP addresses that are not listed in the IP ACL are disconnected.
   - **Add** - add an IP Address to the IP Access Control List, specifying the permitted connection protocols.
   - **Edit** - edit the permitted protocol list for an existing IP entry. For each removed protocol, all ongoing sessions from the specified IP address of that protocol are aborted (if IP Access Control is enabled).
   - **Delete** - delete a client from the IP Access Control list. For each deleted client, all ongoing sessions from that client are aborted (if IP Access Control is enabled). *NOTE: The last client IP address cannot be deleted while IP Access Control is enabled.*

Enabling the ACL

When ACL is disabled - all clients can connect to the ML device using any of the above supported protocols.

When ACL is enabled - only clients specified in the Access Control List can connect to the ML device using the above supported protocols. Incoming access attempts from other IP addresses are denied. In addition, ongoing sessions from client IP addresses not specified in the Access Control List or through non-permitted protocols specified in the list are aborted. If the used protocol is not defined in the IP Access Control List for the accessing IP client, a time out is sent and no connection is established.

NOTE: When enabled, ML device allows to access the system through craft port from any PC.

At least one Client with any permitted access protocol must be configured before Access Control can be enabled.

In addition, the user cannot delete the last entry in the list while the Access Control is enabled. The Configure button is disabled if the Access Control List does not contain any active entry (this prevents the possibility of IP access locking).

NOTE: If no client with permitted Telnet access protocol is defined, the ML device cannot be configured and monitored remotely via Telnet only via the craft port.

➢ To Enable the ACL mechanism

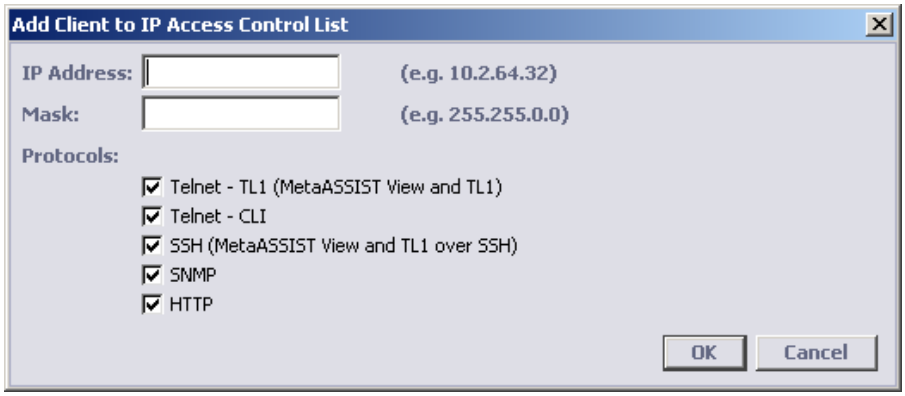
1. In the IP Access Control pane click the **Configure** button. The Configure IP Access Control dialog opens.

2. Check the **Enabled** box.
3. Click **OK**.

Updating the ACL

➢ **To add or edit an allowed IP address to the ACL table**

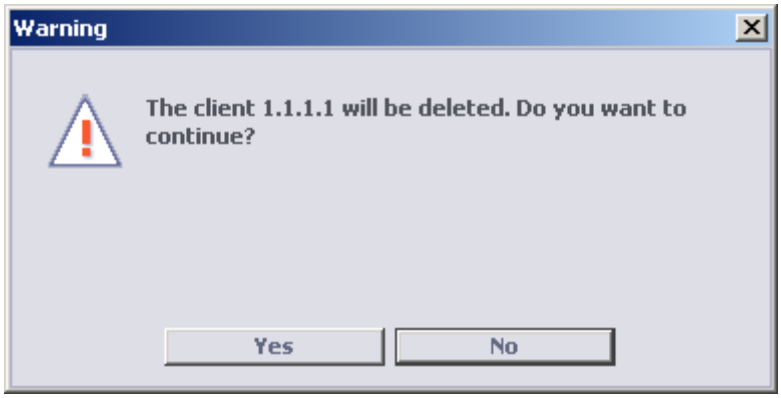
1. In the IP Access Control pane click the **Add** button. The Add Client to IP Access Control List dialog opens.



2. Enter the required data of the new IP address and its allowed protocols as follows:
   - **IP Address** of the client.
   - **MASK** of the IP Address (for a group of IP addresses).
   - Checkmark the allowed protocols for the new IP address.
3. Click **OK**.

➢ **To delete an existing IP address from the ACL table**

1. In the IP Access Control pane, choose the relevant row (of the IP that is to be updated) and click the **Delete** button. The delete confirmation dialog opens.



2. Click **Yes**.

NOTE: For each deleted client, all ongoing sessions from that client are aborted (if IP Access Control is enabled).

SSH - Secure Shell

Authentication, also referred to as user identity, is the means by which a system verifies that access is only given to intended users and denied to anyone else. All machines that implement the SSH protocol (e.g. Management Host with MetaASSIST View or the ML device) support authentication and therefore must own a pair of encryption keys - one public and one private. Encryption capability is always provided on the data path. Authentication however, can be enabled or disabled (by default) in the ML device running as an SSH Server.

SSH protocol provides authentication, encryption and data integrity to secure network communication between management host and the ML device as follows:

- Authentication - ML device supports DSA authentication keys 512, 768, or 1024 bits long.
- Encryption - ML device employs symmetric keys encryption algorithms: AES, DES, 3DES, Blowfish. Encryption is always enabled, whether authentication is enabled or disabled.
- Data integrity - ML device automatically (not-configurable) provides the Message Authentication Code (MAC) algorithm.

NOTE: SSH is not applied to Craft port connection.

When authentication is disabled in the ML230/ML2300 system, then authentication from any management host (running as an SSH client) is allowed.

Managing SSH Communication

This chapter guides you to enable and control SSH communication.

NOTE: SSH communication attributes can be configured/observed only by users with *admin* permissions.

For first time SSH communication operation you should perform as shown in the following table:

Table 60: Task summary—first time SSH communication

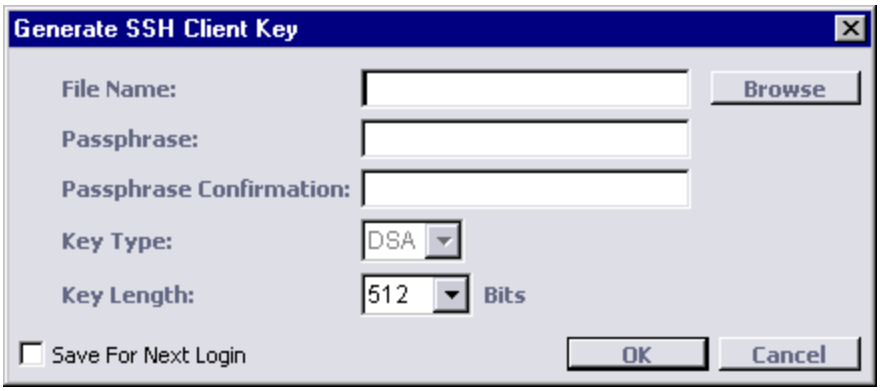
Generate key pair on your Management Host using MetaASSIST View or any third party SSH package. Optional - use the Passphrase. See **Generating SSH Client Key** (on page 12-27).
↓
Add the generated Public key of the Management host(s) to the SSH Server authentication list of the ML device. See **SSH Server Overview** (on page 12-27) to access the function and **Authenticated SSH Client Keys Control** (on page 12-32) for detailed description.
↓
Regenerate the key pair (optional) or view the generated (by default) SSH Server Public key on the ML device. See **SSH Server Overview** (on page 12-27) to access the function and **Generating SSH Server Key** (on page 12-28) for detailed description.
↓
Enable Authentication control on the Server. See **SSH Server Overview** (on page 12-27) to access the function and **Enable Authentication Control on Server** (on page 12-34) for detailed description.
↓
During log in to the ML device using SSH option (on initial connection), the system prompts you to add (*Accept Key <Signature> for Host <IP Address>?*) ML device Public key as a trusted host on your Management Host. If key is trusted (check with network administrator), accept the key.

Generating SSH Client Key

MetaASSIST View assists you in generating a client key pair for SSH communication. These pair keys generated for SSH communication are used by the management host for authentication during an SSH session. Optionally, may secure the management host generated keys by using a passphrase. This prevents access of other users on the same management host to the ML device. This procedure can be performed when not connected to the ML device.

➢ **To generate a SSH client key:**

1. From the **Session** menu (on menu bar), select **Generate SSH Client Key**. The **Generate SSH Client Key** dialog appears.



2. In the **File Name** box, type the file name or click the **Browse** button to indicate a location where the file will be created (optional).
3. To define a passphrase:
   - In the **Passphrase** box, type your new passphrase.
   - To confirm the passphrase, in the **Passphrase Confirmation** box, re-type the passphrase.
4. To select key size for additional protection, from the **Key Length** list box, select the number of bits (512, 768 or 1024).
5. To use the generated key for next login, select the **Save For Next Login** check box.
6. Click **OK**.

SSH Server Overview

Only users with **Admin** privilege rights can view and manage the SSH parameters for the ML device (SSH server).

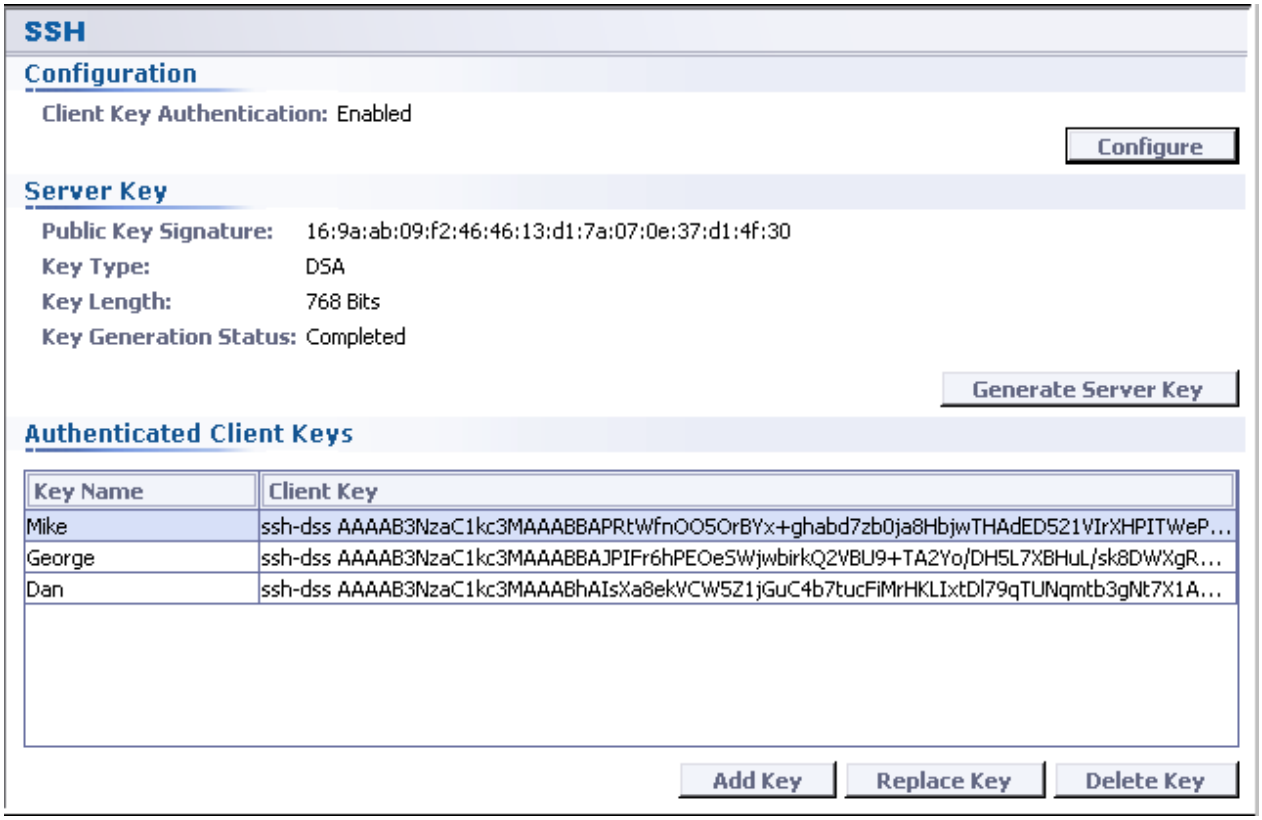
In the **SSH** pane you can:

- Generate Server Key (Public and Private);
- View Server public key parameters (Signature of Public Key, Authentication Key Type, Key Length and Key Generation status);
- Manage Authenticated Clients Public Key storage (add, replace, delete Authenticated Client Key);

- Enabled/Disabled Client Key Authentication feature

➢ **To open the SSH pane**

1. In the Network Element tree, open **Management Access**.
2. Open **SSH**. The **SSH** pane opens in the work area.

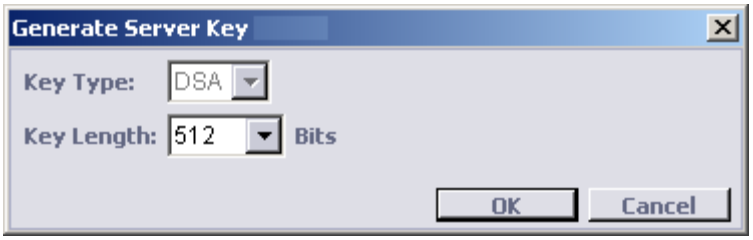


Generating SSH Server Key

After reverting to Factory Setup, the ML device generates the keys automatically. You can also generate Server Keys (public and private) on the system, using DSA type 512, 768 or 1024 bits key length.

➢ **To generate SSH Server Keys:**

1. On the SSH review pane, click **Generate Server Key**. The **Generate Server Key** dialog appears.



2. From the **Key Type** list box, select the key type (currently only keys of type DSA are supported and the selection box is disabled).

3. From the **Key Length** list box, select the key length.
4. Click **OK**. A warning opens "*New server key will be generated. Do you want to continue*". Click **Yes**. A progress bar appears and the **Key Generation Status** is In Progress.

SSH Server/Client Authentication

This chapter describes:

- The authentication and flow when SSH Authentication is Enabled/Disabled.
- Configuring the Authenticated SSH Client Keys Control.

Enabled SSH Authentication

When authentication is enabled then only pre-defined management hosts are authenticated. As shown in the following figure, if the key name is not defined in the ML130/ML1300 system in the Authenticated Public Keys table for management host (IP) "C", the connection will fail after a PC time-out.

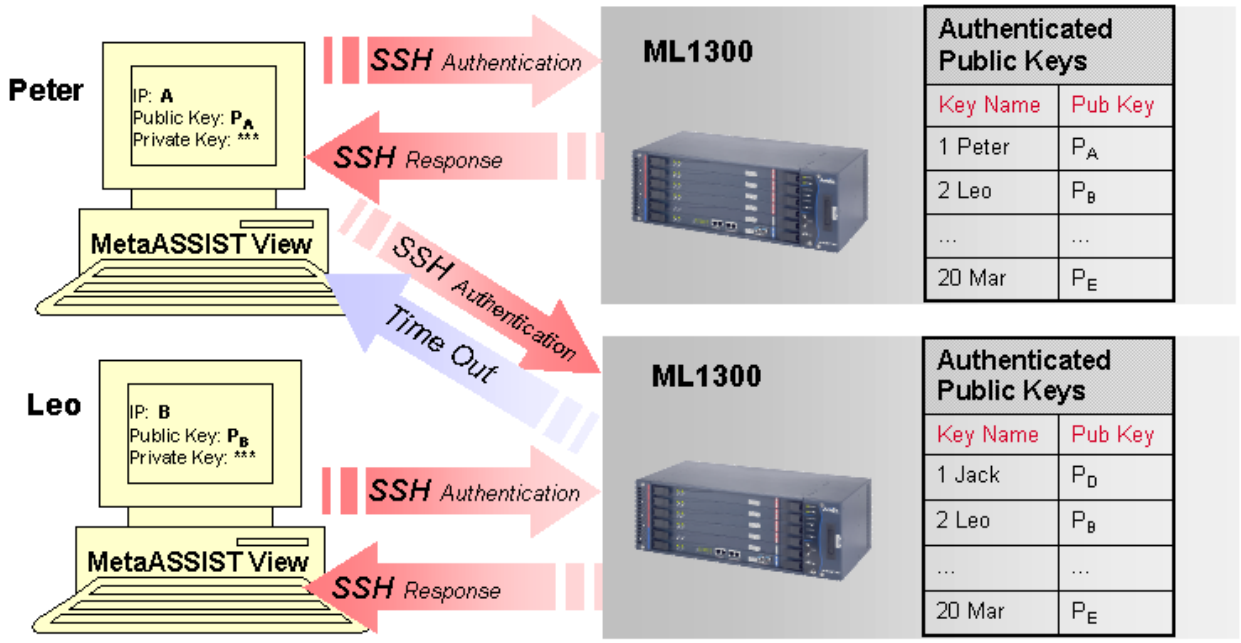


Figure 14: Authentication of Public Keys is Enabled

SSH Server Authentication Flow

When authentication is enabled then to access an account on a Secure Shell server, a copy of the client's Client Key must be uploaded to the server in advance. As shown in the following figure, P_A and P_B are Public Keys of SSH client and should be a prerequisite on the ML130/ML1300 SSH Server.

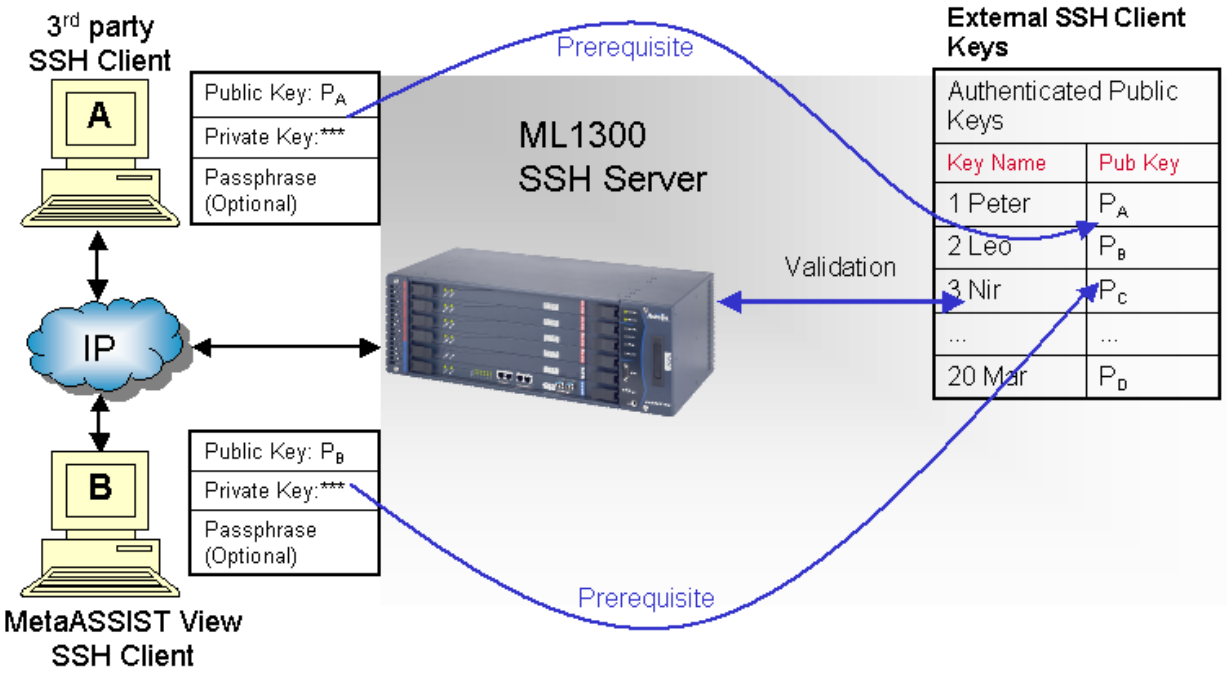


Figure 15: SSH Authentication Flow (on ML device)

SSH Client (MetaASSIST View) Authentication Flow

There is no need for a Server Public Key prerequisite on PC. As shown in the following figure, in MetaASSIST View a pop-up will prompt the user for online confirmation that the Client Key published by the server is indeed the expected key generated by this ML130/ML1300 system.

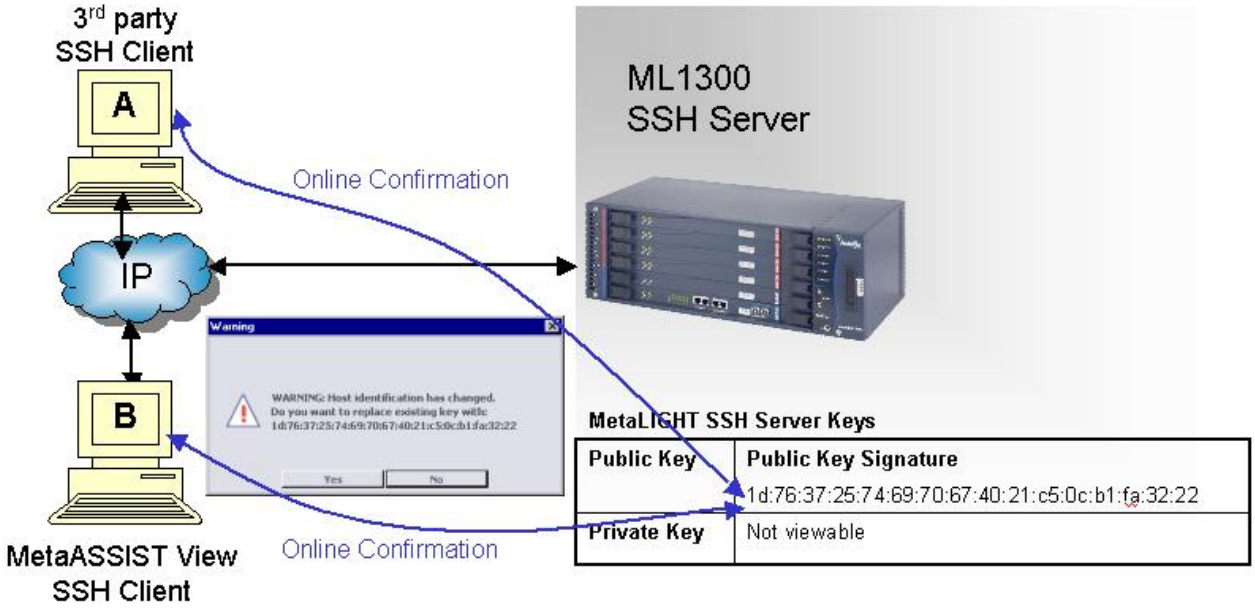


Figure 16: SSH Authentication Flow (on PC)

Disabled SSH Authentication

When authentication is disabled in the ML130/ML1300 system, then authentication from any management host (running as an SSH client) is allowed as shown in the following figure.

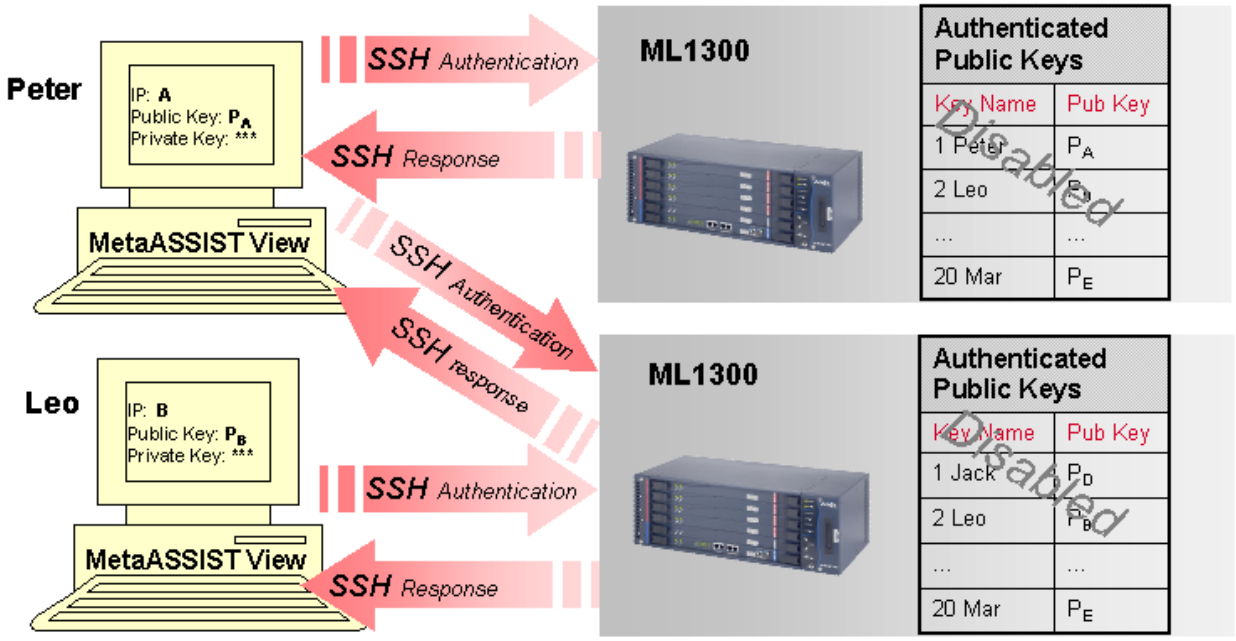


Figure 17: Authentication of Public Keys is Disabled

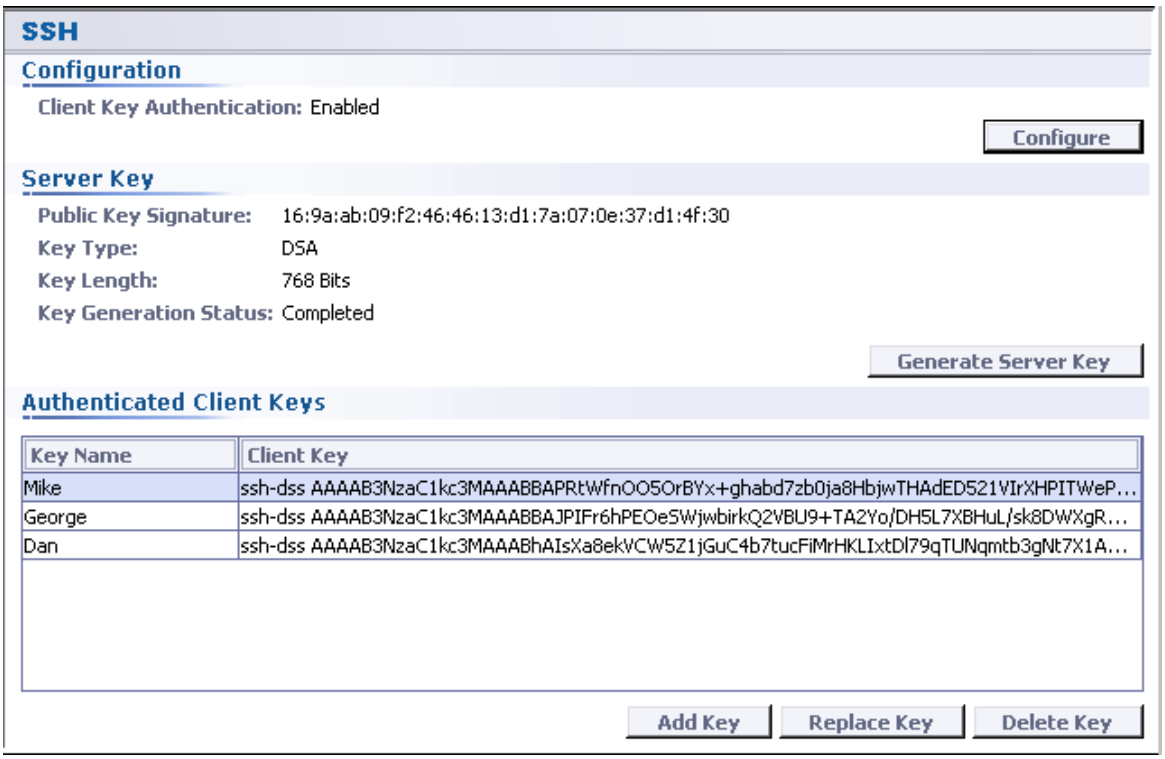
Authenticated SSH Client Keys Control

You can add, replace or delete SSH Client Public Keys from the Server database. After Factory Setup, the Authenticated SSH Client Keys table is empty. MetaASSIST View allows you to add to the table of up to 20 entries.

➢ **To open the SSH pane**

1. In the Network Element tree, open **Management Access**.

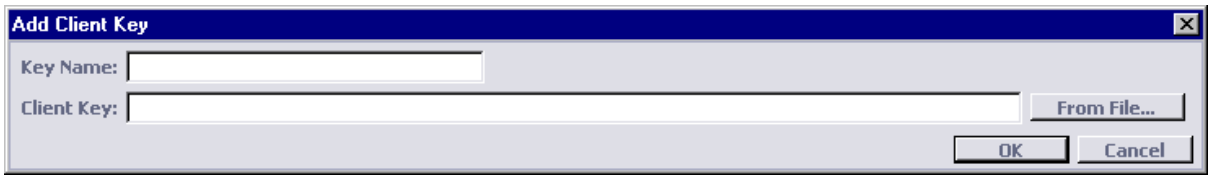
2. Open **SSH**. The **SSH** pane opens in the work area.



Add Key Procedure

➢ **To add a Client Public Key:**

1. On the bottom of the SSH review pane, click **Add Key**. The **Add Client Key** dialog appears.



NOTE: For group operations, open the **Add Client Key** dialog box via the menu bar: **Group Operations**, **SSH**, **Add**.

2. In the **Key Name** box, type the key name.
3. In the **Client Key** box, type the full public client key or click the **From File** button to locate a file containing the client public key.
4. Click **OK**. The **Add Client Key** dialog box closes and the Client Key is added to the list and will be written into the server pubic key database.

➢ **To replace an authenticated Client Key:**

1. In the **Authenticated Client Keys** pane area a list of all authenticated client keys is displayed. From the list, select a Client Key to replace.

2. On the bottom of the SSH review pane, click **Replace Key**. The **Replace Client Key** dialog appears.

3. In the **Key Name** box, view the key name.
4. In the **Client Key** box, type the full new public client key or click the **From File** button to locate a file containing the new client public key.
5. Click **OK**. The **Replace Key** dialog box closes and the Client Key is replaced in the list and the client public key is replaced in the server.

Delete Key Procedure

➢ **To delete an authenticated Client Key:**

1. Select from the list of authenticated client keys a Client Key to delete and click **Delete**. A warning message appears: *'The key <Key Name> will be deleted. Do you want to continue?'*
2. To delete the key, click **Yes**. The client public key is deleted from the list and from the server database.

Enable Authentication Control on SSH Server

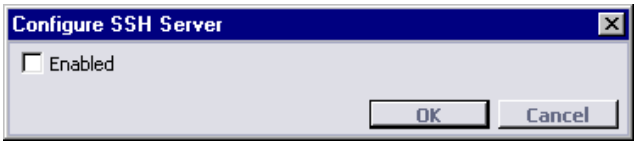
You can enable or disable Client Key Authentication on the Server using the **Configure** button on the **SSH** pane. When authentication of Client Keys is disabled then access from any host is allowed. After Factory Setup, SSH Client Key Authentication control on SSH Server is disabled.

When SSH Client Key Authentication control is enabled, then access is allowed only to those management hosts that were provisioned in the Server Authenticated Client Keys table.

NOTE: When the Authenticated SSH Client Keys table is empty, the **Configure** button is disabled. In addition, you cannot delete the last entry from the table. This prevents users from enabling or having an enabled SSH Client Key Authentication without any Authenticated SSH Client Keys that will lock out SSH access.

➢ **To configure the authentication of SSH Client Keys**

1. Click **Configure**. The **Configure SSH Server** dialog appears.



NOTE: For group operations, open the **Configure SSH Server** dialog box via the menu bar: **Group Operations, SSH, Configure**.

2. To enable SSH Client Key Authentication, select the **Enabled** check box.
3. Click **OK**.

13 Monitoring

MetaASSIST View is used to monitor and analyze the status of the directly connected ML device and any hosted ML systems. MetaASSIST provides a range of real-time monitoring options that allow network administrators to follow the health and activity of Actelis network elements.

This chapter describes the various monitoring tools and how they are used to view faults and information for the overall system and for system elements such as Ethernet Bridge, Equipment, Ethernet Services, etc. (Note that the MetaASSIST EMS application is also available for managing and monitoring all the Actelis elements on a site. For more information, see the MetaASSIST EMS User Manual.)

In This Chapter

Control of Alarmed Conditions

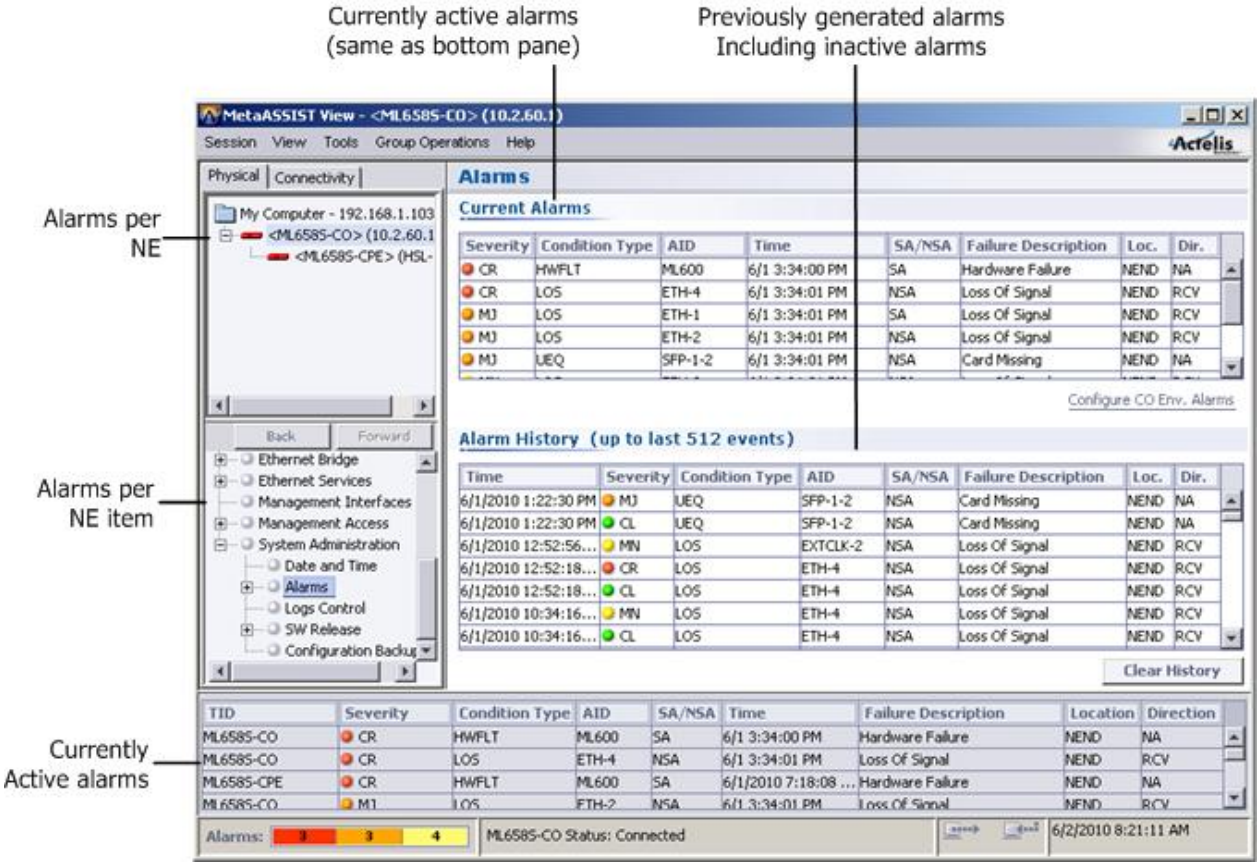
NOTE: The alarms and recommended troubleshooting procedures are described in detail in **Appendix F - Alarms Troubleshooting** (on page F-1).

The status of each NE in the Topology Tree and the status of the NE items (in the Network Element tree) are indicated by various colored icons adjacent to the unit. Every time an alarm is generated by any NE it is displayed in the bottom window area where active alarms from all NEs are displayed, as well as in the Alarms pane of the relevant Network Element. In addition, alarms that are no longer active (history) can be viewed in the Alarms pane of the relevant NE.

The following figure summarizes the available alarm displays.

- Currently active alarms for a connected NE and its hosted NEs (if the connected NE is a CO) - displayed at the bottom of the window area.
- Highest level alarm per NE - in the **Topology Tree**.
- Active alarm per NE *item* (i.e. HSL, Modem, etc.) - in the **Network Element tree**. This enables identifying the general source of the alarm.
- All (active and history) alarms for a selected NE from the Navigation tree - via the Alarms pane of the selected NE (**Alarms Pane View** (on page 13-5)).

NOTE: Clicking on an active alarm links to the NE item and invokes the corresponding pane.



The alarms' levels and notification can be customized by the user per Network Element. For example, a critical alarm can be configured to be sent as a user selected sound (**Configuring Fault Notification Sound Effects** (on page 13-9)). In addition, the fault levels for each NE component can be modified from the corresponding glance (summary) pane and customized to the operator's requirements (**About Alarm Severity and Conditions** (on page 13-8)).

When performing maintenance on a system, alarms can be disabled so fault messages are not unnecessarily sent to the control center (**Disabling Alarms for Maintenance** (on page 13-11)).

NE Connection Status

The status bar provides a short informational note about the current connection status, as detailed in the table below.

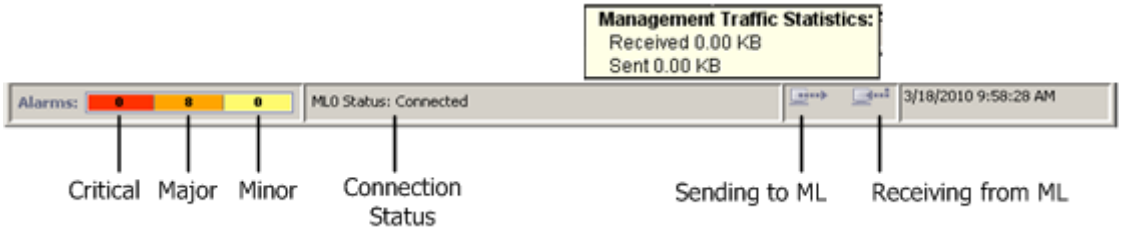


Table 61: Connection Status Table

Status	Description
Connected	MAV is logged-in to ML, via IP or IP-less (Model dependant) connection. All views are up-to-date.
Connected (Upgrade your MAV!)	MAV is logged-in to ML, via IP or IP-less (Model dependant) connection. ML uses TL1VER unregistered on MAV. All MAV-known views are up-to-date.
EOC Connected	MAV communicates with ML40 via EOC, HTTP/CLI are available apart of MAV.
Updating view	MAV is logged-in to ML, via IP or IP-less (Model dependant) connection. Views data is collecting from ML.
Trying to connect	MAV repeatedly trying and waiting for ML terminal response. May be SSH blocked (too many users) May be ACL blocked (IP or protocol denied). //In the Navigation Tree NE appears as slanted blue icon.
Login Failed	MAV stopped any attempt to connect. TL1 Session was Aborted. Telnet Session was Rejected (e.g. unknown port).
Authentication Failed	MAV stopped any attempt to connect. TL1 (local or Radius) authentication failure (user or pwd problem).
Too many sessions are open	MAV stopped any attempt to connect. TL1 Session was Rejected (Too many users on ML).
TL1 Session was Timed-out	MAV stopped any attempt to connect. Closed due to idle timeout.
TL1 Password Expired on NE	MAV stopped any attempt to connect.
Unsupported ML version	MAV stopped any attempt to connect. ML Model/SW/TL1VER discovered are unsupported by MAV SW.
Failed, SSH Key file(s) not found	MAV stopped any attempt to connect. SSH Private/Public Keys are not created or deleted.
Not Connected, IP is reachable	NE is probably not ML. Failed on Actelis discovery or TL1. MAV stopped any attempt to connect.
Not Connected, IP is unreachable	There is no communication (ping/telnet/craft prompt) to ML or other NE. MAV stopped any attempt to connect.
Click on NE to get status	When no NE is selected in Upper Navigation Tree.
Other	Other transient strings may appear.

Alarms Pane View

The **Alarms** pane displays the currently active alarms and the Alarms History tables for Network Element currently selected in the tree. The Alarms pane at the bottom provides a summary of the current alarms from all NEs displayed in the tree.

For more information on the alarms, see **Alarm Information in Summary Tables** (on page 13-7). The Alarms pane also provides access to the Environmental Alarms configuration options for that NE.

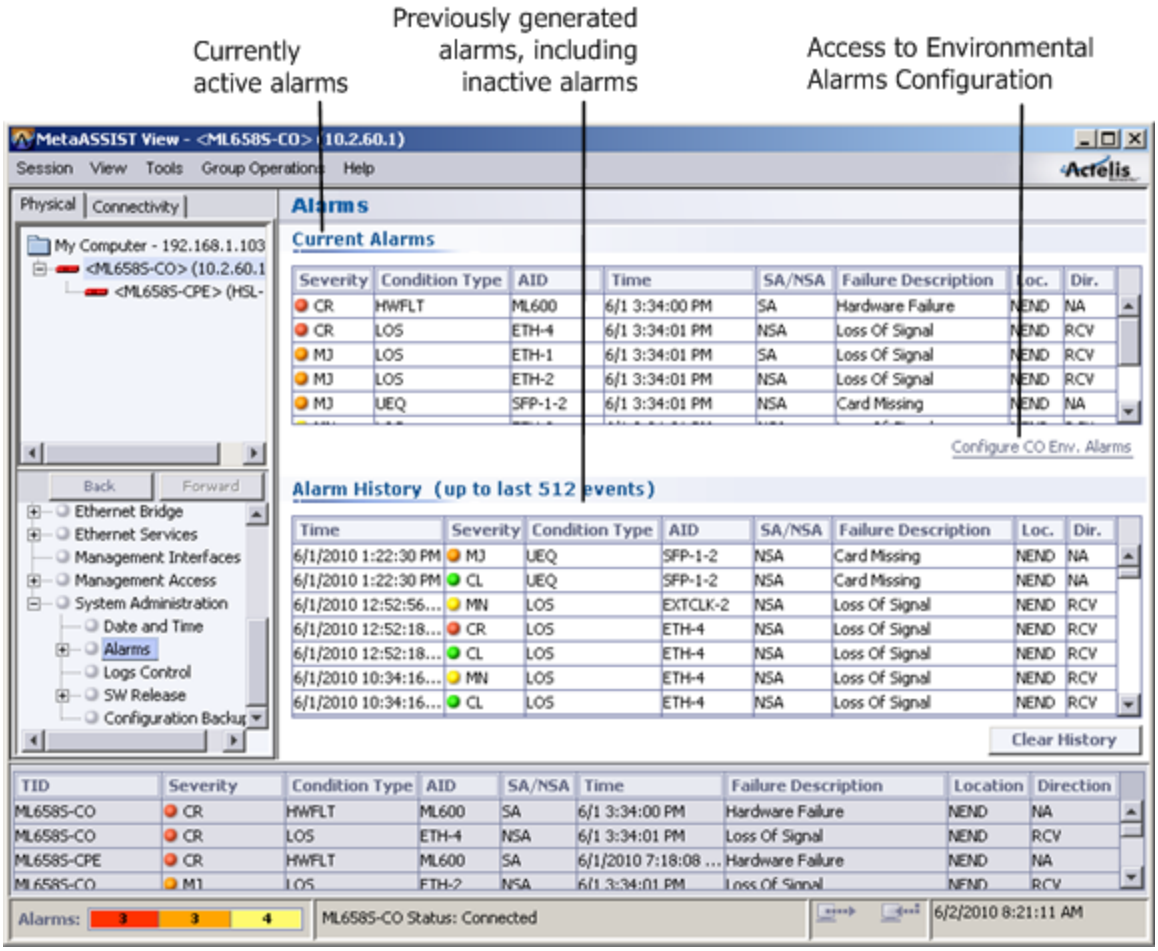
➢ **To view the Alarms pane:**

On the Navigation tree in the Network Element tree, open **System Administration, Alarms**. The **Alarms pane** opens.

The pane is divided into three areas:

- Current alarms - shows active alarms for the NE selected in the Navigation tree
- *Configure CO Env. Alarms* and *Alarms Cut Off* button - provides access to environmental alarms configuration options for the NE and Alarms Cut Off option
- Alarm History - shows all alarms generated for the selected NE, including those that are no longer active. (The display is limited to the last 512 alarms).

NOTE: To reset the Alarm History (Admin privileges only), click the **Clear History** button in the Alarm History area.



Alarm Icons and Color Map

The following table shows the various icons and the status indicated by the icon colors.

Icon meanings

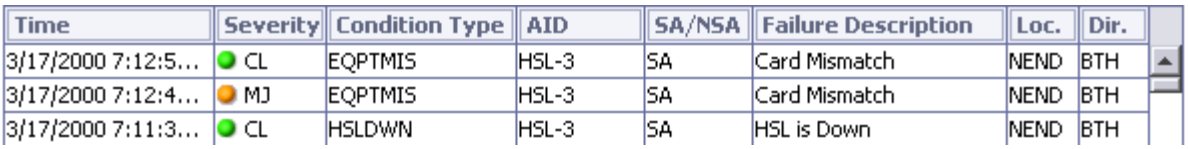
Icon	Meaning
	Gray Icon - for the following cases: No critical, major or minor alarms; Entities that have no alarm status (such as Users); Entities are disabled.
	Green icon - Cleared Alarm
	Red Icon - Critical Alarm
	Orange Icon - Major Alarm
	Yellow Icon - Minor Alarm
	Icon with an X - Inaccessible element
	Tool Icon - Maintenance mode

Alarm Information in Summary Tables

In the alarm summary tables, each alarm is displayed in a row, along with information about the alarm source. The fields may vary slightly depending on whether the alarm is viewed via the *Alarms area* at the *bottom* of the window, or the *Network Element - Alarms pane*.

The following figure shows the Alarms pane for a selected Network Element.

NOTE: Each summary fault row is directly linked to the faulty item. By double-clicking on any summary alarm row, the faulty item is accessed and its glance pane invoked.



Time	Severity	Condition Type	AID	SA/NSA	Failure Description	Loc.	Dir.
3/17/2000 7:12:5...	CL	EQPTMIS	HSL-3	SA	Card Mismatch	NEND	BTH
3/17/2000 7:12:4...	MJ	EQPTMIS	HSL-3	SA	Card Mismatch	NEND	BTH
3/17/2000 7:11:3...	CL	HSLDWN	HSL-3	SA	HSL is Down	NEND	BTH

The following table provides brief descriptions of the fields. For detailed information on troubleshooting procedures for the alarms, refer to Alarmed Conditions Tables.

Table 62: Parameter Description

Field	Description
Time/TID	The field varies according to the table summary. Provides more information such as source NE or time at which alarm was generated.
Severity	The Notification code of the alarm or message and the MTTR (Mean Time To Repair) requirement according to GR-474-CORE. • The severity levels for a Network Element item can be modified according to instructions in **Modifying Alarm Severity** (on page 13-10). • For more details on severity levels, refer to **About Alarm Severity and Conditions** (on page 13-8).
Condition Type	Condition that caused the alarm or message. All conditions are detailed in Alarmed Conditions Tables.
AID	The Access Identifier of the component (entity) involved with the alarm or message.
SA/NSA	The effect that reported event has on system operations. Possible values are: • SA means event is Service Affecting (i.e., it caused part or all traffic to be dropped) • NSA means event is Not Service Affecting (e.g., redundant power input failure).
Failure Description	Textual description of the event
Location (Loc)	The event location. Possible values are: • NEND - (Near End), the problem is in the monitored NE • FEND - (Far End), the problem is in the external system attached to the monitored • BOTH - the problem is both in the monitored and in the external system attached to the monitored

Field	Description
Direction (Dir)	Direction related to the event. Possible values are: • TRMT — the component was transmitting • RCV — the component was receiving • BTH — the component was transmitting and receiving • NA — Not Applicable

About Alarm Severity and Conditions

Table 63: Alarm and Severity Conditions

CR (Critical Alarm)	Critical indicates that a severe, usually service-affecting condition has occurred and that immediate corrective action is imperative, regardless of the time of day or day of the week.
MJ (Major Alarm)	Major is used for hardware or software conditions that indicate a serious disruption of service or the malfunctioning or failure of important circuits. These troubles require the immediate attention and response of a craft person to restore or maintain system capability. The urgency is less than in critical situations because of a lesser immediate or impending effect on service or system performance.
MN (Minor Alarm)	Minor is used for troubles that do not have a serious effect on service to customers or for troubles in circuits that are not essential to system operations.
NA (Not Alarmed)	The Not Alarmed condition is not reported as an alarm. It can be viewed as a NA condition in the Alarms and Condition tables in the appropriate views.
NR (Not Reported)	The Not Reported condition is not reported at all and does not appear in the Alarms and Condition tables.
CL (Cleared Alarm)	The Cleared Alarm notification code appears only in the Alarm History table in the Alarms pane indicating clearance of an alarm.

Configuring Fault Notification Sound Effects

MetaASSIST View provides user configurable sound effects that when enabled, are automatically applied for each ML device alarm report notification. For more information on the notification levels, refer to **About Alarm Severity and Conditions** (on page 13-8).

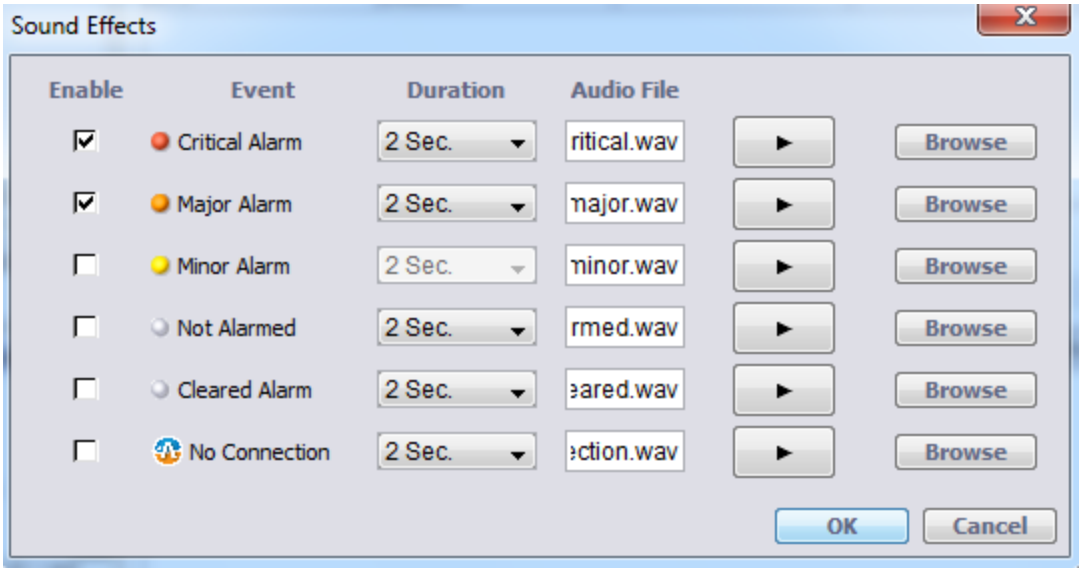
MetaASSIST View runs configurable *.WAV format files for a configurable time period of 1 to 10 seconds. Files longer than this time period are abruptly cut down and files shorter than this time period are repeated until the time runs out.

NOTE: In case of a new alarm report arriving while a previously arrived alarm report tune is being played - the new alarm will not be played at all unless the new alarm report is of a higher hierarchy, which then will interrupt the current tune and play the configured tune of the new arriving alarm.

The sound files can be selected from a default list of files and played prior to activation. The file list can be modified as necessary.

➢ **To configure sound effects:**

1. On the **Tools** menu, select **Sound Effects**. The **Sound Effects** dialog appears.



2. To enable the audio file, select the **Enable** check box next to the appropriate alarm severity.
3. From the **Duration** list box, select the time duration (1-10 seconds).
4. In the Audio File box, type the .WAV file location or locate it by clicking the **Browse** button.
5. To listen to the audio file, in the dialog box, click the **play** button: 
6. For additional alarm severities, repeat steps 2 to 6.
7. Click **OK**.

Managing Element Specific Alarms

For each Network Element item, the alarm severity can be customized and the alarms can be disabled for maintenance.

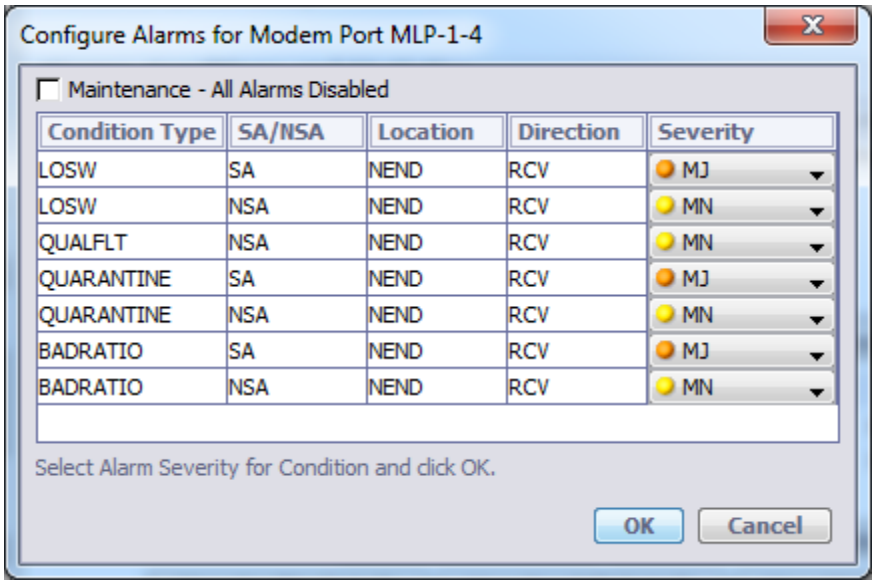
Modifying Alarm Severity

ML products generate alarms of various severities according to the entity and alarm type. The alarm severities can be modified according to the service provider's network servicing requirements. For example, the severity of the alarm may correspond to the required response time.

The alarms may also be disabled for maintenance.

➢ **To modify alarm severity**

1. Click on the item in the **Network Element** tree (i.e. HSL). The corresponding **Configure Alarms** dialog opens (i.e. Configure Alarms for the HSL).



2. Every condition type is displayed along with pre-configured information describing the condition and its default severity. See **About Alarm Severity and Conditions** (on page 13-8). The severity for any of the displayed conditions can be modified.

NOTE: To disable all alarms, check **Maintenance - All Alarms Disabled**. See **Disabling Alarms for Maintenance** (on page 13-11).

3. Click **OK** to save changes.

Operating Alarms

MetaASSIST View allows you to disable alarm display for maintenance purposes. This condition is indicated by the *Maintenance* wrench tool icon next to the relevant element in the Navigation tree and in entities that report alarms. When Modem ports or Ethernet ports are placed in Maintenance mode, service is interrupted on the port. A warning message appears prior to performing this action.

After completing maintenance, make sure you enable the alarms.

NOTE: Users with **write** and **admin** privilege rights can disable alarms from panes using the **Configure Alarms** button. Disabled entities cannot be placed in maintenance mode.

➢ To disable alarms

1. In the Network Element tree, open the required entity. The entity detailed pane opens in the work area.
2. From the work area (in Alarms and Conditions section), click **Configure Alarms**. The **Configure Alarms** dialog appears.
3. Select the **Maintenance - All Alarms Disabled** check box.
4. Click **OK**. The Maintenance  icon appears.

NOTE: To enable alarms, clear the **Maintenance - All Alarms Disabled** check box.

Error Counters, Measurements and Threshold Alerts

The MetaASSIST View provides a set of functions and capabilities necessary for the system to gather and store a range of counters associated with parameters monitored over the network. These counters enable systematic monitoring of the ML device through continuous collection and analysis. The counters are accumulated over pre-determined accumulation periods (15-minutes and 1-day) and maintained in designated storage counters. Additional counters are provided to maintain a recent history of the parameters as follows:

- Up to 32 (15 minute) Historic counters are supported (in addition to the current 15 min counter)
- Up to seven (single day) Historic counters are supported (in addition to the Current single day counter)

In addition, *threshold alerts* are generated in case PM counter crossed a pre-configured threshold value.

These monitoring options are accessed via the **PM Operations Pane** (on page 13-13). The pane is available for various items (e.g. MEP) The pane options differ depending on the element.

PM Operations Pane

The Performance Monitoring options are accessed via the **Glance** pane of the corresponding element. This section describes the relevant PM functions, using the MEP performance counters as an example.

➢ **To access the (MEP) PM options**

From the **Network Element** tree, under **Ethernet Services** click **MEPs** to access the MEP PM options (whereas other PM are accessed through the relevant panes. The relevant pane appears.

The figure below shows a partial image of the MEP pane with the PM options. The options are relevant to the *selected* item (i.e. MEP).

NOTE: Most PM dialog boxes use the same attributes as described in the PM Attribute Descriptions section.

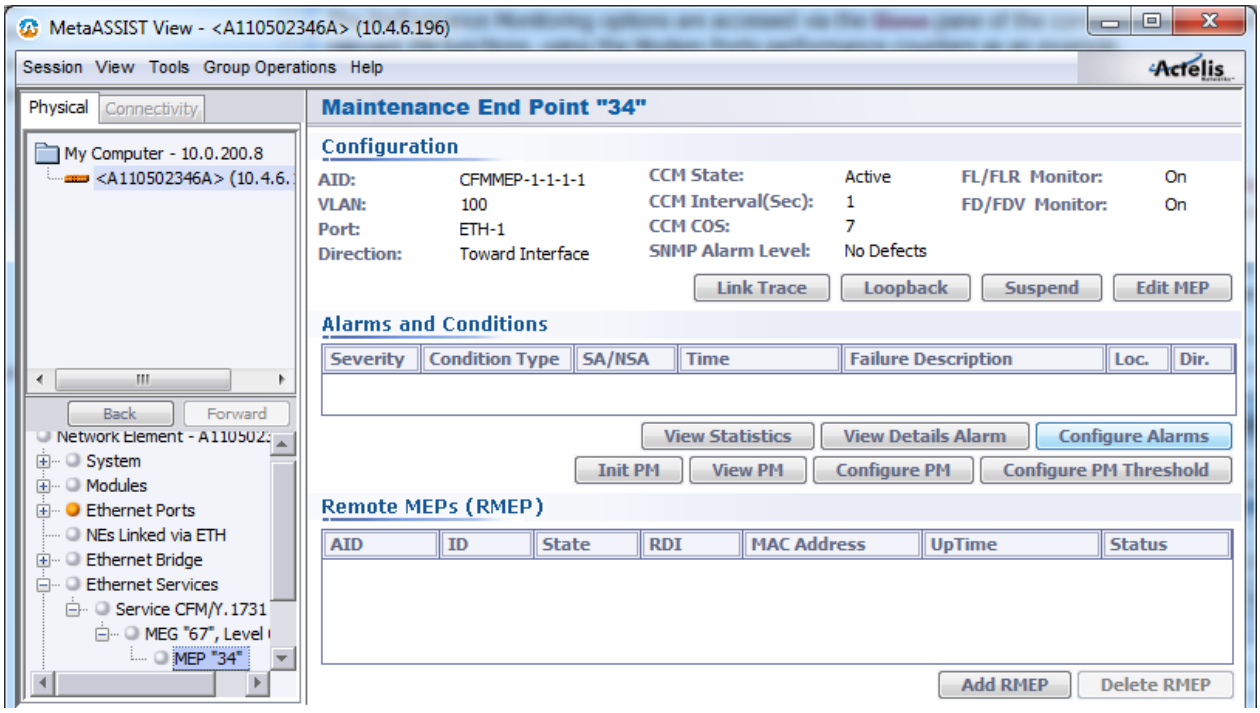


Table 64: PM Options

Button	Description
Init PM (on page 13-18)	Accesses a dialog for resets the selected PM counter and setting the counter acquisition intervals.
Init PM all	Resets all PM counters *without an authorization prompt.*
View PM	Displays the PM counters data, data may be filtered in advance (to shorten the time the operation takes).
Configure PM	Used to disable PM on irrelevant line segments. By default, PM is enabled on all line segments.
Configure PM Threshold	Configures the Thresholds for PM crossing alert, fields may be filtered in advance (to shorten the time the operation takes).

Viewing the Counters and Filtering the Display

In general, performance parameters are raw counts derived by the processing of performance primitives within 1 second intervals. At the end of each second, the data in the current second counter is nominally moved to the current period counters, unless some other action is warranted. At the end of each accumulation interval, the current value of the performance parameter counter is saved in a corresponding "previous period" counter, and the "current counter" is reset to zero.

Performance parameters are accumulated over pre-determined accumulation periods (15-minutes and 1-day) and maintained in designated storage counters. Additional counters are provided to maintain a recent history of the parameter on modem as follows:

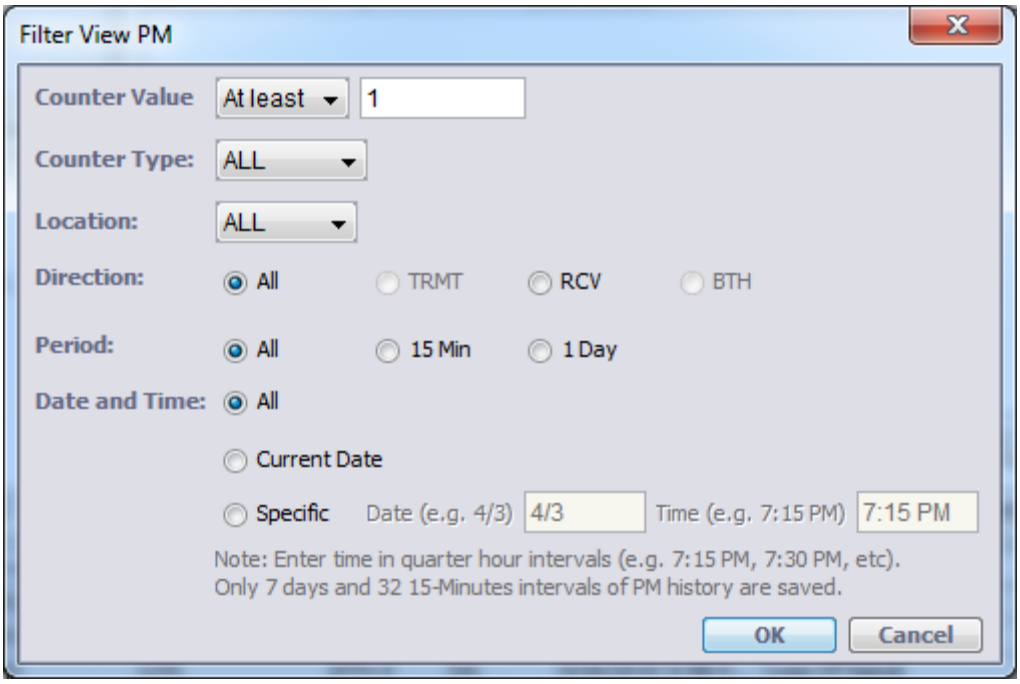
- Up to 32 (15 minute) Historic counters are supported (in addition to the current 15 min counter)
- Up to seven (single day) Historic counters are supported (in addition to the Current single day counter)

Each interval can be defined as incomplete or invalid for that interval. This might happen if the user resets the counter or changes the time of day during the interval.

These storage counters are acting as a pushdown stack. That is, a new value is stored at the most recent history counter, data in every history counter is shifted down to the next most recent history counter, and the last value in the history is discarded.

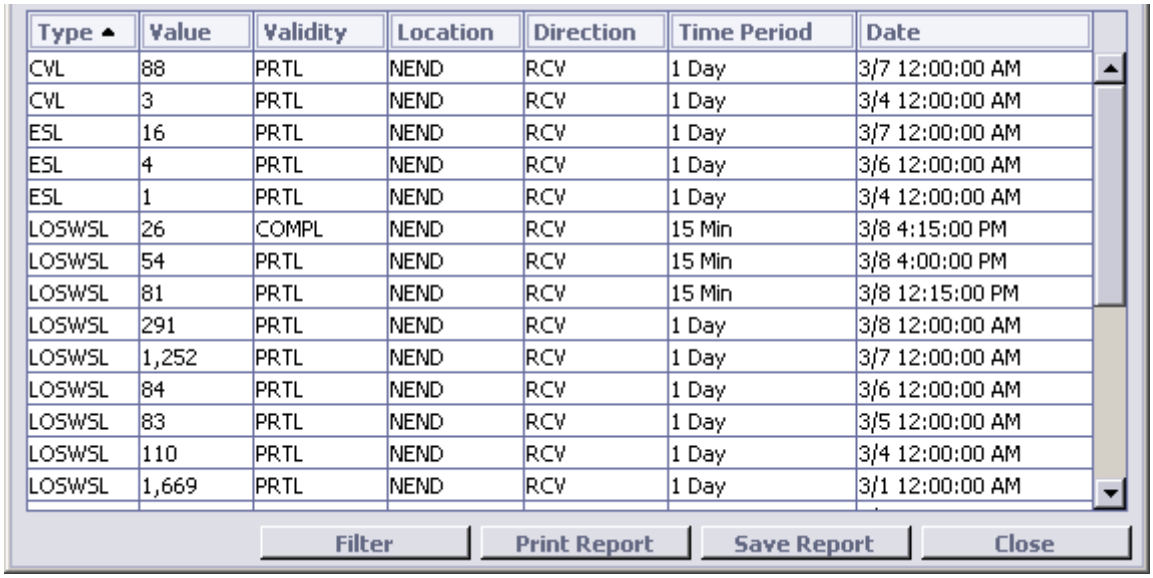
➢ To filter the display and view the counters

1. From the appropriate Glance pane with the **PM Operation** (on page 13-13) options, click **View PM.** The **Filter View PM** dialog appears.



2. From the **Counter Value** box, select a discriminating filter for the counters presentation: At least or At most.
3. select the **Counter Type** list box, select a **counter type** (on page 13-19). See **Counter Types** (on page 13-19) for a description of the counters.
4. Select the **Location, Direction** and **Period** options as required.
5. Select **Date and Time** options:
   - All - displays all counters acquired
   - Current date - displays counters acquired over the current date (today)
   - Specific - displays counters acquired over the specified time period.

6. Click **OK**. The **View PM** dialog appears.



Type	Value	Validity	Location	Direction	Time Period	Date
CVL	88	PRTL	NEND	RCV	1 Day	3/7 12:00:00 AM
CVL	3	PRTL	NEND	RCV	1 Day	3/4 12:00:00 AM
ESL	16	PRTL	NEND	RCV	1 Day	3/7 12:00:00 AM
ESL	4	PRTL	NEND	RCV	1 Day	3/6 12:00:00 AM
ESL	1	PRTL	NEND	RCV	1 Day	3/4 12:00:00 AM
LOSWSL	26	COMPL	NEND	RCV	15 Min	3/8 4:15:00 PM
LOSWSL	54	PRTL	NEND	RCV	15 Min	3/8 4:00:00 PM
LOSWSL	81	PRTL	NEND	RCV	15 Min	3/8 12:15:00 PM
LOSWSL	291	PRTL	NEND	RCV	1 Day	3/8 12:00:00 AM
LOSWSL	1,252	PRTL	NEND	RCV	1 Day	3/7 12:00:00 AM
LOSWSL	84	PRTL	NEND	RCV	1 Day	3/6 12:00:00 AM
LOSWSL	83	PRTL	NEND	RCV	1 Day	3/5 12:00:00 AM
LOSWSL	110	PRTL	NEND	RCV	1 Day	3/4 12:00:00 AM
LOSWSL	1,669	PRTL	NEND	RCV	1 Day	3/1 12:00:00 AM

Filter Print Report Save Report Close

7. You may **Save Report** in HTML format or **Print** the report.
8. To change the Filter, click **Filter**. The **Filter View PM** dialog appears.

PM Attribute Descriptions

Most PM dialog boxes use the following attributes as described below.

Table 65: View PM parameter list

Parameter	Description
Type	The counter types include all possible counters for this interface, see MLP PM Types and **MEP PM Types** (on page 13-20)
Value	The measured value of the monitored parameter.
Validity	Indicates availability and reliability of information in a particular interval as follows: ADJ - Data has been manually adjusted or initialized; COMPL - Data has been accumulated over the entire time period; LONG - Data accumulated over greater than the indicated time period; NA - Data is not available; OFF - Performance monitoring was turned off as configured in the **Turning On/Off the PM Counters** (on page 13-19); PRTL - Data is accumulated over some portion of the time period.
Location	The location of the required information: NEND - Near End or FEND - Far End.
Direction	Direction for monitor or control operation. The direction to ML device is Receive (RCV). The direction from ML device to external equipment is Transmit (TRMT). ALL - All directions (RCV only is supported); TRMT - Transmit direction only (not supported); RCV - Receive direction only; BTH - Both directions (not supported).

Parameter	Description
Time Period	The accumulation time period (interval) for PM parameters. Default value is 15 min.
Date and Time	The starting date and time of the selected monitoring interval. Can be: **All** - For any applicable date and time when all available intervals are monitored. **Current** - Current date and time of the system. **Specific** - Specific date and time
Threshold	The threshold value of a specific PM counter. Thresholds are applicable for both 15-minute and 1-day current intervals. Threshold value equals to 0 implies that threshold control is disabled. If the Threshold value is empty, no change can be made in multiple operations.

System Time of Day (TOD) adjustment will cause performance data interval timestamp changes as follows:

- When TOD is adjusted forward or backward then ALL recent history interval timestamps are changed forward or backward accordingly;
- When TOD changes due to DST(Daylight Saving Time) start (one hour is skipped), then recent history intervals sequence will skip the non-existing hour, e.g. 01:15; 01:30; 01:45; <DST start> 03:00; 03:15, etc. sequence will appear;
- When TOD changes due to DST end (last hour is repeated twice), then recent history intervals will represent this hour twice (before and after DST end) by intervals with duplicated timestamps, e.g. 01:00, 01:15; 01:30; 01:45; <DST stop> 01:00; 01:15, etc. sequence will appear;
- Changing the DST range can cause a shift in interval timestamp as follows:
  - If an interval was collected within the DST range and after changing the range it is not within the DST range then its timestamp will shift backward;
  - If an interval was collected outside the DST range and after changing the range it is within the DST range then its timestamp will shift forward.
- TOD changes can cause partial or long intervals.

Configuring PM Counters Collection

The PM counter collection can be configured by setting the following parameters:

- Start time within a 24 hour day when the accumulation process starts
- The frequency at which the counters are collected
- The line segments over which counters are collected - by default, counters are collected from all line segments

Setting PM Start Time

Use the steps described in this section to set the time in the day when the PM starts.

➢ **To set the PM time:**

1. In the Network Element tree, under **System Administration**, select **Date and Time**. The **Date and Time** pane opens.
2. In the invoked pane, under **Local Time,** click **Set PM Time.** The **Set Daily PM Start** dialog appears.

3. From the **PM Start Time** list box, select the start hour when the PM counter accumulation begins. Click **OK**.

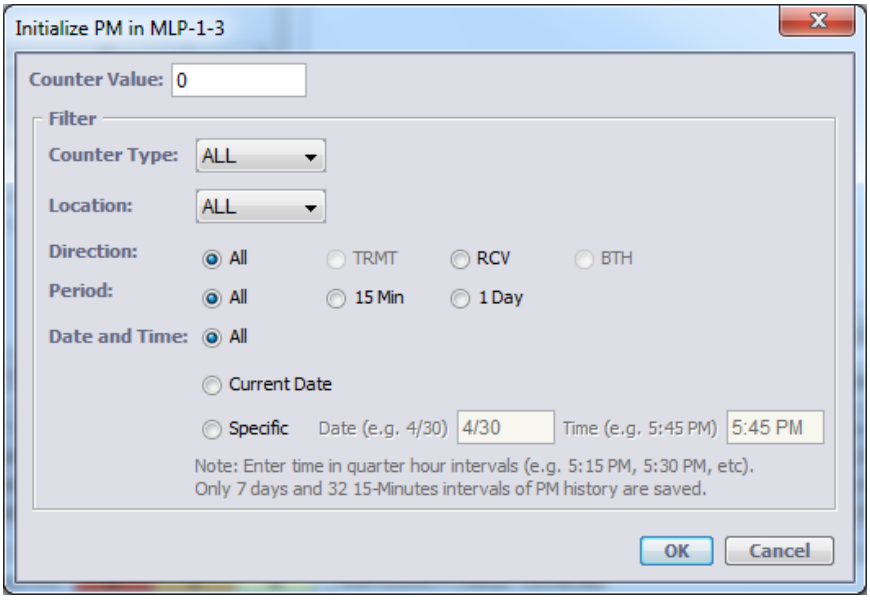
Initializing PM Counter

The initialization resets or sets a specific value to the PM counter selected by the filter. ALL the counters can be reset at once by clicking the **Init PM ALL** button in the **PM Operations pane** (on page 13-13).

➢ **To configure the PM counters collection**

NOTE: The procedure described below is the same for all counters.

1. From the appropriate pane (see **PM Operations Pane** (on page 13-13)), click **Init PM**. The **Initialize PM in MLP** dialog appears.



2. Set the **Counter Value** - sets the value of the selected counter(s), default value is '0'. The counters that are initialized are determined by the Filter.
3. Filter:
   - **Counter Type** - determines the type of counters (i.e. ESL, UASL). You may choose to collect All counter types, a specific counter type or counter types from NEND or FEND.
   - **Location -** determines the location along the span from which the counters are collected. You may choose to collect counters from the complete span (All) or from a specified segment in the span (i.e. NEND, FEND).
     Direction – Direction is always Receive (equivalent to All).
     Period - determines the counter values will be collected:
   - All - all counters
   - 15 Min - 15 minutes counters
   - 1 Day - one day counters

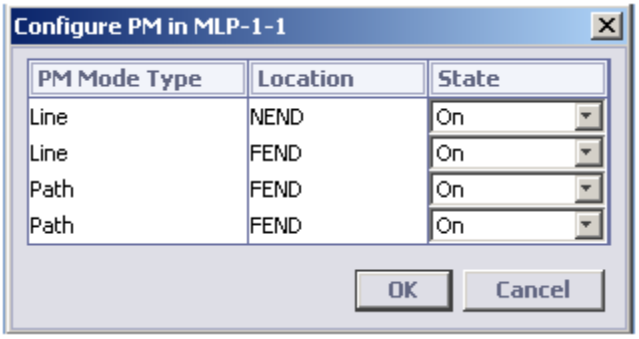
   Date and Time over which the counters are saved:
   - All - continuously saves counters
   - Current Data -
   - Specific - saves counters generated on the specified dates.
4. Click **OK**.

Enabling/Disabling Line Segment's PM collection

The **Configure PM** button opens the Configure PM dialog box that allows you to turn on or off the PM counters.

➢ **To turn the PM counters on or off for each modem:**

1. In the **Network Element** tree, open **Modem Ports, Modem Port MLP <ID>**. The Modem Port MLP <ID> pane opens.
2. In the **Alarms, Conditions and Statistics** area, click **Configure PM**. The Configure PM in MLP <ID> dialog appears.



   Each PM is displayed according to Mode Type, Location and State (ON/OFF).
3. To disable a PM Mode type, from the **State** list box, click **Off**.
4. Click **OK**.

Counter Descriptions per Element Type

This section describes the Counter types for each element.

NOTE: Some of the counters are common, while others are specific to each type of line.

MLP PM Counter Types (NEND and FEND)

ML device modems provide the following PM types.

Table 66: PM Counter Type for NEND and FEND

Parameter	Description
CVL	Code Violation-Line. Number of Line Coding Violations (CV-L) that occurred during the interval. On CO model, locn=NEND, dirn=RCV means US, locn=FEND, dirn=RCV means DS. On CPE model, locn=NEND, dirn=RCV means DS, locn=FEND, dirn=RCV means US.
ESL	Number of line errored seconds. The DSL parameter Errored Second is defined as a count of 1-second intervals during which one or more CRC anomalies are declared (and/or one or more LOSW defects are declared). Errored Seconds (ES) are not counted during UnAvailable Seconds (UAS).
FECC	Count of FEC (FFEC for xTU-R) anomalies (corrected code words) occurring in the channel during the interval. This parameter is inhibited during UAS or SES. If the FEC is applied over multiple channels, then each related FEC (or FFEC) anomaly SHOULD increment each of the counters related to the individual channels.
FECSL	Count of seconds during this interval that there was at least one FEC correction event for one or more bearer channels in this line. This parameter is inhibited during UAS or SES.
FINITFLT	Count of failed full initializations on the line during this interval.
FINITSUM	Count of full initializations attempted on the line (successful and failed) during this interval.
INM-IAT0-L to INM-IAT7-L	Count of Inter arrival time of Impulse Noises. Graphical representation is also available. Refer to **Impulse Noise Monitoring** (on page 6-29).
INM-INPEQ1-L to INM-INPEQ17-L	Count of required equivalent Impulse Noises protection. Graphical representation is also available. Refer to **Impulse Noise Monitoring** (on page 6-29).
LOSSL	Count of Loss Of Signal
SESL	Count of Severely Error Seconds
UASL	Count of Unavailable Seconds

MEP PM Counter Types

The following table summarizes the MEP counters.

Table 67: MEP PM Counter Type

Parameter	Description
FDV	• Frame Delay Variation is defined as the value (in microsec) between the average and the minimal Frame Delay measured during monitored interval. See implementation details on **Y.1731 Tools** (on page 11-26). • Frame Delay is reported on MEP AID, per RMEP-{1-5} locations individually. To get counters, MEP FD parameter should be set to Y, and at least 1 RMEP should be defined in the MEP
FLR	• Frame Loss Ratio is a measurement in a percentile form of Frame Loss relatively to Total Frame (received or sent). • Frame Loss Ratio is reported in 0.001% units , i.e. 50 means 0.05% of FLR. • Frame Loss Ratio is reported on MEP AID, for NEND/FEND/RMEP-{1-5} locations as defined for FL counter. • Frame Loss Ratio during the interval is recalculated each 1-minute to provide averaged and reliable result. • See implementation details on **Y.1731 Tools** (on page 11-26).
FD	• Frame Delay is a measurement of traffic round-trip delay, in microsecond units. • See implementation details on **Y.1731 Tools** (on page 11-26). • Frame Delay is reported on MEP AID, per RMEP-{1-5} locations individually. To get counters, MEP FD parameter should be set to Y, and at least 1 RMEP should be defined in the MEP.
FL	• Frame Loss is a counter reports (in frames) number of unexpectedly lost frames. Frame Loss is reported on MEP AID, for NEND and FEND location, suitable for E-Line deployments. NEND location means Ingress direction (MEP RX direction quality). • FEND location means Egress direction (MEP TX direction quality). To get counters for NEND/FEND locations, MEP SEQNUM parameter should be set to N, MEP FL parameter should be set to Y, and at least 1 RMEP should be defined in the MEP. • Frame Loss is reported on MEP AID, per NEND and RMEP-{1-5} locations, suitable for E-Line/E-LAN/ E-Tree deployments. To get counters of MEP RX (Ingress) direction quality per each RMEP individually, MEP SEQNUM parameter should be set to Y, MEP FL parameter should be set to Y, and at least 1 RMEP should be defined. • See implementation details on **Y.1731 Tools** (on page 11-26).

Threshold Alerts

The following sections describe the process of **setting PM counter threshold** and of **Viewing PM threshold crossing alerts**.

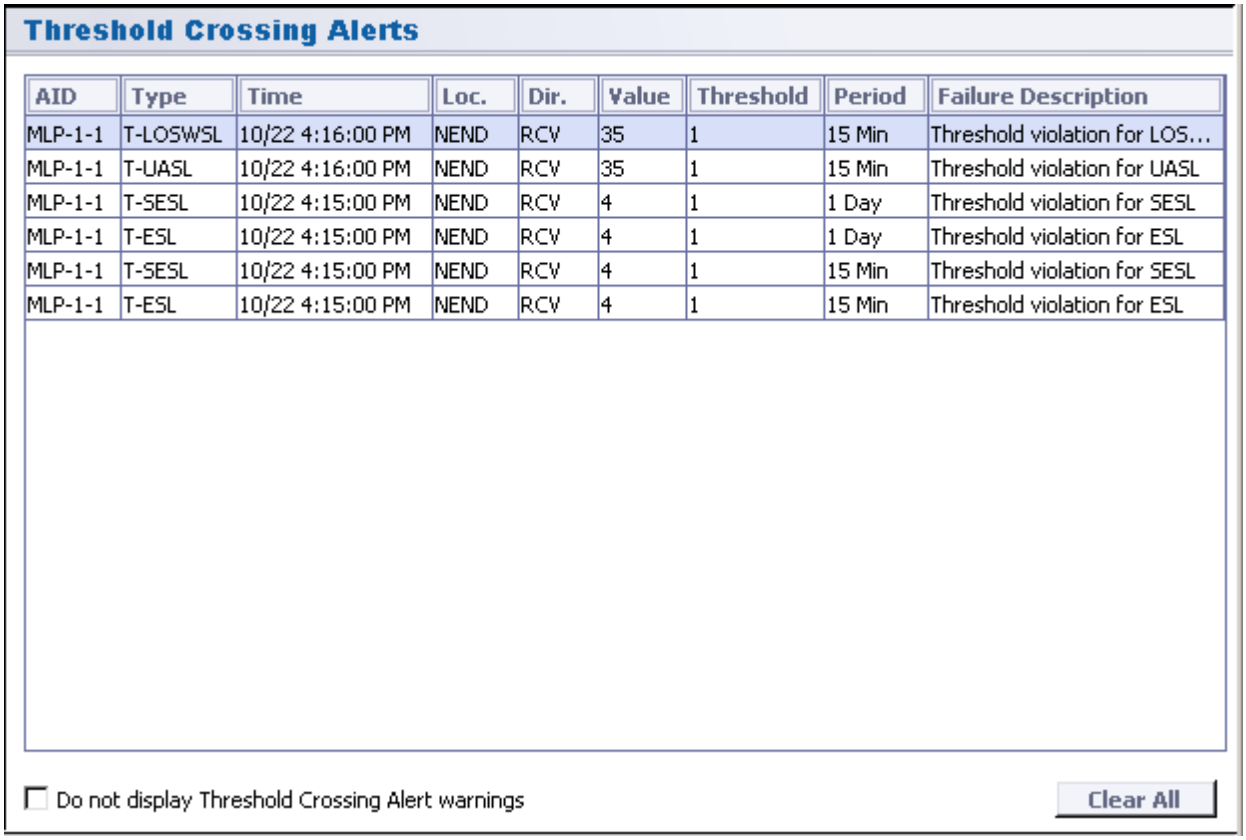
Viewing PM Threshold Crossing Alerts

The ML device reports the PM counters threshold crossing event by notification (alert and not alarm) which do not persist and is not retrievable from the ML device. MetaASSIST View collects the notifications (while the session with the specific ML device is open) and displays all notifications in glance view on a separate pane, accessible from Network Element Tree, **System Administration**, **Alarms**, **and Threshold Crossing Alerts**.

Notifications can be disabled via the **Threshold Crossing Alerts** (TCA) pane or when a pop-up notification appears.

➢ To monitor threshold cross alerts

1. In the **Network Element** tree, open **System Administration**, **Alarms**, **Threshold Crossing Alerts**. The **Threshold Crossing Alerts** pane opens.



2. To clear all Threshold Crossing Alerts, click **Clear All**.
3. To stop displaying Threshold Crossing Alert warnings, select **Do not display Threshold Crossing Alert warnings** check box. This step should be repeated for each NE to avoid TCA warnings from displaying.

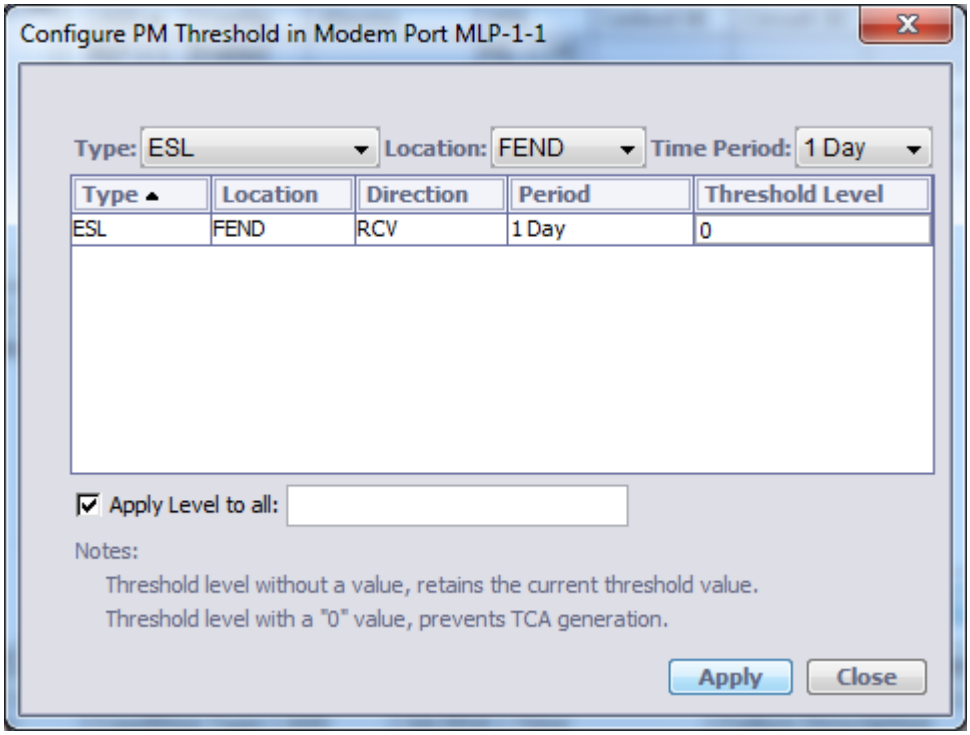
In case TCA warning appears, either click **Close** to close the dialog box or click **Do not display Threshold Crossing Alert warnings** check box to stop displaying future TCA warnings on this NE. Repeat this step for each NE when TCA warning appears.

Setting PM Counter Thresholds

The **Configure PM Threshold** button allows setting threshold control on PM counters. The Threshold can be assigned per each MLP individually, for each PM counter type, for 15-min and 1-day interval separately.

➢ **To set threshold control for each modem:**

1. In the **Network Element** tree, open **Modem Ports, Modem Port MLP <ID>**. The **Modem Port MLP <ID>** pane opens.
2. Click **Configure PM Threshold**. The **Filter Configure PM Threshold** dialog appears.



The filtering options allow you to minimize the amount of data to configure:

- **Type -** lists the counter types. Select a specific counter type or ALL to set the threshold for all counters.
- **Location** - select a specific (NEND, FEND, Line-x, etc.), or ALL to set the threshold for counters from all locations.
- **Time Period -** select **Period** over which the threshold will be applied (recommended selection is 1 Day).

3. In the **Apply level to all,** enter the threshold level value (in seconds). This causes an alert report when the number of counted error seconds exceeds crosses configured threshold level. (Note that '0' level, prevents TCA generation.
4. Click **OK**.

Ethernet Performance Monitoring

This section describes the available Ethernet performance monitoring options. These include:

- Port Statistics
- Bandwidth Usage
- MAC Forwarding Database
- Ethernet Service OAM MEP Performance
- Ethernet Connection (CO-CPE Linked)
- Ethernet Topology (other NE Linked)

Port Statistics

For each Ethernet port, statistics on the traffic can be displayed. For example, Rx and Tx frames, discarded frames, valid and invalid frames, etc.

Ethernet statistics counters can be manually reset. These counters are also automatically reset when Ethernet port (ETH <ID>, COLAN (MGMT), HSL<ID>) is deleted or reverted to factory setup. All counters support 64 bits.

➢ **To view statistics for a selected Ethernet port**

Invoke the pane of the individual Ethernet port (The Ethernet Port Workspace) and click the **View Statistics** button. The **Ethernet Statistics** dialog appears. Use the **Reset** and **Refresh** buttons to initialize and update the statistics values.

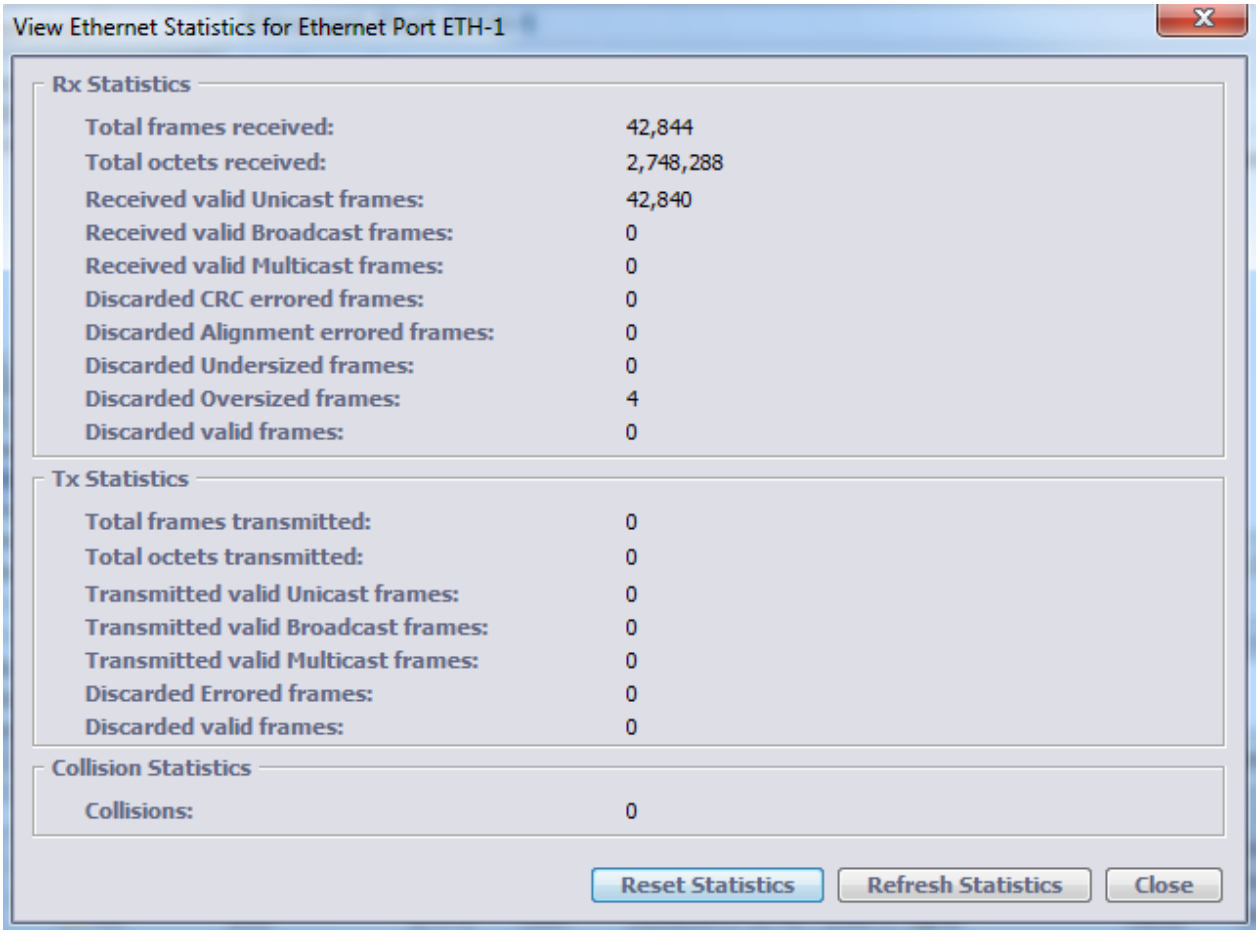


Table 68: Rx Ethernet Statistics

Rx Counter	Description
Total frames received	The total number of frames received by this interface. Counts all frames before sanity validation (errors, MFS size, etc.)

Rx Counter	Description
Total octets received	The total number of octets received on the interface, including framing characters. The ingress port buffer truncates frames of any size larger than the MFS, and the truncated octet tail is not counted in this counter.
Received Valid Unicast frames	The number of valid unicast frames received by this interface. In ML700, Multicast and Broadcast frames are counted together with Unicast.
Received Valid Broadcast frames	The number of valid broadcast frames received by this interface.
Received Valid Multicast frames	The number of valid multicast frames received by this interface
Discarded CRC-error frames	The number of received legal size frames discarded due to CRC errors Counts both Discarded CRC-error frames and Discarded Alignment-error frames.
Discarded Alignment-error frames	The number of received legal size frames discarded due to alignment (not byte-aligned) errors Not in use, is counted by Discarded CRC-error frames.
Discarded Undersized frames	The number of received and discarded as inbound undersized (less than 64 Bytes) frames with or without CRC errors.
Discarded Oversized frames	The number of inbound oversized frames larger than the MFS (Maximum Frame Size), with or without CRC errors.
Discarded valid frames	• The number of inbound frames that were discarded even though no errors had been detected. • Frames discarded due to Ingress Rate Limit are not counted. • Frames may be discarded for one of the following reasons: • VLAN violation: undefined VLAN or Frames with VID that is not allowed on the port. • MAC address violation: frame with identical; source/destination MAC addresses, frame switched back to its ingress port, etc. • Congestion on ingress port. • Frame switched to an egress port which is down; • Frame somehow received on an ingress port that is down. • Frame is switched to an egress port that is congested (for example, when egress rate limit is applied on that port). • IEEE Reserved Multicast Frames are dropped as configured via L2CP control table (for example STP BPDU or OAM PDU). • IEEE 802.3 Pause Frames are counted as discarded regardless of Flow Control configuration on the port.

Table 69: Tx Ethernet Statistics

Tx Counter	Description
Total frames transmitted	The total number of frames transmitted by this interface.
Total octets transmitted	The total number of octets transmitted out of the interface, including framing characters

Tx Counter	Description
Transmitted Valid Unicast frames	The number of valid unicast frames transmitted by this interface.
Transmitted Valid Multicast frames	The number of valid multicast frames transmitted by this interface. For frames configured to be dropped by L2CP application, the Tx counter is not incremented.
Transmitted Valid Broadcast frames	The number of valid broadcast frames transmitted by this interface.
Discarded error frames	The number of outbound frames that were discarded because of errors during transmission
Discarded valid frames	The number of outbound frames that were discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a frame could be to free up buffer space. Egress Rate limited frames are counted by receiver port counter as Rx discarded valid frames. If flow control is ON but link partner does not obey Pause, discarded frames are not counted.

Table 70: Tx Ethernet Statistics

Collision	Description
Collisions	The number of collisions detected. This is only an estimate of the number of collisions and can only be detected while in transmit mode, but not while in receive mode.

Bandwidth Usage

ML700 devices enable monitoring the Ethernet bandwidth parameters per port and per *service*. This section describes both options.

Ethernet Interface Bandwidth Monitoring

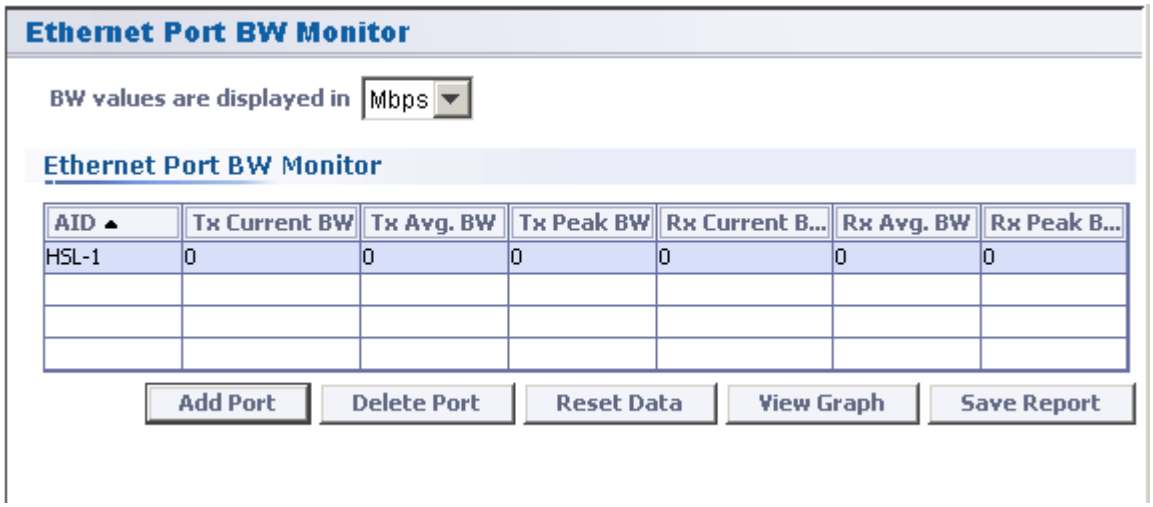
MetaASSIST View allows you to monitor bandwidth usage (average, current or max) during on-going sessions for up to four ports at a time. In addition, a graph of the transmitted and received bandwidth can be displayed for individual ports.

Monitoring Port Bandwidth Parameters

You can monitor the bandwidth parameters for up to four user defined ports at a time.

➢ **To monitor the bandwidth of an Ethernet port**

1. In the Network Element tree, open **Ethernet Bridge**, **Port BW Monitor**. The **Ethernet Port BW Monitor** pane opens.



Each line in the pane contains a port added for monitoring and information on that port bandwidth. Up to four ports can be defined.

NOTE: Use the **BW Presentation in** to determine the measurement units of the display. Note that when choosing the **View Graph** option, the measurement units will be as selected in the **BW Presentation in** field.

2. To add a port to the list:
   - Click **Add Port**. The **Add Port for BW Monitoring** dialog appears.

   - From the **Port** list box, select the port and click **OK**.
   - Repeat for additional ports.
3. You can also perform the following operations:
   - Clear statistics on selected ports - select the relevant ports (more than one port may be selected at a time) and click **Reset Data**.
   - Delete selected ports from the list - select the relevant ports (more than one port may be selected at a time) and click **delete**.
   - View a graph of the average Tx and Rx bandwidth of a selected port - select the port and click **Show Graph.** Refer to **Port Traffic Graph** (on page 13-30).

Port Traffic Graph

MetaASSIST View allows you to view a graphical representation of the Port traffic over time. You can view either the Tx and Rx or both concurrently on the same graph. The graph can also be saved to a report in .csv or .html format.

NOTE: Graphs may slow down PC operation due to lack of resources.

➢ **To display the graph**

1. In the Network Element tree, open **Ethernet Bridge**, **Port BW Monitor**. The **Ethernet Port BW Monitor** pane opens.
2. On the table, select a row.
3. Click **View Graph**. The **BW Monitor for <Port>** dialog appears.

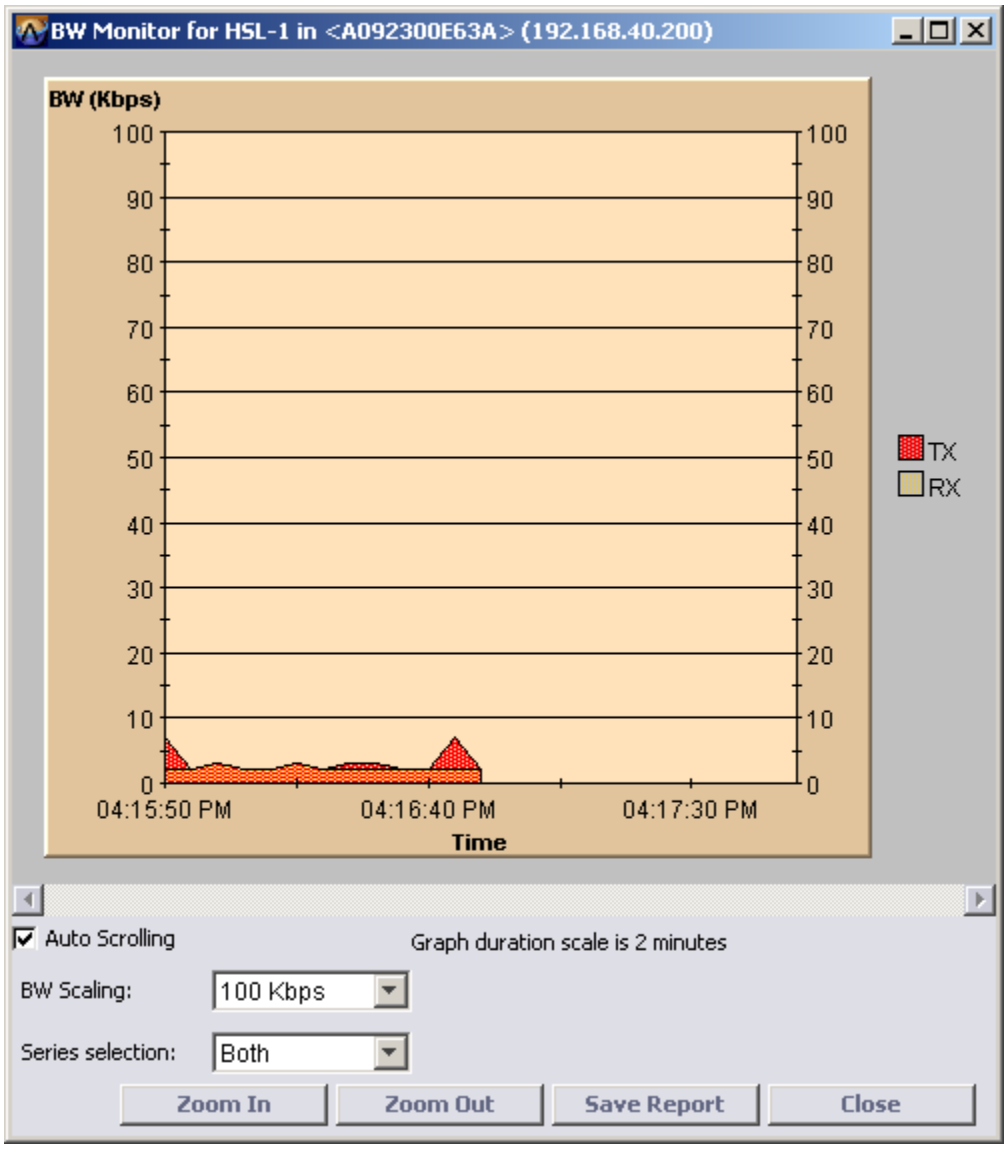


Table 71: Navigating the Graph

To....	Do this....
Choose the display	Select the item in **Series Selection**
Disable Auto-Scrolling (option is enabled by default)	Clear the **Auto Scrolling** check box
Modify BW Scaling	Select the required value from the **BW Scaling** drop box
Display Tx data, Rx data or both	Under **Series Selection** choose the type of data (Tx, Rx or Both)
Zoom-in or -Out	Use the **Zoom-in** and **Zoom-out** buttons
Save the report	Click the **Save Report** button, and choose the requested location and format (html or csv)

Service Bandwidth Monitoring

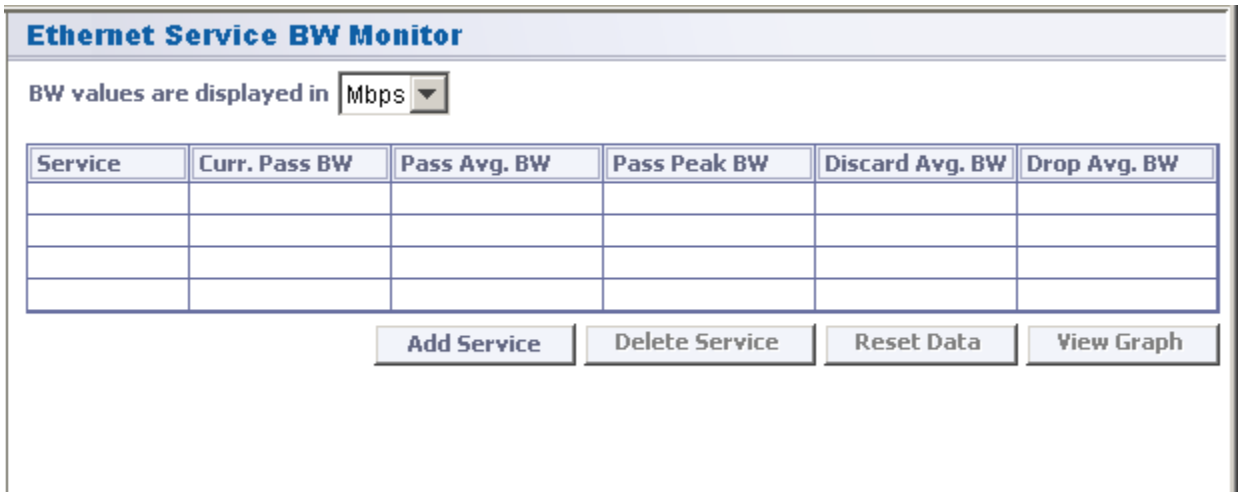
MetaASSIST View allows you to monitor Ethernet BW usage (average, current or max) during on-going sessions for up to four services at a time. In addition, a graph of the transmit and receive bandwidth can be displayed for individual services.

Monitoring Service Parameters

You can monitor the bandwidth parameters for up to four user defined services at a time.

➢ **To monitor the bandwidth of a service**

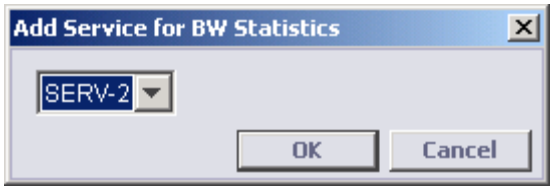
1. In the Network Element tree, expand **Ethernet Services** and click **Service BW Monitoring**. The **Ethernet Service BW Monitor** pane opens.



   Each line in the pane contains a service added for monitoring and information on that service bandwidth. Up to four services can be defined.

2. The **BW Values are displayed in** sets the measurement units of the display. Note that when choosing the **View Graph** option, the measurement units will be as selected in the **BW Values are displayed in** field.
3. To add a service to the list:

- Click **Add Service**. The **Add Service for BW Statistics** dialog appears.



- From the list box, select the service and click **OK**.
- Repeat for additional services to be monitored.

4. You can also perform the following operations:
   - Clear statistics on selected services - select the relevant services (more than one service may be selected at a time) and click **Reset Data**.
   - Delete selected services from the list - select the relevant services (more than one service may be selected at a time) and click **delete**.
   - View a graph of the average Tx and Rx bandwidth of a selected service - select the service and click **Show Graph.** Refer to **Service Bandwidth Graph** (on page 13-32).

Service Bandwidth Graph

MetaASSIST View allows you to view a graphical representation of the Port traffic over time. You can view either the Tx and Rx or both concurrently on the same graph.

Note the following:

- By default, the graph auto scrolls. You can disable the auto scroll by clearing the **Auto Scrolling** check box.
- BW scaling can be modified via the **Resolution** list box with values of 100Kbps, 1 Mbps, 10 Mbps, 100 Mbps and 1 Gbps.
- The window size in seconds or minutes is always displayed.
- You can zoom in and zoom out of the display.

NOTE: Graphs may slow down PC operation due to lack of resources.

➢ **To display the graph:**

In the **Network Element** tree, open **Ethernet Services**, **Service BW Monitor**. The **Service BW Monitor** pane opens. On the table, select a row. Click **View Graph**. The BW Monitor for <Port> dialog appears.

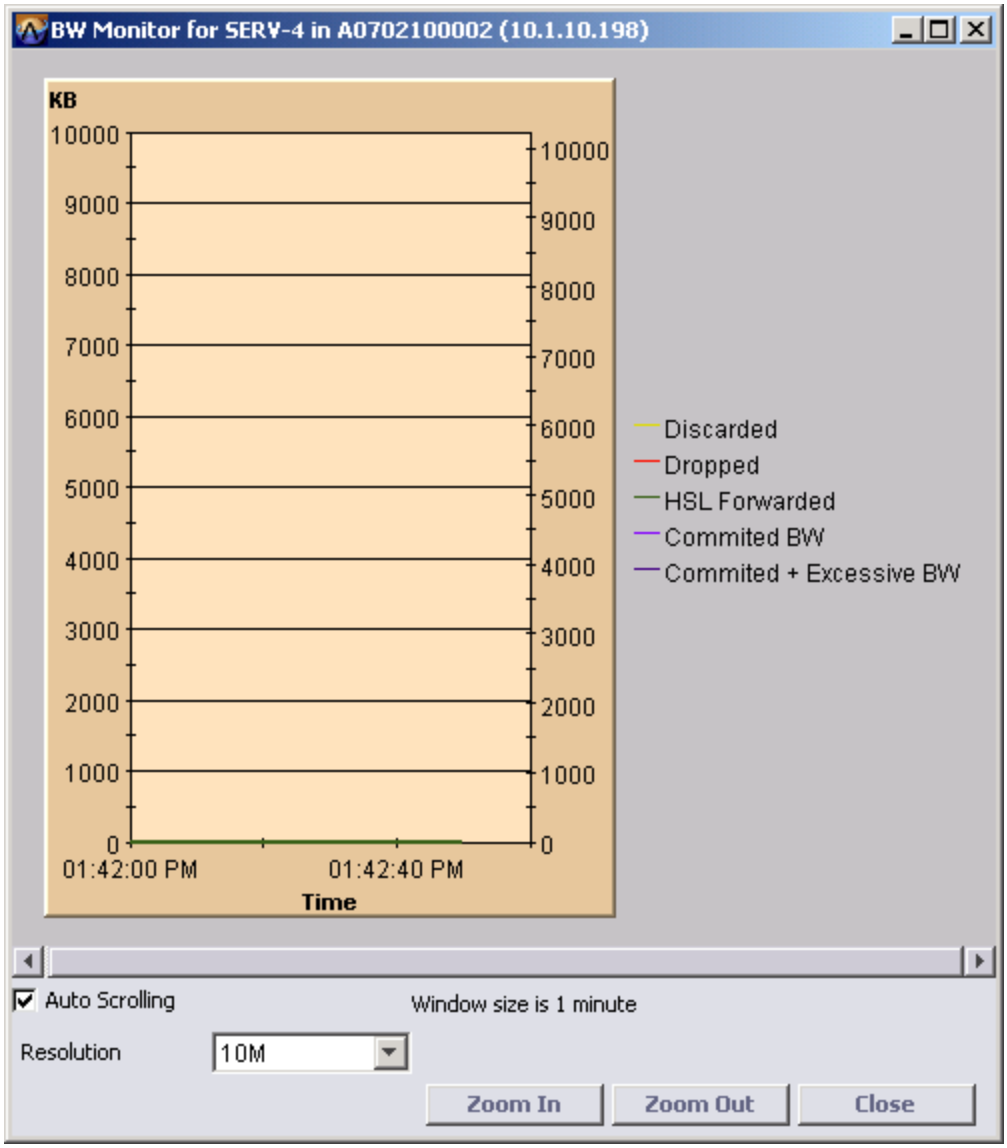


Table 72: Navigating the Graphical Display

To...	Do this...
Disable Auto-Scrolling	Clear the **Auto Scrolling** check box.
Select BW scaling	From the **Resolution** list box, select the BW scaling
Select Tx, Rx or Both, from the **Series selection** list box	Select the appropriate option

Zoom in the display	Click **Zoom In**
Zoom out the display	Click **Zoom Out**
Close the graph,	Click **Close**
Display additional graphs repeat steps 2 and 3	The graphical displays remain displayed on your monitor until closed.

MAC Forwarding Database

When all features are disabled, the Forwarding Database size is 8K on ML700

When monitoring the forwarding database, be aware of the following:

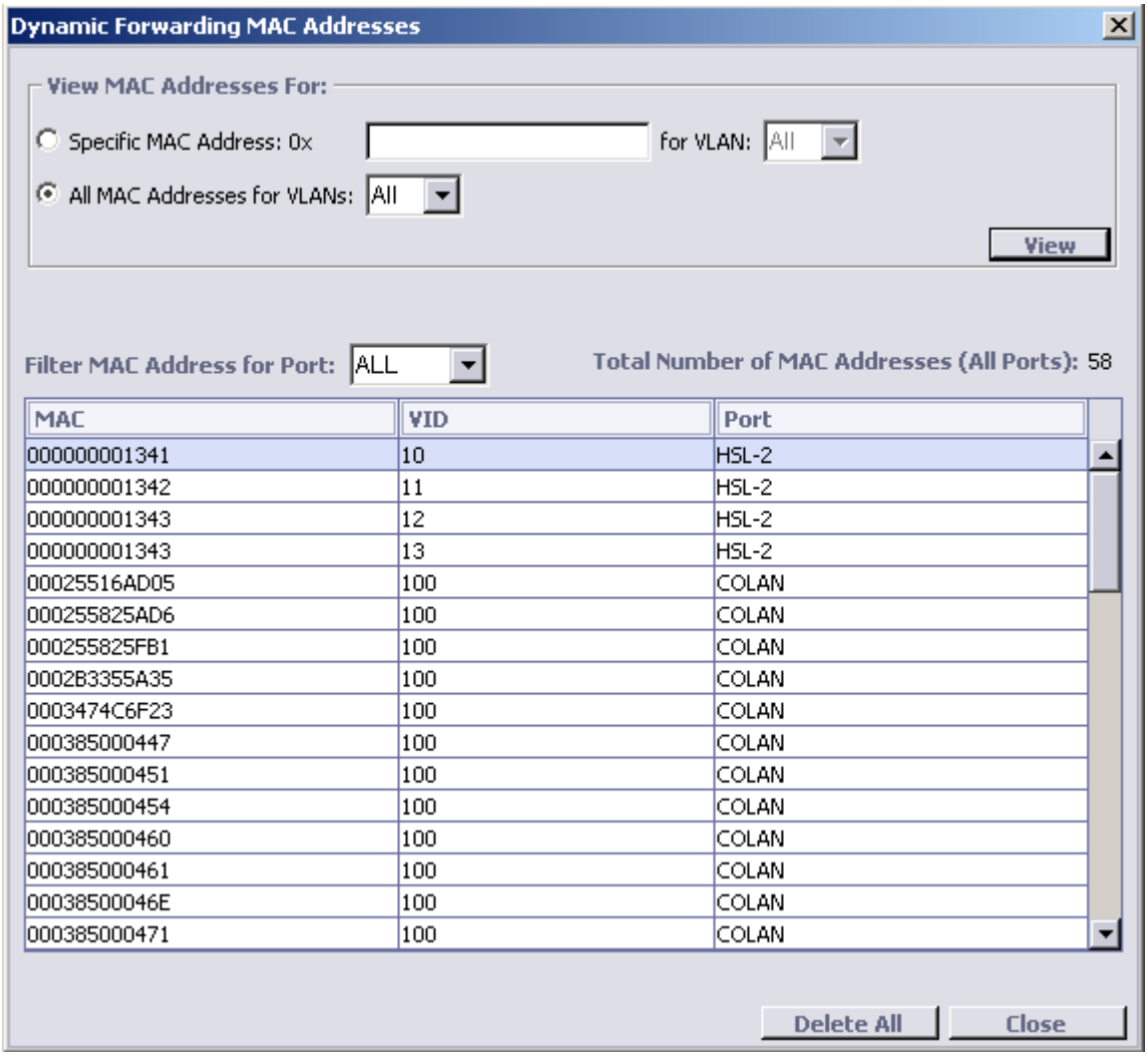
- Due to the hash function implementation of the Forwarding database, some MAC addresses (falling into the same place in the hash table) are learned but may not be displayed in the Forwarding database.
- L2CP feature uses 0.6K of 8K for internal purposes.
- Forwarding Database is affected by working features as follows:
  - CPU MAC Address is permanently reserved in the Forwarding database but cannot be viewed;
  - When Ingress Rate Limiting is enabled (on any port), ML700 allocates 3 entries per each VLAN (all of them) in advance, to allow IEEE L2 Control Protocol (L2CP). The allocated addresses can be viewed in the Forwarding database:
    - 0x01-0x80-0xC2-0x00-0x00-0x01 - 802.3x Full duplex Pause Frames Address;
    - 0x01-0x80-0xC2-0x00-0x00-0x02 - 802.3ad Slow Protocol Multicast Address;
    - 0x01-0x80-0xC2-0x00-0x00-0x03 - 802.1X Port Access Entity (PAE) Address.
  - When STP feature is enabled (in the bridge), ML700 allocates 3 entries per each VLAN (all of them) in advance, to allow STP interoperability with Cisco. The allocated addresses can be viewed in the Forwarding database:
    - 0x01:0x00:0x0c:0x00:0x00:0x00 - Cisco ISL;
    - 0x01:0x00:0x0c:0xcc:0xcc:0xcc - Cisco Discovery Protocol;
    - 0x01:0x00:0x0c:0xcc:0xcc:0xcd - PVST+ Cisco Protocol.

Caution: Viewing all MAC addresses in the table via the craft port may take a few minutes and may affect management access of other users.

➢ **To monitor the entire Forwarding database:**

1. In the Network Element tree, open **Ethernet Bridge**. The **Ethernet Bridge** pane opens.
2. In the Forwarding MAC Addresses area, click the **View Dynamic Addresses** button. The **Dynamic Forwarding MAC Addresses** dialog appears.
3. To view specific MAC addresses, in the **View MAC Addresses For** area select the **Specific MAC Address** option and type in a specific MAC address in HEX format.
4. To view all MAC addresses, in the **View MAC Addresses For** area select the **All MAC Addresses for VLANs** option and from the list box, select **All**.

5. To view MAC addresses, learned in particular VLAN, in the **View MAC Addresses For** area select the **All MAC Addresses for VLANs** option and from the list box, select <**VLAN ID**>.
6. Click **View**. The MAC addresses are displayed.



7. To filter the display, from the **Filter MAC Address for Port** list box, select ALL, COLAN (MGMT), specific ETH or HSL.
8. To delete the database, click **Delete All**.

Ethernet Service OAM MEP Performance

MEP performance can be monitored through the **MEP Pane** (on page 11-11): under **Ethernet Services**, choose **Service OAM**, select the relevant **MEG** and choose the specific **MEP** to be monitored).

Two types of analysis tools are available:

- PM tools - detailed descriptions for monitoring instructions are provided in **Error Counters, Measurements and Threshold Alerts** (on page 13-12).

- For Y.1731 OAM - the CFM MEP statistics pane is also available. The pane is described below.

  The pane displays the CFM and Y.1731 PDU messages for the relevant MEP, in the Tx and Rx direction. CFM PDU counters enhance Ethernet OAM interoperability management. Legal, Illegal Supported and unsupported CFM PDUs are counted per MEP or system and allows isolating configuration mismatches and possible vendor incompatibility.

➢ CFM MEP Statistics Pane

To invoke the MEP Statistics pane, select the relevant MEP in the Network Element tree (under **Service/MEG**) and in the invoked MEP pane, click **View Statistics.** The statistics are described in the table.

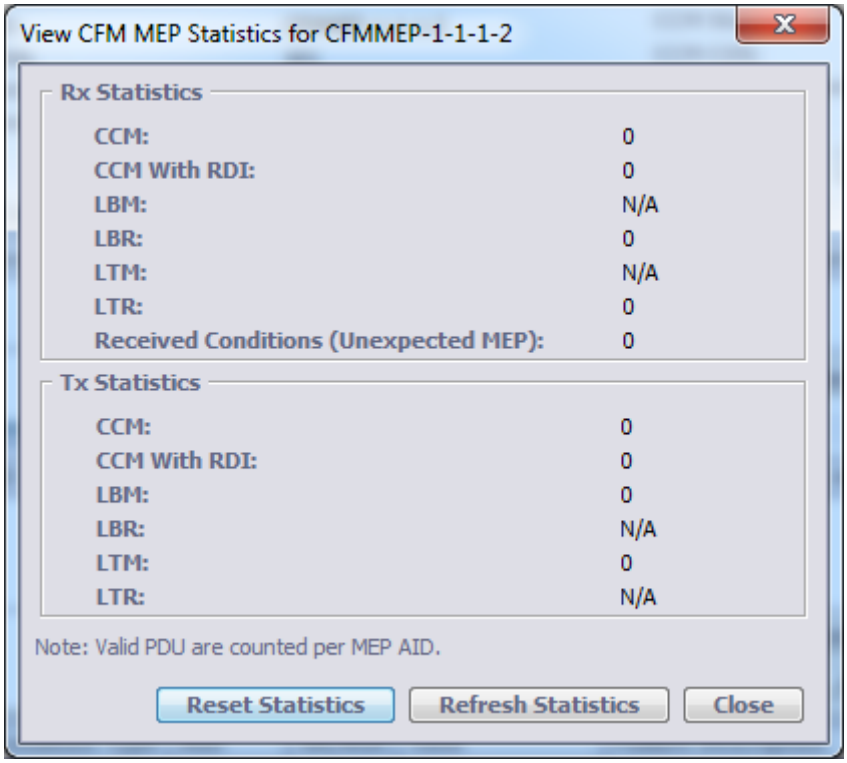


Table 73: MEP Statistics Descriptions

Rx Statistics	
RX CCM	Received Continuity Check Messages counter. When a MEP is enabled on ML and it's Remote MEPs (RMEPs) are manually registered, all valid and not alarmed CCM received from the RMEPs are counted.
RX CCM with RDI	Received Continuity Check Messages with Remote Defect Indication counter. When MEP is enabled on ML and it's Remote MEPs (RMEP) are manually registered, all valid CCM received from the RMEP with indication of RDI (RMEP reports on a problem to see ML MEP) are counted separately from valid non alarmed CCM.
RX LBM	Received Loop Back Messages counter. Unsupported per MEP

RX LBR	Received Loop Back Response message counter. All LBR responses received back upon Loopbacks applied from the ML MEP are counted.
RX LTM	Received Link Trace Messages counter. Unsupported per MEP .
RX LTR	Received Link Trace Response message counter. All LTR responses received back upon Link traces applied from the ML MEP are counted.
RX DMM	Received Delay Measurement Messages counter. Unsupported per MEP .
RX DMR	Received Delay Measurement Response message counter. All DMR responses received back upon Delay Measurements applied from the ML MEP are counted.
Received Conditions (Unexpected MEP)	Count CCM from Remote MEPs which are not registered manually on the ML MEP.
Tx Statistics	
TX CCM	Transmitted Continuity Check Messages counter. When a MEP is enabled on ML, all valid and not alarmed CCM sent by the MEP are counted.
TX CCM with RDI	Transmitted Continuity Check Messages with Remote Defect Indication counter. When MEP is enabled on ML and it's Remote MEPs (RMEP) are manually registered , but at least one of them do not send CCM, will cause ML MEP to send CCDM with RDI . All this messages are counted separately.
TX LBM	Transmitted Loop Back Messages counter. All Loopback operations originated from the MEP are counted.
TX LBR	Transmitted Loop Back Response message counter. Unsupported per MEP.
TX LTM	Transmitted Link Trace Messages counter. All Link trace operations originated from the MEP are counted.
TX LTR	Transmitted Link Trace Response message counter. Unsupported per MEP
TX DMM	Transmitted Delay Measurement Messages counter. All Delay measurement operations originated from the MEP are counted.
TX DMR	Transmitted Delay Measurement Response message counter. Unsupported per MEP .

Ethernet Connection (CO-CPE Linked)

The Ethernet Connection pane enables service providers to verify connectivity, monitor traffic flow and view the relevant configuration options on a defined link between two devices or on a single interface. The information is displayed in an intuitive, graphical pane: as a selection criterion is chosen, the pane automatically displays all relevant connection points and EVC information. For each selected link or interface, the following information can be displayed and analyzed:

- Port configuration
- Bridge and link configuration and status parameters

- Traffic statistics in each direction on the link
- Information on the VLANs, EVC configuration and EVC statistics

➢ To invoke and navigate the Ethernet Connectivity tab

In the Main window, click the **Connectivity** tab and click **Ethernet Connection.** The Ethernet Connections pane is invoked.

The pane is divided into the following areas:

- NE 1 and NE 2 - shows the NEs whose interfaces or interconnection is to be analyzed. For each NE, the IP, VLANs and interfaces are displayed. The display is affected by the setting of the **Automatic Link** option.
- Automatic Link - This option is ENABLED by default - selecting any item (IP address, VLAN or Port), automatically displays all the associated items on *both* NEs. If Automatic Link is DISABLED, each item stands on its own. If it is modified, the associated items do not change accordingly. This enables analyzing each element on its own.
- Tabs at the bottom of the pane provide a range of detailed analysis options.

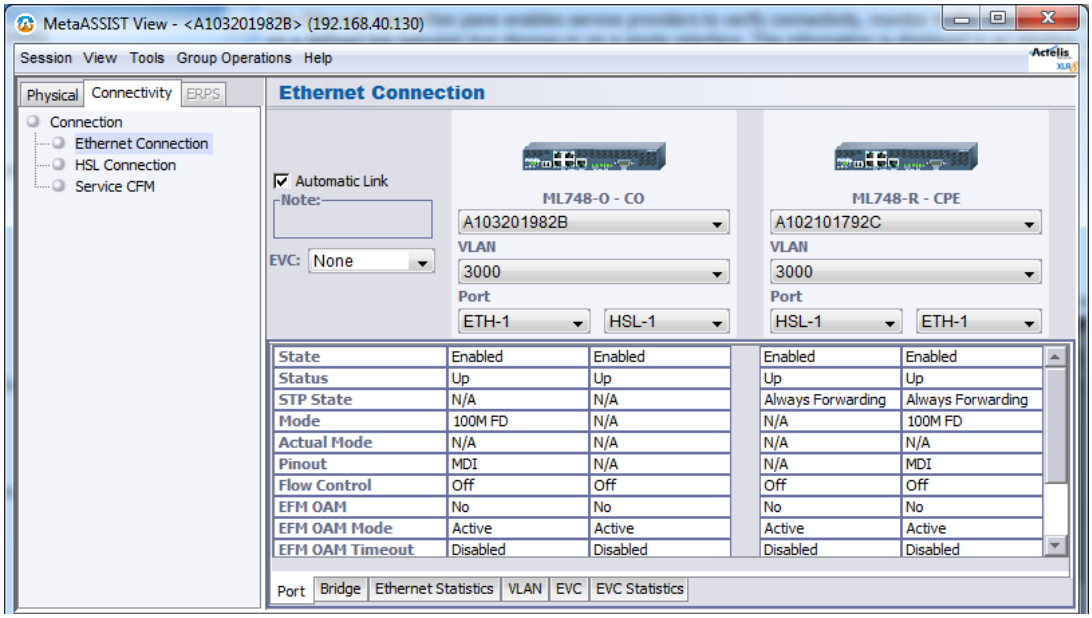


Table 74: Ethernet Connectivity Tabs

Tab	Description
Port	Shows the configuration and status of an individual interface or two interfaces comprising a link (according to the selected option and whether Automatic Link is enabled)
Bridge	Shows Bridge level configuration and status for each of the defined NEs
Ethernet Statistics	Shows traffic flow on the link or on a single interface in the *selected direction*
VLANs	Shows the Port Membership and Tag for each VID, for each displayed NE
EVC	Shows the configuration for selected EVC
EVC Statistics	Quantifies various statistics for selected EVC. Selected statistics can be displayed as graphs.

➢ **To analyze a link**

1. The link of interest can be selected using two methods:
   - From the Physical tab - **Network Element** tree, expand the **Ethernet Port** item and choose the relevant port. For example, **HSL <AID>.** Select the **Connectivity** tab. The selected interface will be displayed along with any other interfaces and the VLANs relevant to the link.
   - From the Connectivity tab:
     - Under the relevant **NE**, select the HSL or ETH interface, the corresponding information will be invoked.
     - Under **Automatic Link -** choose the relevant EVC. The corresponding connections will be displayed in the NE pane areas.
2. The above figure shows an end-to-end link connection between HSL-1 on the ML700 CO and ML700 -R. The service is defined by VLAN 3000.
3. Click the relevant tab to show the required link information.

Ethernet Topology (other NE Linked)

If the LLDP option is locally enabled for all the NEs participating in the Ethernet Topology, each NE is capable of discovering the other attached NEs and display each NE self-advertised information in the **NEs linked via Ethernet** pane in a tabular form along with relevant information on each element. See LLDP Configuration for a description on how to enable LLDP (LLDP disabled by default).

➢ **To display a list of the NEs linked via Ethernet**

In the Network Element tree, select **NEs Linked via Ethernet**. The corresponding pane listing the NEs linked via Ethernet appears.

The parameters describing each NE Ethernet port link are listed in the table following the figure.

NOTE: The **Details** button is useful for non-Actelis vendors, where LLDP messages include extra-parameters (all mandatory parameters are represented in the table). MAV lists the HEX values of optional TLV (type-length-value) parameters, sent in LLDP.

Network Elements Linked via ETH

AID	Port ID Type	Port ID	Chassis Type	Chassis ID	System Name	Enterprise
COLAN						
ETH-1						
ETH-2						
ETH-3	LOCAL	ETH-1	NETWORKADDR	10.1.6.13	123456789012345...	5468
ETH-4						
ETH-6	LOCAL	ETH-5	NETWORKADDR	10.1.6.8	ML628-33	5468

Details

Table 75: LLDP Parameters

Parameter	Description
AID	Port Identification on an NE which is directly connected via MAV.
Port ID (and Port ID type)	Port Identification on an attached NE as discovered by LLDP: • For ML NE - Port Type is LOCAL name • On another device it can be set as SNMP IfTable Index, IfEntity Index, etc. The type of presentation is determined on the attached NE.
Chassis ID (and Chassis Type)	NE identification of the attached NE as discovered by LLDP: • For ML NE - Chassis ID is represented by its' Network Address (IPv4) • On any other device it can be set as: Local name, SNMP SysName, etc.
System Name	NE name of the attached NE, ML NE provides TID/SID of the system.
Enterprise	The unique SNMP identification of Equipment Vendor. Actelis Networks Enterprise OID = 5468.

HSL Link Monitoring

Detailed information on HSL can be viewed via the following tools:

- HSLs Details area in the HSL pane - shows basic information
- HSL Details pane - shows detailed information on each parameter
- HSL connection glance view - displays the configuration of the HSLs and Modems, and provides a range of monitoring tools
- Information on modem ports allocated to the HSL: rates, synchronization status, etc.

HSL Details Area

The Details Status area in the **HSL** pane, provides detailed information on HSL Status, Modem Ports and Calibration Parameters. Before the HSL is calibrated, only some of the information is displayed. During calibration, a progress bar is displayed in the Status area.

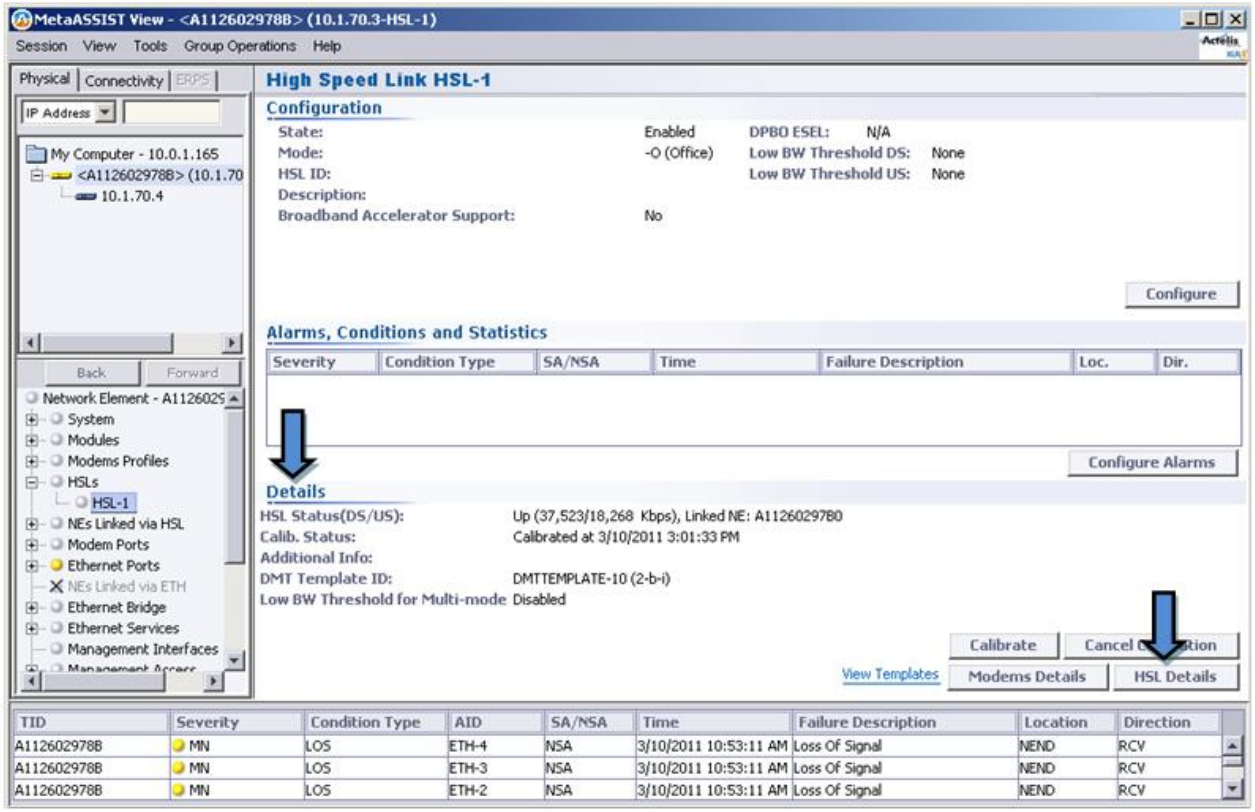


Table 76: Detail fields

Parameter	Description
HSL Status	Up - The High Speed Link is up and provides bandwidth available for services. When HSL is up, the Linked NE information is available (presenting the sum of data rates of the link) and displayed with Linked NE TID and HSL-<ID> (as numbered on remote site). Down - The High Speed Link is down and no bandwidth is provided for services.
Calib. Status	• Not Calibrated - Calibration was not performed. All provisioned (enabled) modems are synchronized or trying to synchronize at minimal rate. • Calibrated to US and DS rates - Calibration was performed for all modems that were enabled during last calibration. Calibration information includes information about modems that successfully passed or failed qualification. All enabled but not qualified (failed to qualify) modems are not trying to synchronize at all, even at minimal rate. • Calibrating,% (Retry <number>) - The link is down due to calibration in progress. If new calibration was requested, it is suspended until on-going calibration is auto-aborted (it takes a few minutes) and then starts automatically. The number of retries is displayed. Endless retries may indicate on wrong profile settings (e.g VDSL2 profile on very long loop). Stop the calibration by clicking the **Stop Calibration** button. Ethernet service capabilities of the HSL will be displayed as Available BW in Bandwidth parameters • Pending Calibration - Requested calibration is pending, waiting for enabled modems to synchronize. For additional reasons, see the following table.

Table 77: HSL Status parameters - HSL -O (Office) mode only

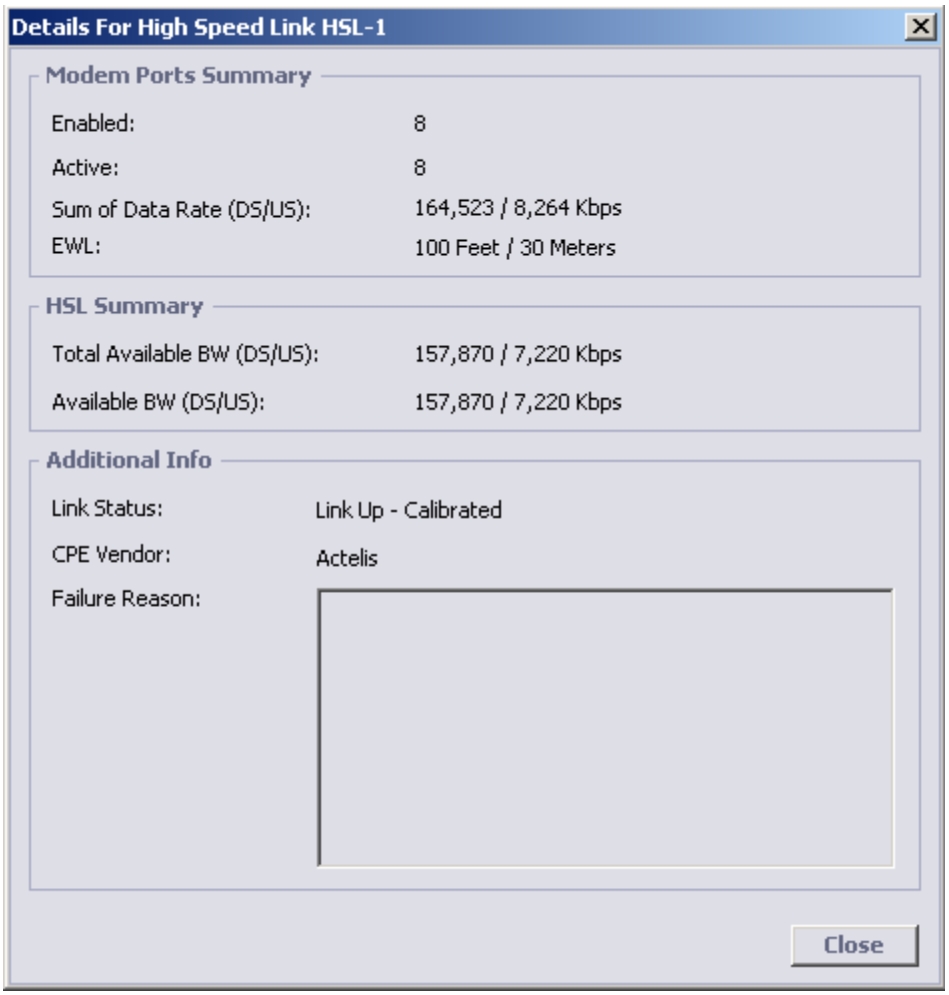
Parameter	Description
Not enough active lines	No modem complies with calibration requirements (e.g. required NM)
Recovering	The link is down due to HSL currently in recovery process. System is attempting to synchronize enabled modems. Service will be resumed automatically. This may take a few minutes.
Low ETH Bandwidth	The link is up with a bandwidth lower than the LOW BW threshold configured for this link.
<Empty>	When HSL is up or calibrating for the first time.

HSL Details Pane

The HSL Details pane provides information on the modem ports, calibration parameters and calibration status/results.

To view the HSL Details pane

In the Network Element tree, click **HSLs**, **HSL-<ID>** and then click on the **HSL Details** button. The HSL Details pane appears. Individual area parameters are described in the following sections.



The HSL Details pane is divided into the following areas:

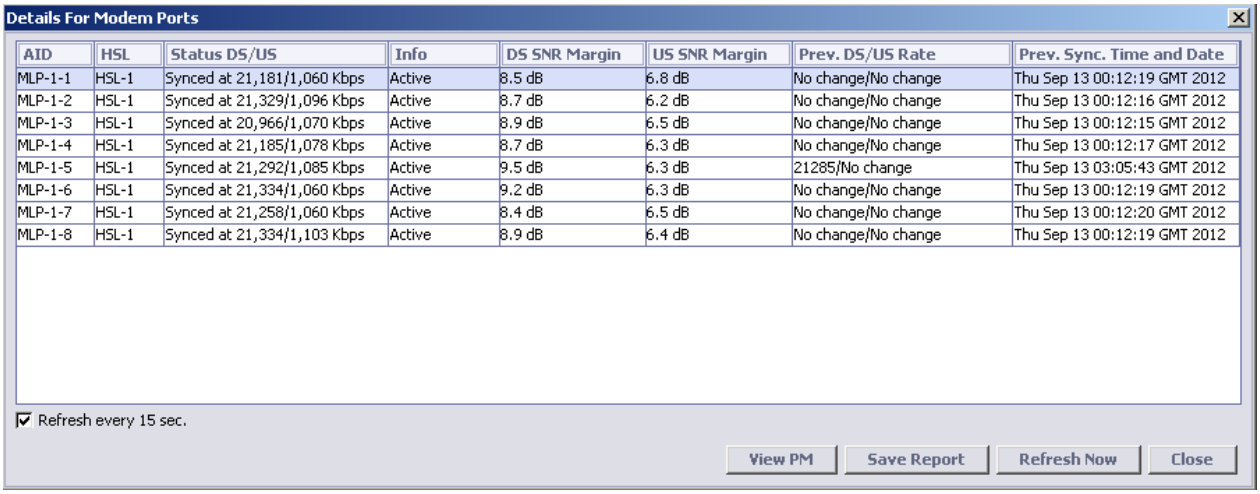
- Modem ports Summary- shows information on the number of enabled modems, active modems, sum of data rates (i.e. without bonding overhead) and EWL.
- HSL summary - BW values and general status of selected HSL.
- Additional Info - Link status

Table 78: HSL Details

Modem Ports Parameters	**Description**
Enabled	Number of enabled modems for the link.
Active	Number of currently active modems
Sum of Data Rate	The Sum of Rates represents the total HSL BW (not including overhead) and is relevant only for –O (Office) mode.
EWL	EWL is provided only in case of link without BBA. About EWL: The ANSI T1.417 standard defines deployment guidelines in terms of an Equivalent Working Length (EWL) of multi-gauge cable. EWL is intended to provide equivalence between the length of a multi-gauge loop and that of a straight 26-AWG loop. It is auto-measured in any Spectral Mode. EWL = (1.41) x L28+ L26+ (0.75) x L24+ (0.60) x L22 + (0.40) x L19, where L26, L24, L22, and L19 are the lengths of 28-, 26-, 24-, 22-, and 19-AWG cable in the subscriber loop excluding any bridge taps, respectively.
DS Attenuation with BBA (at 300kHz)	Downstream Attenuation (measured at 300kHz) is provided only in case of link with BBA. The measured attenuation is composed of the two segments attenuation (ML700-O to BBA and BBA to ML700-R) minus BBA's gains.
US Attenuation with BBA (at 100kHz)	Upstream Attenuation (measured at 100kHz) is provided only in case of link with BBA. The measured attenuation is composed of the two segments attenuation (ML700-O to BBA and BBA to ML700-R) minus BBA's gains.
HSL summary Parameters	**Description**
Total Available BW	Total Ethernet bandwidth with redundant capacity. Redundant capacity may exist in case that the link capacity exceeds ML700 L2 capacity (500Mbps at DS and ~250Mbps US). In such case the excessive capacity serves as redundancy in case of modem failure or modem rate reduction.
Available BW	Currently available Ethernet bandwidth over HSL for service connections. In a deployment where link capacity shall be smaller than available BW, use the Egress Rate Limit to reduce the Ethernet BW over HSL.
Additional Info	**Description**
Link status	Link status (e.g. Calibrated, Recovering)
CPE Vendor	Actelis - for all Actelis devices
Failure Reason	This field contains information only if there is a fault; otherwise, it is empty.

Modem Ports (MLP) Details

The **Modem Glance pane** (on page 4-14) **Details** button provides traffic, status and other information for all the modems.



The following table describes the Modem Port Details parameters that can assist you in monitoring the Modem Ports.

Table 79: MLP Details pane parameter list

Parameter	Description
Status	The modem operational status value. • Synched at - Modem is synchronized on the current DS/US rate. • Trying - Modem is trying to synchronize on the current rate. • Not Used - Modem failed during qualification. • Deactivated - Modem is removed from service. • Quarantine – modem with errors during several seconds is quarantined to prevent the errors from the HSL. Modem is restored to normal operation automatically after one minute free of errors. • BADRATIO – HSL is limited to the modems rate ratio (slowest modem to fastest modem) of 1:4. In case that the ratio is not supported the HSL during calibration truncates higher modem(s) rate or disqualify lower modem(s) rate to achieve best performance. In case the modems rate decreases after calibration, the modem is placed in quarantine (i.e. not delivering traffic) instead of being disqualified.
Info	Modem Information status. • Init - Modems are initializing. • No Signal - Loss of signal. See Modem Ports Alarms Troubleshooting. • Loss of Sync - Modem is out of synchronization. See Modem Ports Alarms Troubleshooting. • Active - Modem is in use by the High Speed Link. • Failure - Indicates a fault on the modem. • <Empty> - Transient status.

Parameter	Description
DS/US SNR Margin	Lowest SNR margin (dB) measured at the termination points over the copper pair line for the US or DS (depending on the column).
Previous sync time	Provides the date and time of previous activation time
DS/US Previous rate	Provides previous DS and US data rate

HSL Connection (CO-CPE Linked)

The HSL Connection glance view displays the configuration of the HSLs and Modems, and provides the following monitoring options:

- Compare parameters of the CO versus the CPE HSL/MLP.
- Debug mismatches between the configured BW the HW limitations for CO and CPEs.
- Find out Ethernet Available BW which can be below EFM Bonded BW.

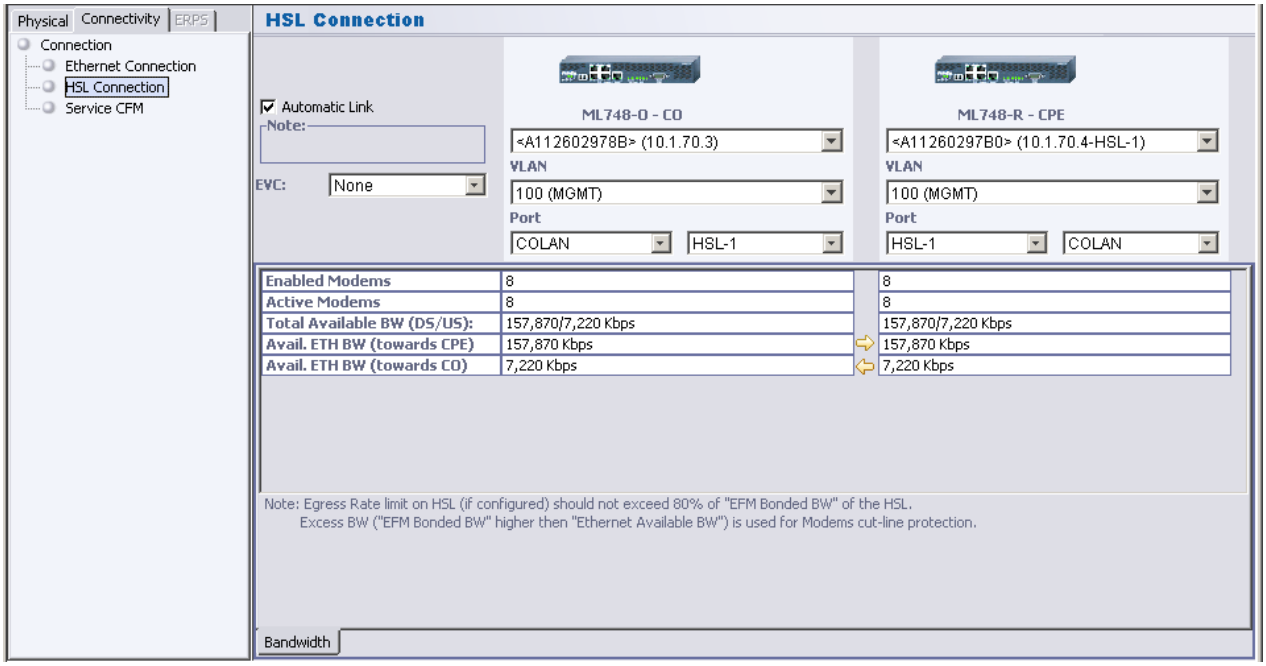
The HSL connection view highlights mismatches between CPE and CO configured parameters.

➢ **To invoke and navigate the HSL Connection tab**

In the Main window, click the **Connectivity** tab and click **HSL Connection.** The HSL Connection pane is invoked.

The pane is divided into the following areas:

- NE 1 and NE 2 - shows the NEs whose HSL Connections are analyzed. For each NE, the ID, VLANs and interfaces are displayed.
- HSL Connection Parameters - displays all the associated items on *both* NEs. This allows analyzing and comparing between the relevant parameters of the CO and CPE simultaneously.



Copper Line Monitoring

MetaASSIST View provides a range of copper line monitoring tools used to view and analyze essential data of signal quality, rate, power, SNR, BER) for each transceiver point and perform fast fault isolation. Refer to MLP PM Counter Types for a list of counters.

Table 80: MLP Copper Line Monitoring Tools

Copper Line Monitoring Tool	Description
Inventory Details (on page 13-48)	Provides information on the CPE connected to a specific copper-pair.
DMT Band Details (on page 13-49)	Line performance information such as signal and line attenuation, noise.
View Rate Details (on page 13-50)	Shows the Rate Profile defined and attained bandwidth rates.
View Spectral Details (on page 13-51)	Shows basic Spectral Profile definitions and values.
View Quality Details (on page 13-52)	Shows basic Quality Profile definitions and values.
Loop Diagnostic Tools	INM Impulse Noise Monitoring and DMT sub-carrier analysis tools

Inventory Details

This Line Inventory pane provides information on the CPE connected to a specific copper-pair.

➢ **To view Line Inventory details:**

In the Network Element tree, click **Modem Ports**, **MLP <AID>** pane. In the **MLP <AID>** pane, click **View Line Inventory**. The **View Line Inventory in MLP <AID>** opens in the work area.

NOTE: Available only for a single modem belonging to an ML700 CO unit.

Port	Location	Serial Num.	CLEI	PN	Model	HW Ver.	SW Ver.	Data	System Vendor ID
MLP-1-1	FEND (CPE)	A11260297B0	0000000000	501RG0237	ML748-R	D02	7.14/10	CURRENT	ATNW

Table 81: Line Inventory Details

Line Inventory is available in –O models only and provides information on the peer side (–R unit)

Field name	Description
Port	Port identification
Location	Always FEND (Far End)
Serial Number	Serial number of the equipment where the modem port is detected.
CLEI	CLEI (catalog code) of the equipment where the modem port is detected.
Model	Model of the equipment where the modem port is detected.
HW Version	Hardware Version of the equipment where the modem port is detected.
SW Version	Software Version of the equipment where the modem port is detected.
Data	Indicates if the displayed data is current.
System Vendor ID	ATNW = Actelis Vendor

DMT Band Details

NOTE: Refer to MLP PM Counter Types for details on counters.

SNR Margin and Attenuation are main copper line performance characteristics. These are monitored per modem per second. SNR is automatically controlled to be never less than Baseline SNR + 1dB, (which guarantees reliable data transport, i.e. maintains a BER of 10-7). If SNR on a modem is less than defined above, then the modem will be automatically adjusted in rate to comply with required SNR margin (either via SRA, Seamless Rate Adaptation, if enabled or via modem initialization). Using this self-recovery mechanism, the system avoids false alarms and unnecessary human intervention.

Alarm indication behaves as follows:

- LOWSNRM Alarm is raised on crossing threshold down (SNR margin becomes equal or less than the threshold value);
- LOWSNRM Alarm Clearance is sent on crossing threshold up (SNR margin becomes larger than the threshold value by at least 1 dB);
- HIATTN Alarm is raised on crossing threshold up (Loop attenuation becomes equal or higher than the threshold value).
- HIATTN Alarm Clearance is sent on crossing threshold down, usually after modem synchronization (Loop attenuation becomes larger than the threshold value by at least 1 dB).

➢ **To view Line Performance details:**

In the Network Element tree, under **Modem Ports,** select the modem port of interest (i.e. MLP-1-1) and in the displayed pane **Details** area, click the View **Band's Details** button. The following information appears.

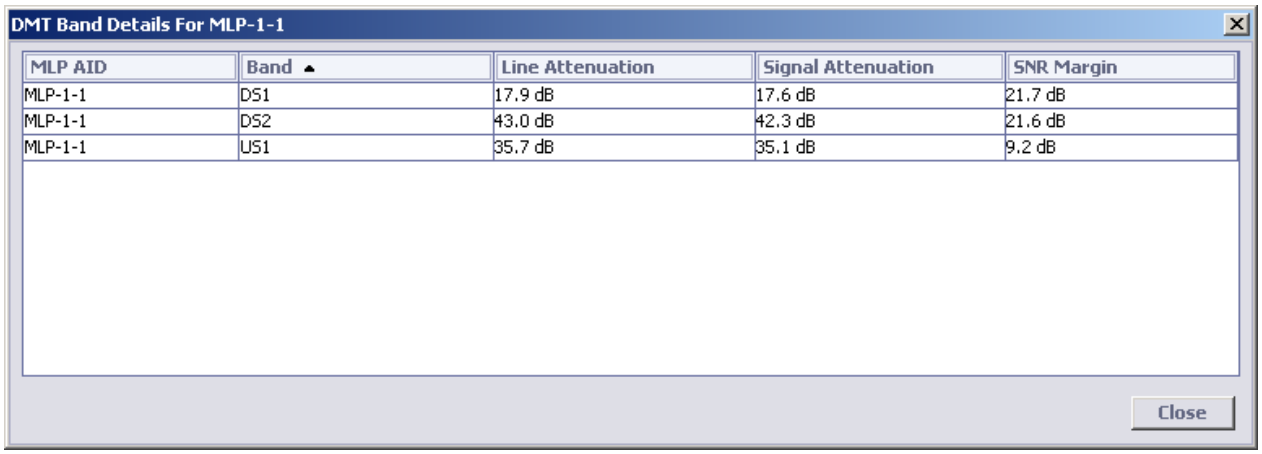


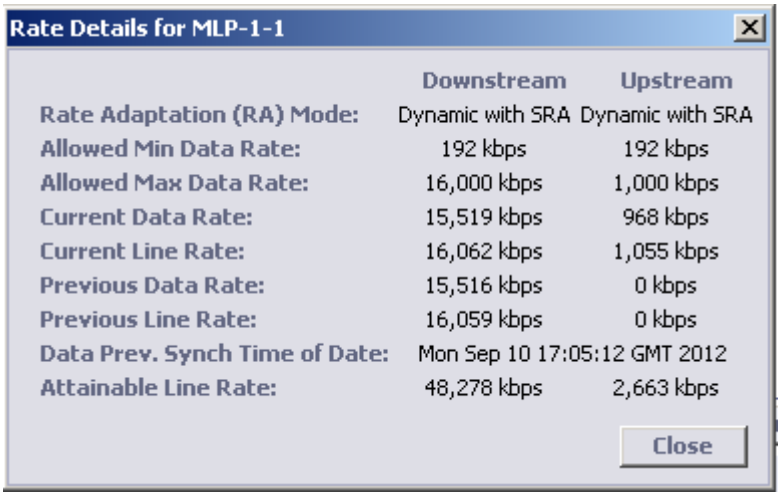
Table 82: Line Performance details

Field name	Description
MLP AID	Copper pair identification.
Band	Band, e.g. DS1, US1, DS2
Line Attenuation	Line attenuation per band (LATNds and LATNus) – loop attenuation over all subcarriers of this band during loop diagnostic mode and initialization.
Signal Attenuation	Signal attenuation per band (SATNds and SATNus) - loop attenuation over all subcarriers of this band during show time.
SNR Margin	Signal to Noise Ratio Margin (SNRMds and SNRMus) – scalar value (overall band)

View Rate Details

➢ **To view Rate Details**

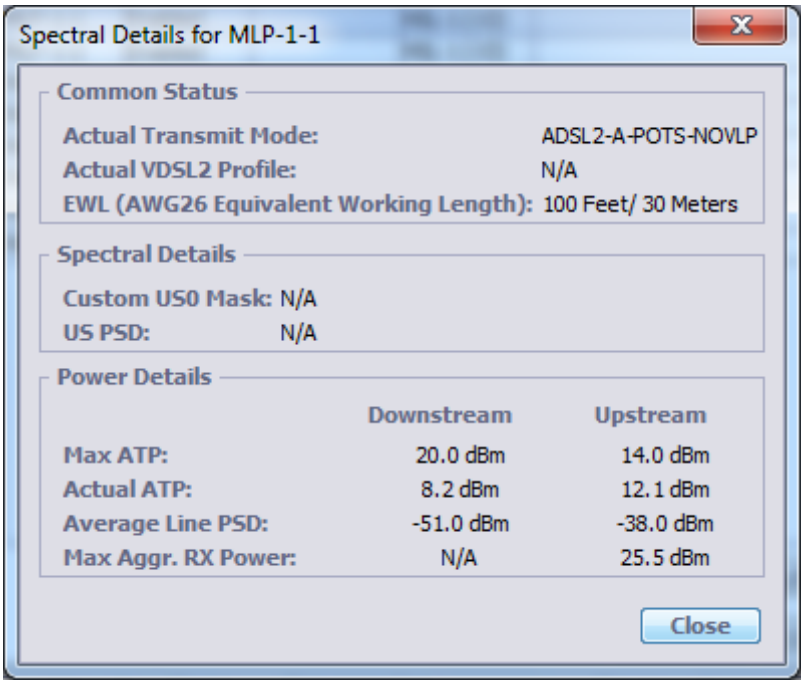
In the Network Element tree, under **Modem Ports,** select the modem port of interest (i.e. MLP-1-1) and in the displayed pane **Details** area, click the **Rate Details** button. The following information appears.



View Spectral Details

➢ **To view Spectral Details**

In the Network Element tree, under **Modem Ports,** select the modem port of interest (i.e. MLP-1-1) and in the displayed pane **Details** area, click the **View Spectral Details** button. The following information appears.

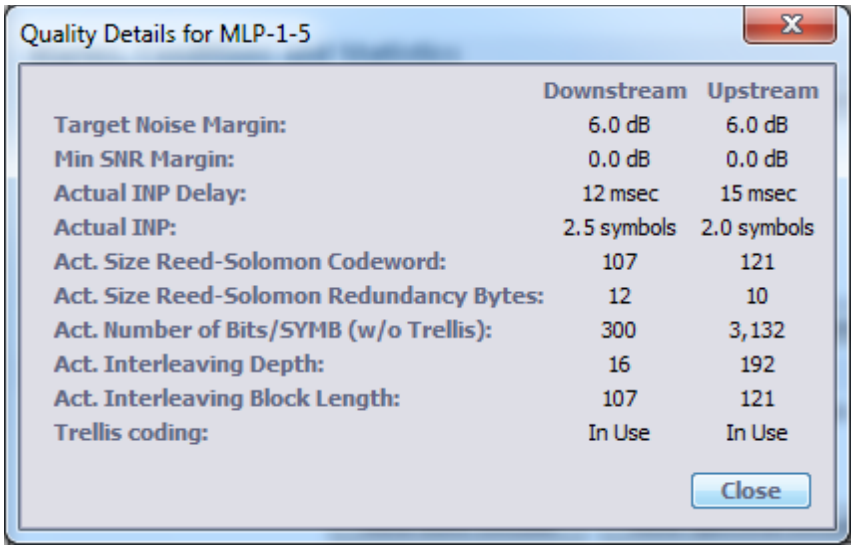


Note: in case of link with BBA the EWL parameter is replaced by DS attenuation at 300 KHz and US attenuation at 100 KHz. Refer to Table 78: HSL Details for details.

View Quality Details

➢ **To view Quality Details**

In the Network Element tree, under **Modem Ports,** select the modem port of interest (i.e. MLP-1-1) and in the displayed pane **Details** area, click the **Quality Details** button. The following information appears.



Loop Diagnostic Tools

The following tools are provided for Cooper Loop diagnosis:

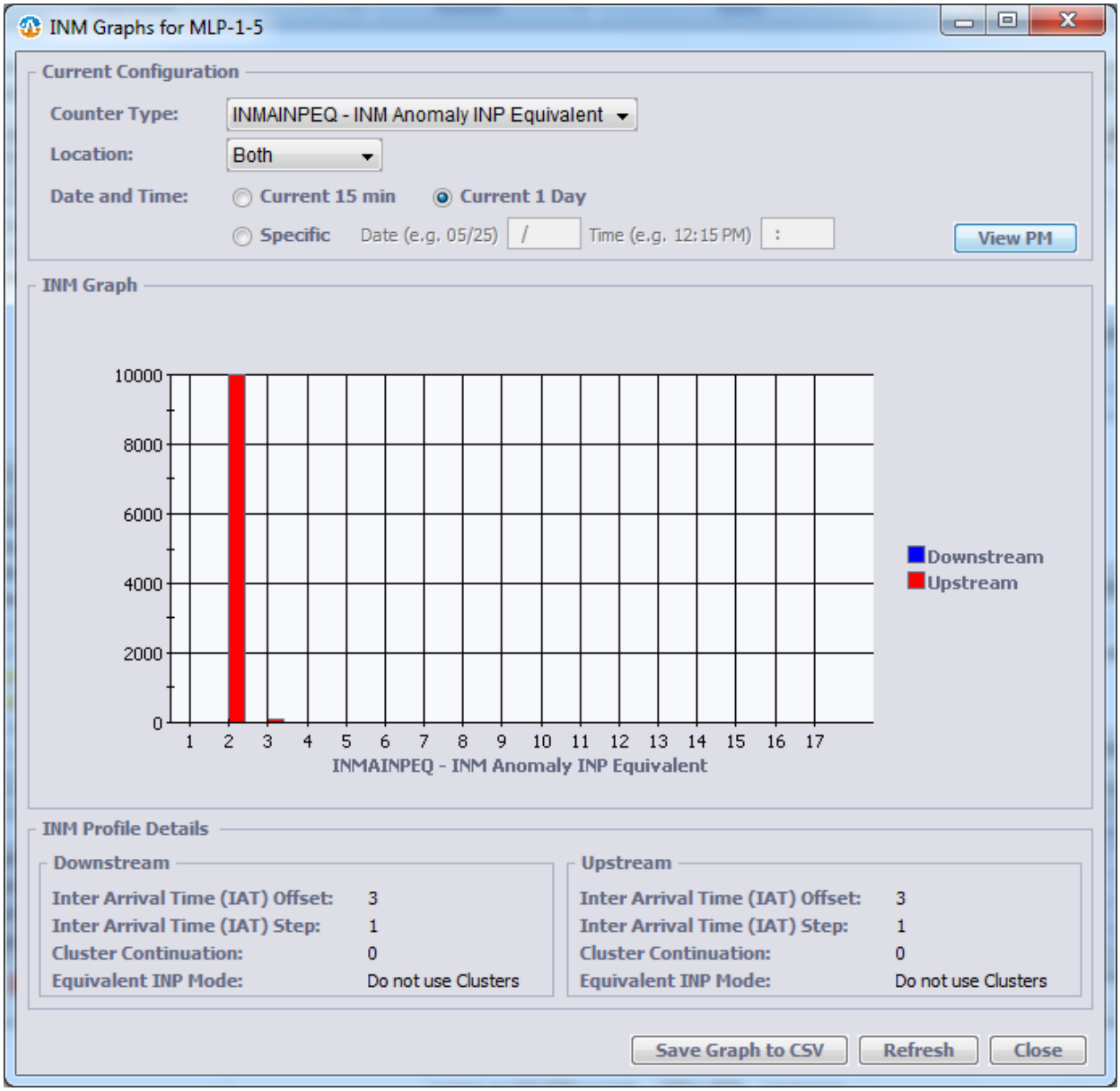
- **INM Graph** (on page 13-53)
- **DMT Sub-carrier analysis** (on page 13-54)

Impulse Noise Monitoring Graph

Use the INM Graph tool to measure Impulse Noise according to the parameters set in the **Impulse Noise Monitor** (on page 6-29) profile. Two types of counters can be accumulated in either or both Upstream and Downstream direction according to a user defined time period.

➢ To use the INM analysis graph

1. In the Network Element tree, under **Modem Ports,** select the modem port of interest (i.e. MLP-1-1) and in the displayed pane **Details** area, click the **View INM Graph** button. The following dialog appears.



2. The defined **INM profile settings** (on page 6-29) are listed at the bottom of the window. These may be modified via the INM Profile dialog: in the **Network Element** tree, under **Modem Profiles**, **Quality Management**, **Impulse Noise Monitoring Profiles.**

3. Choose the counter type to be accumulated:
   - INMIAT - INM Inter-arrival time between clusters.
   - INMAINPEQ - INM anomaly and INP equivalent graph.
4. Under Counter type - choose if data is accumulated in the Downstream (Blue), Upstream (Red) or both.
5. Under Date and Time - choose the time period over which data will be accumulated:
   - Current 15 minute - next 15 minutes
   - Current day - 24 hour period starting from when View PM is clicked.
   - Specific - specified time frame
6. Click **View PM** to show chart.

NOTE: Use **Save Graph to CSV.** to save chart in tabular form for use with another application.

DMT Sub-carrier Analysis

DMT Sub-carrier Graphs can assist in monitoring and debugging xDSL link. The MAV provides visual representation (graphs) of various parameters of subcarriers. The parameters may be viewed according to the sub-carrier index or according to tone frequencies. Graph may be saved in '.csv' format for future analysis. Graph may be zoomed in for better resolution.

➢ To use the sub-carrier analysis graph

1. In the Network Element tree, under **Modem Ports,** select the modem port of interest (i.e. MLP-1-1) and in the displayed pane **Details** area, click the **View SC (Sub-Carrier) Graphs** button.
2. Select the graph attributes according to the tables following the image below, and then click **Get Graph.** A graph corresponding to the defined options appears.

You can zoom in the graph as well as save the graph to a tabular format.

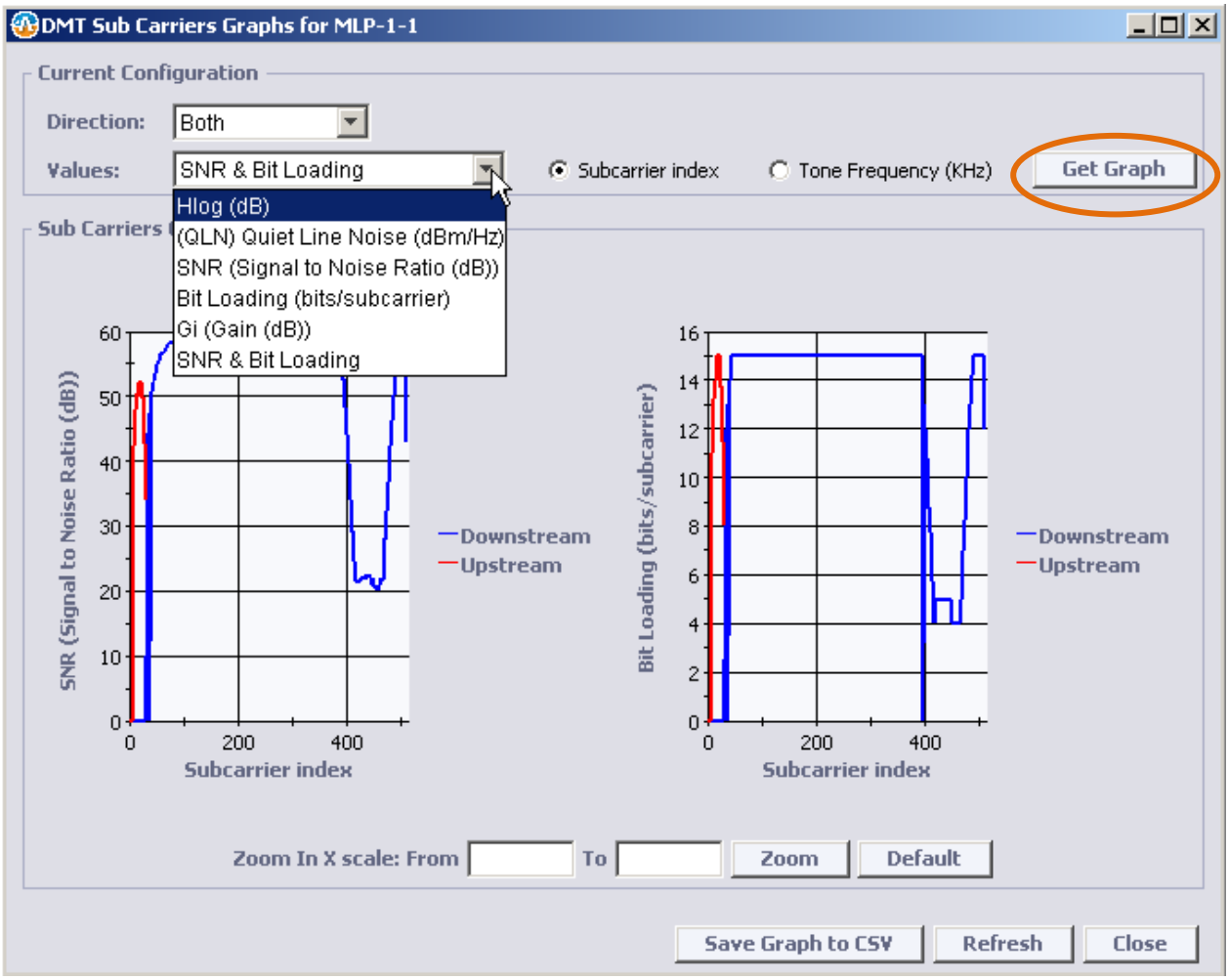


Table 83: Graph Attributes

Directions	Upstream data only, Downstream data only or Both (Upstream and Downstream)
Values	Type of graph parameters as detailed in the following table.
Sub-carrier Index	X-scale according to sub-carrier index
Tone Frequency	X-scale according to tone frequencies
Zoom	Zoom into the graph for a larger display according to the defined Zoom In X Scale
Save graph to CSV	Save graph in tabular form

Table 84: Graph Parameters

Channel Characteristics Function Hlog(f) per sub-channel	The channel characteristics function H(f) is the frequency response of the channel, i.e., amplitude magnification at each frequency point, which can be used for analyzing the physical copper loop condition, for example, determining line quality and presence of bridge taps. Its magnitude values are depicted in a logarithmic scale, Channel characteristics, Hlog(f).This function yields valuable information about the physical condition of the copper loop and its topology.
Quiet Line Noise PSD QLN(f) per sub-channel	The quiet line noise PSD QLN(f) for a particular sub-carrier is the rms (Root Mean Square) level of the noise present on the line, in absence of ADSL signals. Quiet line noise provides a wideband spectral analysis function. QLN(f) can be used for analyzing crosstalk or RF interference, for example, spikes in a plot of this data would indicate interference
Signal-to-Noise Ratio	The signal-to-noise ratio SNR(f) for a particular sub-carrier is a real value that represents the ratio between the received signal power and the received noise power for that sub-carrier. The SNR(f) data provides the user with information about the capacity of the line. The signal-to-noise ratio can be used to derive the impact of topology or spectral issues on a line. The interference combination of Hlog(f), QLN(f) and SNR(f) can be used to troubleshoot why the data rate is not able to reach the maximum in a given loop.
Bit loading	The Bit Loading provides the amount of bits transmitted per sub-carrier per DSL frame. Sub carrier with higher SNR may transmit more bits (up to 15 bits). Graph may be set according to Subcarrier Index **or** Tone Frequency (Khz)
Actual PSD Shape	Actual PSD Shape (verify if supported, I don't think it's supported today) provides the transmitted PSD (Power Spectral Density) in dBm/Hz. The actual PSD depends on multiple parameters such as used technology, profile, spectral limitations (UPBO, DPBO, RFI notch etc.) loop length, etc.
Gi (Gain in dB)	Gi provides the transmit gain used by the modem to equalize the SNR over the sub-carriers. Gain values are -14.5 dB up to +2.5 dB (usually the values are between -1.5dB and 1.5dB)
SNR/Bit Loading	This graph provide both charts (SNR and Bit loading) together.

14 Administration

This chapter describes how to perform various administration operations such as configuration backup and restore, updating software on ML systems, log file management, updating MetaASSIST View software, accessing the system via CLI, and more.

These types of operations can be performed via the MetaASSIST View or, if the available computer is not running MetaASSIST, some of the operations can be performed by opening a session to the ML device from any standard Web browser. Accordingly, this chapter is divided according to MetaASSIST View operations and Web Browser operations.

In This Chapter

Using MetaASSIST View

This section describes how to perform the following administration procedures via the MetaASSIST View:

Configuration Backup and Restore

ML devices can export (backup) and import (restore) Configuration Setup as binary files. It is recommended to backup the configuration after each configuration change by saving a copy of all provided ML device data on any available IP host in the LAN where the ML device is connected. The file will be saved with default (or user defined) name in either the default directory (C:\MetaASSIST) or a user defined directory. The directory specified by the user can be on the host or in another specified destination (using HTTP, FTP or TFTP).

Backup and Restore Requirements

➢ **To perform Backup and Restore using the MetaASSIST View**

- File transfer is to be performed only via non-serial interface; connection cannot be via the CRAFT port.
- IP attributes must be configured on the directly attached NE (while the indirectly attached NE unit can be an IP-less device).
- If FTP/TFTP is used, the FTP or TFTP server must be installed and correctly configured on the host computer.

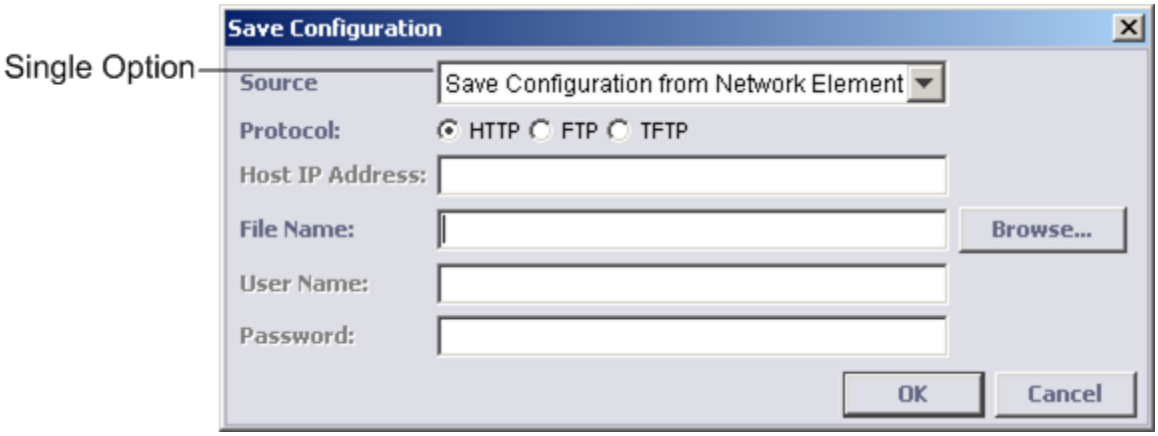
NOTE: Timeout on the TFTP server must be configured to be greater than 30 seconds.

Backup of the Configuration File

➢ **To save the configuration file**

1. In the **Network Element** tree, open **System Administration**.
2. Open **Configuration Backup**. The **Configuration Backup** pane opens in the work area.
3. On the Host, run an FTP/TFTP server (the FTP/TFTP directory must point to the configuration backup directory). Skip this step for HTTP.

4. Click **Save Config**. The Save Configuration dialog appears.



5. Select a protocol option for download (HTTP, FTP or TFTP).
6. In the **Host IP Address** box, type the server IP address (for HTTP, skip this step).
7. In the **File Name** box, type a file name for the configuration file (for HTTP, you can browse for a backup directory). MetaASSIST View automatically adds the *.dat* extension.
8. For FTP only, in the **User Name** and **Password** boxes, type the user name and password of the FTP server account.
9. Click **OK**. The configuration file is uploaded and saved.

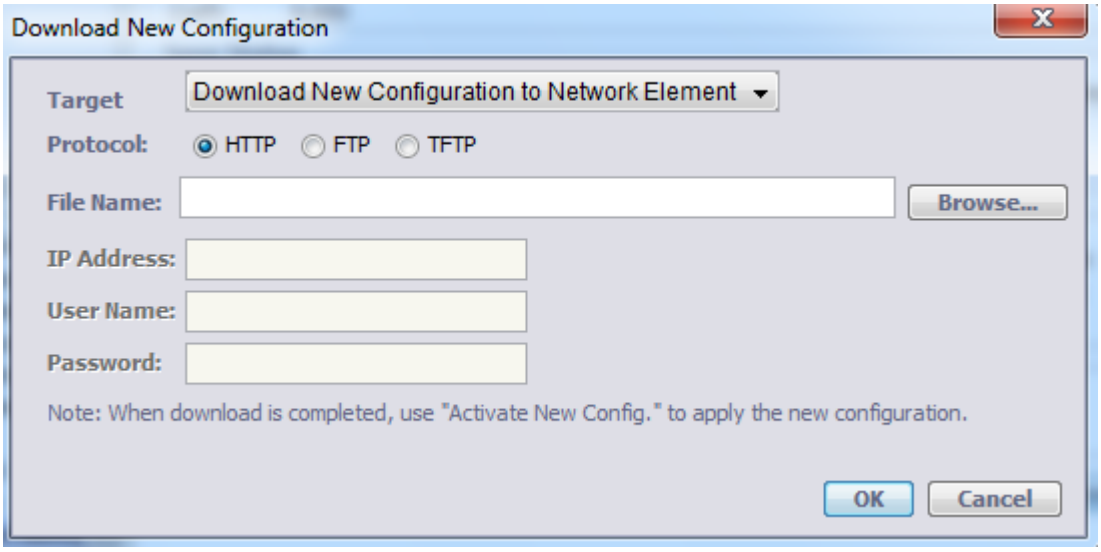
Restoring Step 1: Downloading a Configuration File

To restore the configuration of the ML device system, download a previously saved configuration file to the ML device. During download, the configuration file is checked for validity and compatibility. An error message is displayed if the configuration file is invalid (binary file was manually edited) or incompatible (differences in software version or NE hardware model between the backup and the NE where the backup is restored).

➢ To download the configuration file to the ML device

1. In the Network Element tree, open **System Administration**.
2. Open **Configuration Backup**. The **Configuration Backup** pane opens in the work area.
3. On the Host, run an FTP/TFTP server. The FTP/TFTP directory must point to the configuration directory where the configuration file is stored (for HTTP, skip this step).

4. Click **Download New Config.** The **Download New Configuration** dialog appears.



5. Select a protocol option for download (HTTP, FTP or TFTP).
6. In the **File Name** box, type a file name for the configuration file with a *.dat* extension. If you are using HTTP, you may also use the **Browse** button to locate the directory or the file in which the backup file should be stored - in any case, the file name should have a *.dat* extension.
7. In the **IP Address** box, type the IP Address of the FTP/TFTP server (for HTTP, skip this step).
8. For FTP only, in the **User Name** and **Password** boxes, type the user name and password of the FTP server account.
9. Click **OK**. The configuration file is downloaded to the ML device.

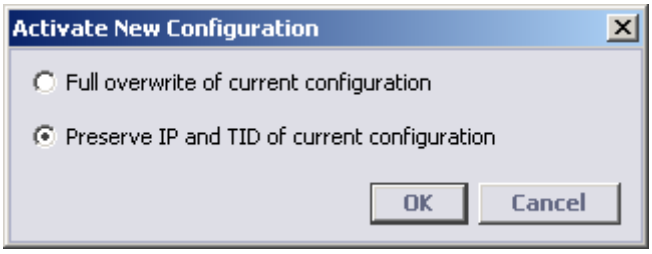
Restoring Step 2: Applying a Configuration File

This procedure is used to activate the restored configuration file. This may take a few minutes.

NOTE: In order to delete the new configuration, go to **Deleting Configuration File** (on page 14-5).

➢ To apply the new configuration file

1. In the Network Element tree, open **System Administration**.
2. Open **Configuration Backup**. The **Configuration Backup** pane opens in the work area.
3. Click **Activate New Config.** The **Activate New Configuration** dialog appears.



4. Select the desired activation method:

- Full overwrite of current configuration - apply full backup file, including unique management identification of NE and unique per deployment HSL Calibration setting and Calibration results. This type of activation is suitable for replacing a faulty ML device.
- Preserve IP and TID of current configuration - apply backup file partially:

  TID, IP, Craft port rate Calibration configuration – all are preserved as configured on the ML NE itself (not according to the backup file);

  Calibration data will not be applied (Calibration, if required, will be re-started from the beginning).

  This type of activation is suitable for deployment of a number of new ML devices with common configuration, but unique identification and deployment case (reach and quality of copper).

5. Click **OK**.

Deleting Configuration File

This is used to delete a restored configuration file before it is activated.

➢ **To delete the new configuration file**

1. In the Network Element tree, open **System Administration**.
2. Open **Configuration Backup**. The **Configuration Backup** pane opens in the work area.
3. Click **Delete New Config**. A warning message appears. Confirm by Clicking **OK**.

Log Files Management

ML devices are capable of registering *all* events that occurred on the device - these include events for both automatically-performed and manually-triggered operations. The ML device maintains and sorts all information as two event types: User Logs and Support Logs.

- **User Logs** - events that affect the behavior of deployed NE. By default the ML device is configured to collect User Logs and store them locally (on flash memory) on the ML itself as log files. These files are maintained as described in **User Log Files** (on page 14-8).

  In addition, some NEs have a Syslog Client mechanism that can forward the relevant events of each User Log to remote storage locations (Syslog Server). Syslog Client on ML devices is maintained as described in **Syslog Client on ML** (on page 14-6).
- **Support Logs** - "debug" information used by Actelis Customer Support experts. These files are maintained as described in **Support Log Files** (on page 14-10).

User Log file data is provided in clear ASCII text format. Support Log file data is provided in ASCII format but may be scrambled. Each log has a size limit of 1MB and is cyclical; i.e. when the limit is reached, the oldest 500KB of data are deleted automatically. Only users with Admin privileges can access the Log files.

NOTE: The Audit log file size is 500KB (with 50% Threshold to flash overloaded file, 0.5MB and 0.25MB accordingly).

User Log files and Support Log files can be observed directly from ML via a Web browser. For more details see Using Web Browser.

Syslog Client on ML

Each ML NE has a Syslog Client mechanism that operates according to RFC 3164. The Syslog client on ML NE supports up to four Syslog Server Destinations, with configurable IP and UDP ports. The Syslog client on ML NE can be configured per destination with three types of events to be sent:

- **Audit** (identical to events collected in AUDIT Log file on the ML)
- **TL1 Alarm**
- **TL1 Commands** (identical to events collected in COMMAND log file on the ML)

NOTE: TL1 Command log can be additionally controlled for level of details to be sent, see **Configuring the COMMAND log file** (on page 14-9).

Syslog Content

For successful integration of ML Syslog Client with Syslog Server, the following format and content of standard Syslog fields that appear in ML records should be taken into account.

Table 85: Syslog Fields Description

SYSLOG Event Field	SYSLOG Facility Field	SYSLOG Severity Field	SYSLOG Priority Field	SYSLOG TAG Field	SYSLOG Content Field
TL1ALARM	14 (log alert)	For CR/SA: 1 For CR/NSA: 1	113	TL1ALARM	Triggered upon REPT ALM <AIDTYPE>. Example of the record content: *10.2.7.17 "ETH-2:CL,LOS,NSA,10-05,13-01-42,NEND,RCV:|"Loss Of Signal|""*
		For MJ/SA: 2 For MJ/NSA: 2	114		
		For MN/SA: 3 For MN/NSA: 3	115		
		For CL: 5 (notice)	116 (14x8+5)		Triggered upon Clearance of TL1 alarm.
		NR	-	-	Unsupported
		NA	-	-	Unsupported, as duplicated in COMMAND log
AUDIT	13 (log audit)	5 (notice)	109 (13x8+5)	AUDIT	Record as in Audit log

SYSLOG Event Field	SYSLOG Facility Field	SYSLOG Severity Field	SYSLOG Priority Field	SYSLOG TAG Field	SYSLOG Content Field
TL1CMD	10 (security / authentication)	5 (notice)	85 (10x8+5)	TL1CMD	All records from Command Log (except autonomous REPT ALM <AIDTYPE>), and in accordance with COMMAND log level configured via TL1. In REPT record, provide type of REPT (EQPT, MLP, etc.) as provided in TL1. TL1 responses for Multiple Operations (with PARTIAL or MERR result) may be not optimized and printed as is in TL1 (multiple rows).

Configure Syslog Client

➢ **To configure Syslog server Destination**

1. From the **Network Element** tree select **System Administration**.
2. Select **Logs Control** which will invoke the Logs Control pane.
3. In the **Syslog Files (Remote storage)** area, Click **Add**. The Add to Syslog Server List dialog appears.

4. Define the destination location parameters:
   - IP address
   - UDP Port
   - Logs to be saved to that destination
5. Checkmark the Send logs to Destination and click **OK**. The newly added location is added to the Syslog Files table.
6. Repeat for additional storage locations.

NOTE: After adding entries to the table, each entry can be edited or deleted.

User Log Files

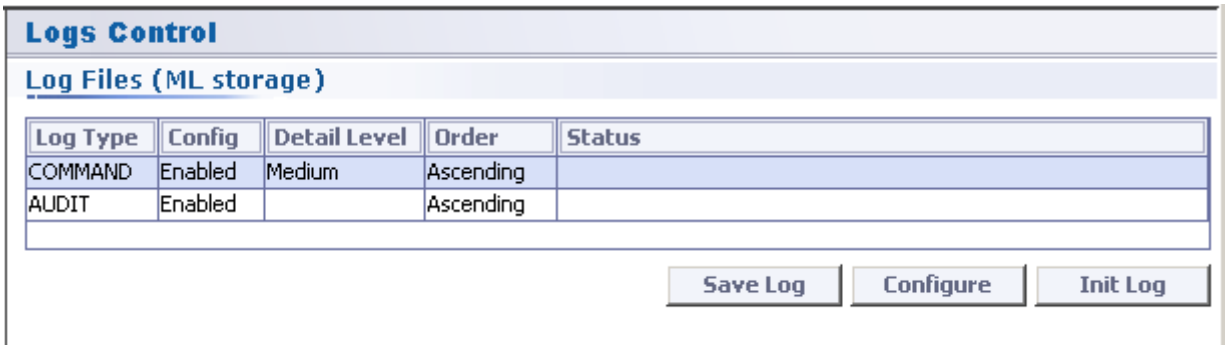
The following user log files are provided:

- **COMMAND log** - includes all ML device TL1 commands and responses, as configured by the detail level (see **Configuring the COMMAND log file** (on page 14-9)). The COMMAND log assists in locating possible causes of the faults in the ML device.
- **AUDIT log** - includes management access events and SNTP synchronization events (see **Configuring the AUDIT log file** (on page 14-9)). The ML device does not log any broadcast session attempts and attempts on permanently closed ports.
  Each successful access attempt is logged with the following information:

  Timestamp of event, IP source / IP destination addresses and protocol type.
  For rejected attempts, the reason for rejection is also provided: Rejected by Access Control, rejected by account authentication (SNMP, TL1 or HTTP).

This chapter describes how to manage User Log files stored locally on ML using **Log Control** pane.

1. In the **Network Element** tree, open **System Administration**.
2. Open **Logs Control.** The **Logs Control** pane opens in the work area.



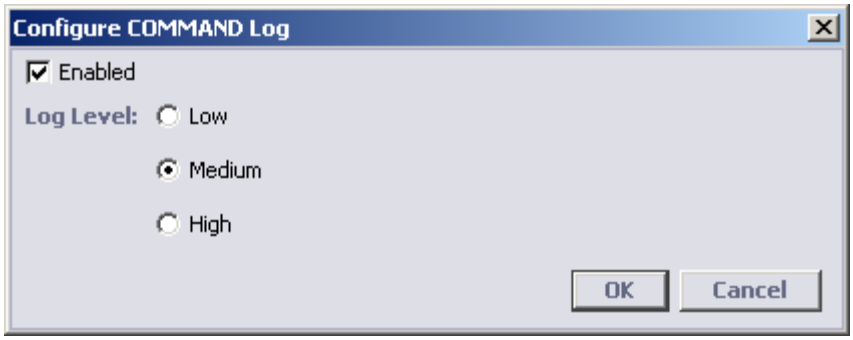
3. In the **Log Files (ML storage)** area, the following operations may be performed:
   - **Configure** the selected type of user log file
   - **Save Log** - save the user log file
   - **Init Log** - Clear (initialize) the specific user log file

Configuring the COMMAND log file

The level of details in which collected information is written to the COMMAND log file can be determined by the administrator.

➢ **To enable and configure the command log file details level**

1. From the **Logs Control** pane, in the **log files** area, select the **COMMAND log** row and click **Configure**. The Configure COMMAND Log dialog appears.

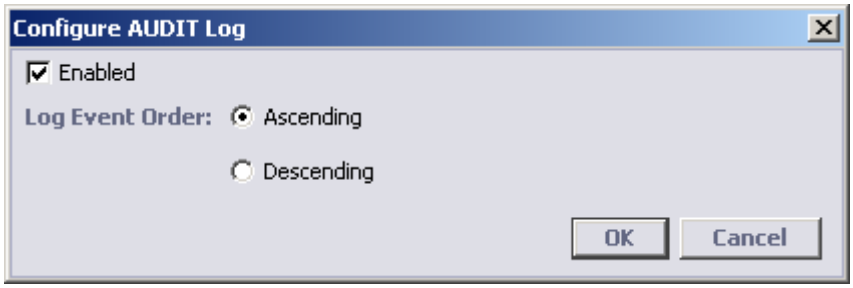


2. To enable the log file, select the **Enabled** check box.
3. From **Log Level** options, select the required log level of the information to be collected (default is medium):
   - Low - All configuration commands and their responses.
   - Medium - All configuration commands, their responses and autonomous messages.
   - High - All commands, their responses and autonomous messages.
4. Click **OK**. The Log Type updated configuration is displayed in the log files table.

Configuring the AUDIT log file

➢ **To enable and sort the Audit log file order**

1. From the **Logs Control** pane, in the **log files** area, select **AUDIT log** and click **Configure**. The Configure AUDIT Log dialog appears.



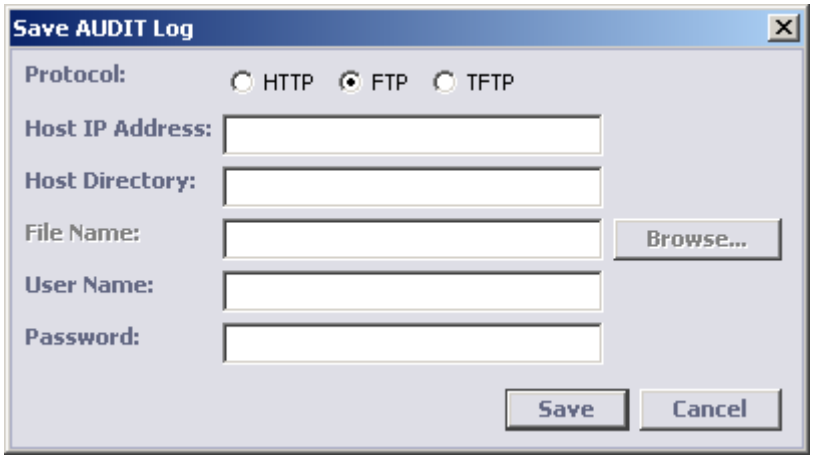
2. To enable the log file, select the **Enabled** check box.
3. From **Log Event Order** options, select the log event chronological order:
   - **Ascending** (default)
   - **Descending**
4. Click **OK**. The updated configuration is displayed in the log files table.

Saving the log file

The log files can be saved to a computer through HTTP or to a Host computer through FTP or TFTP (for the later options, host IP address must be configured). The files can be viewed using any text editor. Saving the log file must be performed via the Ethernet/COLAN (MGMT) ports, not via the Craft port.

➢ **To save a log file**

1. From the **Logs Control** pane, in the **log files** area, select the required log type and click **Save Log**. The Save Log dialog appears.



2. From the **Protocol** options, select one of the following:
   - **HTTP** - copy the file to your computer. File Name and Host Directory are required.
   - **TFTP, FTP** - copy the file to a Host computer. Host IP Address, Host Directory are required. *For FTP - User Name and Password of user account on the FTP server are also required.*
3. Click **Save**. The selected log file is downloaded from the NE to the defined computer.

Clearing a Log File

Each log file can be cleared.

➢ **To clear a log file**

1. In the Element Tree expand **System administration**, click **Log Control**, in the pane select the requested log type and click **Init Log**. A warning message opens.
2. Click **Yes**. The selected log is cleared (initialized).

Support Log Files

The following Support Log Files are available:

- INFO log - registers selected internal software operations, which assist engineers in the Customer Support department in locating system software problems.
- BLACKBOX log - registers critical system events. Important for system troubleshooting.
- INSTALL log - registers calibration conditions. Assists in troubleshooting when installing the system.

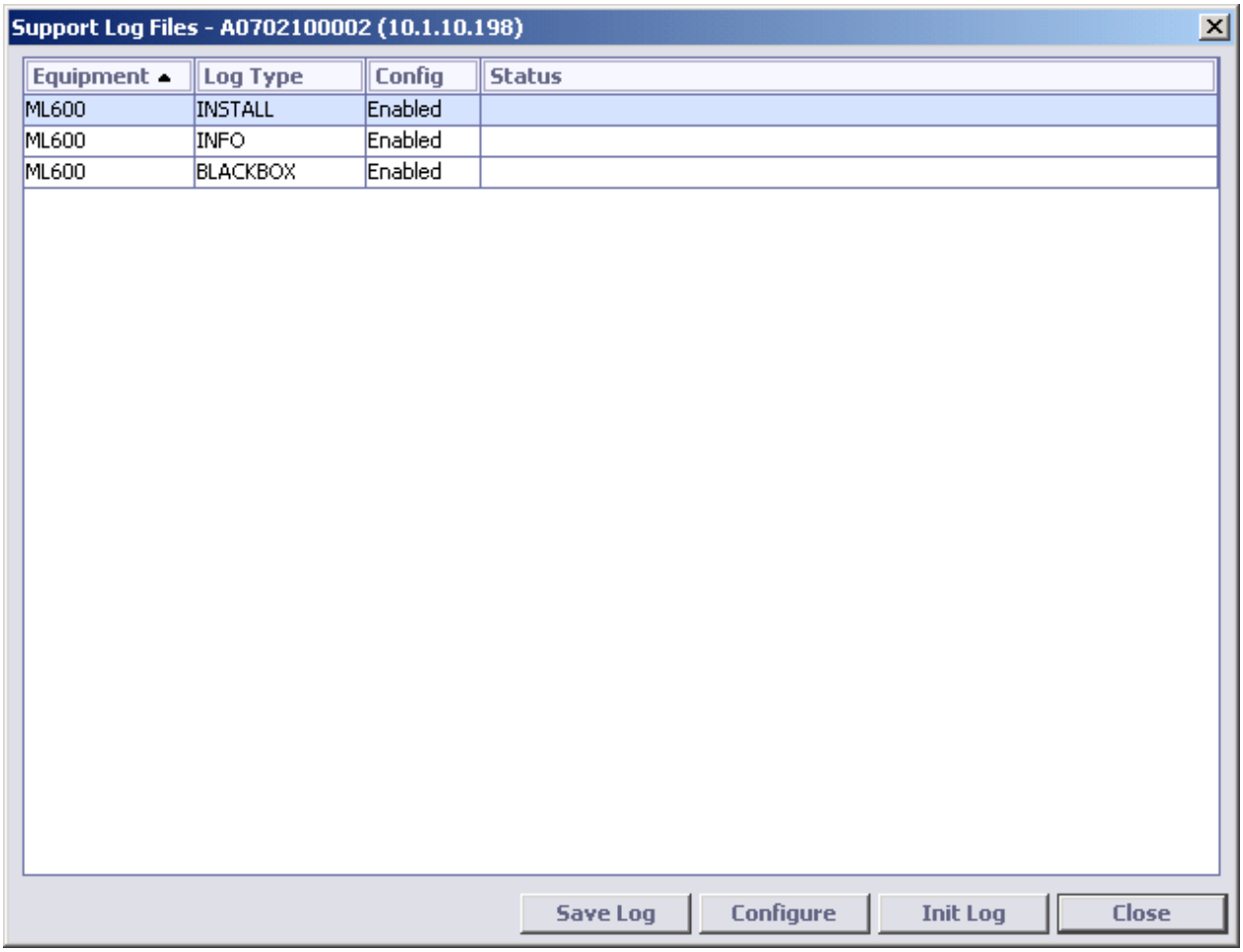
The log files can be managed (disabled, saved, etc.) via the Support Log Files pane.

➢ To invoke the Support Log Files pane

From the **Tools** Menu, click **Configure Support Logs**. The Support Log Files dialog appears. The pane summarizes the types of enabled log files and provides access to log file management options via buttons at the bottom of the pane.

The buttons functions are:

- Save - used to save the selected log file in HTTP, FTP or TFTP format.
- Configure - used to disable a selected log file.
- Init Log - clears the selected log file (after a verification message).

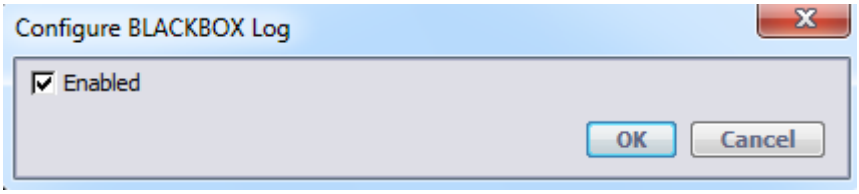


Configuring the log file

All Log Files are enabled by default. Disabled log files do not accumulate logs of that type.

➢ **To disable log file**

1. From the **Support Log Files** pane, select the required log type and click **Configure**. The **Configure Log** dialog of the selected log type appears.



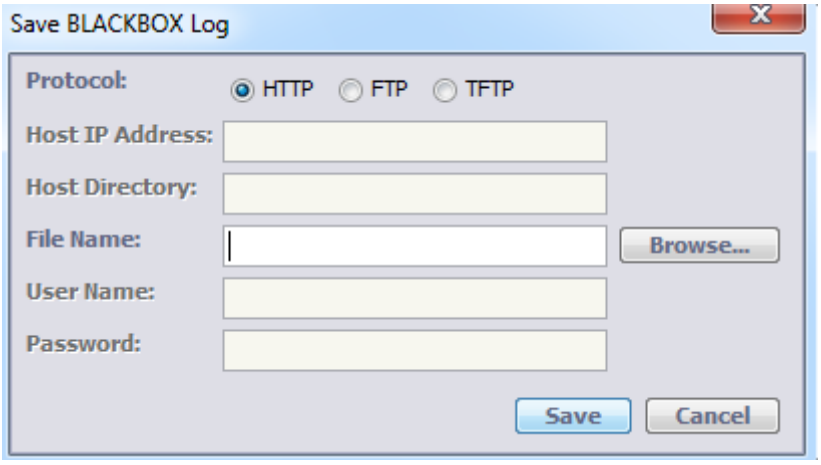
2. To disable the log file, uncheck the **Enabled** check box.
3. Click **OK**. The **Configure Log** of the selected type dialog box closes.

Saving the support log file

The log files can be saved to the computer through HTTP or to a Host computer through FTP or TFTP (host IP address must be configured). The files can be viewed using any text editor. Saving the log file must be performed via the Ethernet/COLAN (MGMT) ports, not via the Craft port.

➢ **To save a log file**

1. From the Log Files pane, select the required log type and click **Save Log**. The **Save Log** dialog of the selected log type appears.



2. From the **Protocol** options, select one of the following:
   - **HTTP** to copy the file to your computer. File Name is required;
   - **FTP** to copy the file to a Host computer. Host IP address and Host Directory, User Name and Password of user account on FTP server are required.
   - **TFTP** to copy the file to a Host computer. Host IP Address and Host Directory are required;
3. According to the selected option, type the required information.

4. Click **Save**. The selected log file is downloaded from the specified Network Element to the defined computer.

Clearing a Support Log File

Each log file can be cleared.

➢ **To clear a support log file**

1. From the **Tools**->**View Support Logs**->**Support Log Files** pane, select the **log type** and click **Init Log**. A warning message opens.
2. Click **Yes**. The selected support log is cleared (initialized).

ML Software Control

Software upgrade can be performed by using MetaASSIST View.

NOTE: The SW upgrade procedure can also be performed via a web browser. For more details see Using Web Browser.

The process consists of:

- Downloading the software from the Host
- Activating the new software
- Committing the software

SW Upgrade (not Downgrade) can also use the Auto Upgrade process which performs Downloading, Activating and Committing SW automatically.

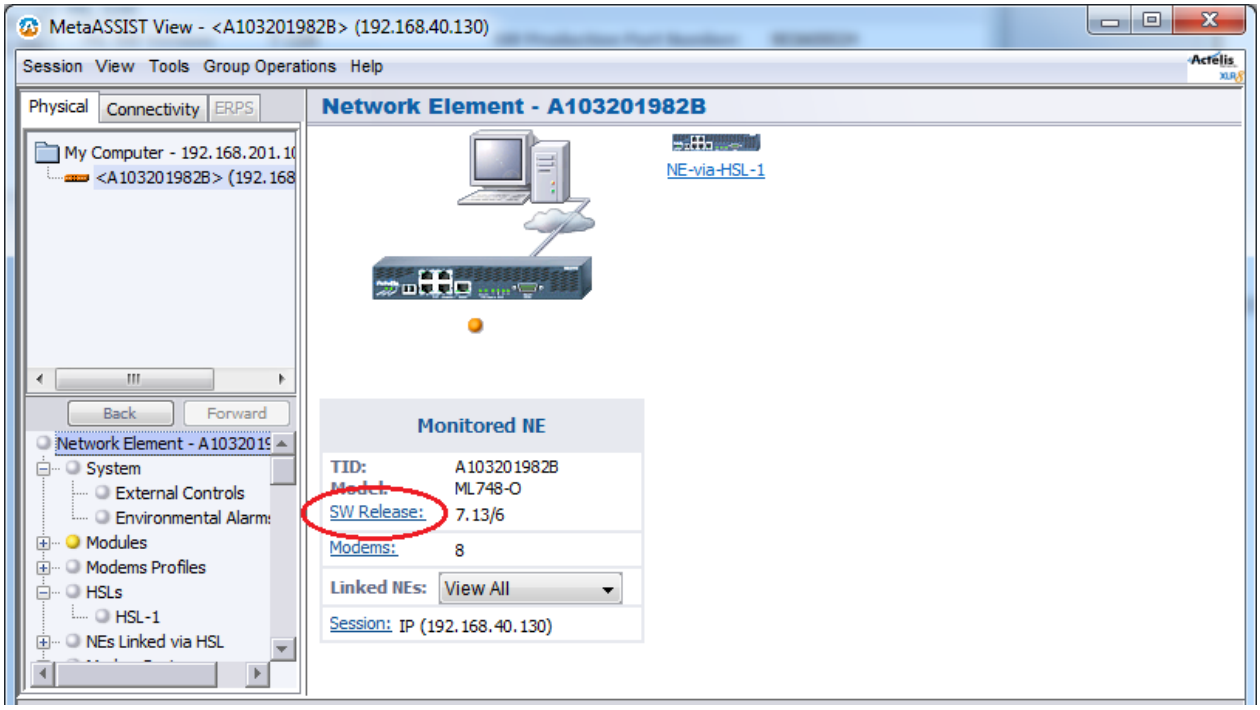
NOTE: Any restart aborts SW Download and SW Activate actions but does not affect Cancel and Commit actions (always completed). Successfully downloaded SW is not affected (removed) by any restart.

SW Release Pane

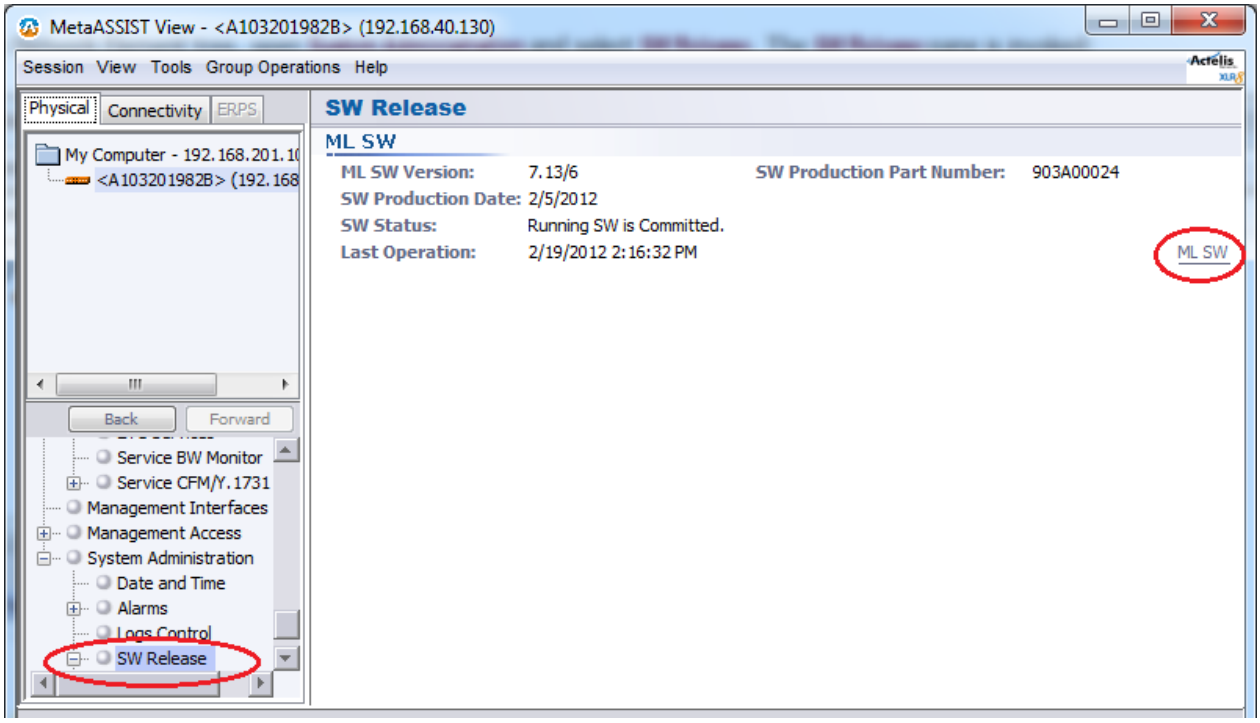
The ML SW Release Pane provides information on the SW in the currently accessed system, status of SW upgrade and various upgrade related options.

➢ To open the ML SW Release pane

1. In the Network Element tree, open **System Administration** and select **SW Release**. The **SW Release** pane is invoked:



2. Click on **ML SW** to invoke the **ML SW Release** pane.



The ML SW Release pane is divided into two window areas:

- Running SW Release - provides status information on the currently running SW.
- SW Upgrade/Downgrade - shows status of SW upgrade

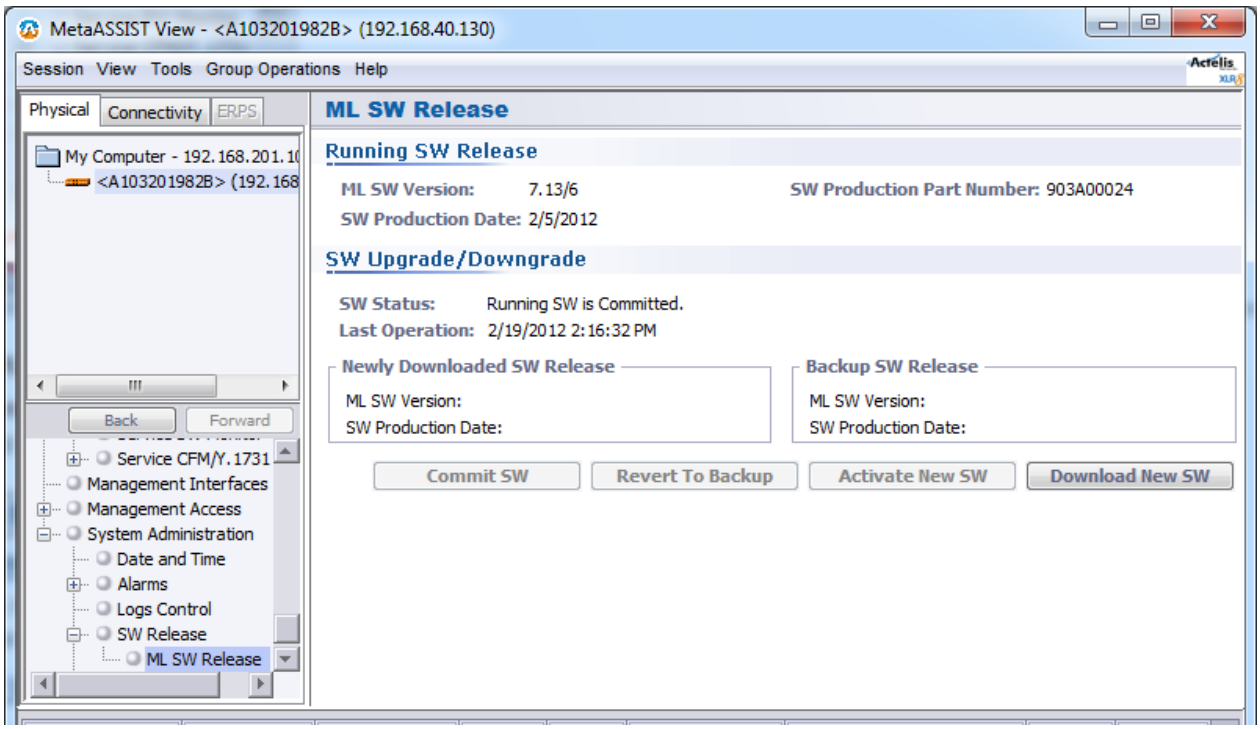


Table 86: SW Upgrade/Downgrade Buttons

Button	Procedure
Download New SW	**Downloading the Software from the Host** (on page 14-16).
Activate the New SW	**Activating the New Software** (on page 14-17)
Commit SW	**Committing the New Software** (on page 14-18)
Revert to Backup	**Reverting to Backup** (on page 14-18)

Requirements for Upgrading the System Software

➢ **To perform this procedure**

- File transfer is to be performed only via non-serial interface; connection cannot be via the craft port.
- IP attributes must be configured on the ML-CO unit, where the ML-CPE unit can be an IP-less device.
- If FTP/TFTP is used, the FTP or TFTP server must be installed and correctly configured on the host computer.

NOTE: Timeout in the TFTP server must be configured to greater than 30 seconds.

Downloading the Software from the Host

NOTE: This procedure can also be performed via a web browser. For more details see Using Web Browser.

ML700 system supports three methods of software download:

- HTTP;
- FTP (requires external FTP Server);
- TFTP (requires external TFTP Server).

➢ **To download software from the Host:**

1. In the **Network Element** tree, open **System Administration**.
2. Expand the **SW Release**. ALL the SW release options will appear.

   Notes:
   1. If some SW update elements are not available, they will be grayed out.
   2. The OLH and the MetaASSIST view SW updates are performed from the same pane.

3. On the Host, run an FTP or TFTP server (the FTP/TFTP directory must point to the new ML700 SW). Skip this step for HTTP.

4. In the work area pane, click **Download New SW**. The **Download New SW** dialog appears.

5. Select a protocol option for download (HTTP, FTP or TFTP).
6. In the **IP Address** box, type the IP Address of the FTP/TFTP server (enabled only for FTP/TFTP).
7. In the **File Name** box, type the file name (this is a file with an *.mft* extension). If required, click **Browse** to search for the file.
8. In the **User Name** box, type the user name (enabled only for FTP).
9. In the **Password** box, type the password (enabled only for FTP).
10. Click **Download**. A progress bar is displayed in the SW Release pane. Please wait until download is completed (the download time depends on the link speed and may take a few minutes (for an Ethernet MGMT link).

NOTE: If the **Download** New SW button is disabled it is possible that a previous SW Upgrade is still in progress. Check the SW Upgrade procedure status. Complete the process by either clicking the **Commit SW** (recommended) button or the **Revert to Backup** button. If the **Commit SW** button is disabled you can click either the **Delete New SW** (recommended) button or the **Activate New SW** button.

Activating the New Software

While downloading the software, the ML device (via System Administration, SW Release pane) displays the SW loading status.

➢ **To activate the new software**

1. In the Network Element tree, open **System Administration**.
2. Open **SW Release** and select **ML SW Release**. The ML SW Release pane opens in the work area.
3. In the work area, click **Activate New SW**. The **Activate New SW** confirmation dialog appears with the following message: "This action can cause traffic hit. Do you want to continue?"
4. To confirm the restart operation, click **Yes**. The ML device will automatically reconnect after the restart operation.
5. After ML device restart is completed, service is restored within a few minutes.

6. When SW update is completed, and the ML device is running with new software, it is recommended to check system integrity and service as follows:
   - Verify that no alarms exist (PROGFLT and/or HWFLT). See **Troubleshooting Alarmed Conditions** (on page 15-6).
   - Check that all other configuration data (VLAN, Bridge, Ethernet) were successfully preserved during SW upgrade.

Committing the New Software

Once you verified that the system is operating correctly you should commit the new software. If you want to revert to previous SW release, perform Revert to Backup, see **Reverting to Backup Software** (on page 14-18). Once the new software is committed, it is impossible to revert back to the old software release. Committing the new software completes the SW upgrade and provides SW backup on the ML device. Another SW upgrade cannot be performed until the previous process is completed, either by committing the new software or reverting to the previous one.

➢ **To commit the new software**

1. In the Network Element tree, open **System Administration**.
2. Open **SW Release** and select **ML SW Release**. The **ML SW Release** pane opens in the work area.
3. In the work area, click **Commit SW**.

NOTE: In case when CPE/RT NE is not provided with IP address (kept un-managed), open the **NEs Linked via HSL** pane and click the **Commit SW** button to commit the SW.

Reverting to Backup Software

This operation invokes the Backup SW available on ML. This operation is only allowed before Commit SW operation is applied.

After Commit SW, the Backup software is the same as the currently running software.

NOTE: Any Configuration changes that occurred in the new (not committed) SW will be lost upon Revert SW operation.

➢ **To revert to backup software**

1. In the Network Element tree, open **System Administration**.
2. Open **SW Release** and select **ML SW Release**. The **ML SW Release** pane opens in the work area.
3. In the work area, click **Revert to Backup**.

File Restore

The following types of files (one each) can be stored in memory storage on the ML devices:

- ML SW Release – the ML software

- OLH – An On Line Help version of the User Manual of the ML device.

Only one file of each type can be stored on the ML device; a new file of the same type, overwrites an existing file. The files are updated by downloading the required software revision from a host computer to the ML device.

Restarting the ML NE

The following restart options are available on the ML device:

- **Restart:** Restarts the system and preserves configuration parameters. Users with admin or write privileges can perform this restart.
- **Restart with Factory Setup preserving management interface configuration:** Restarts the system with initial system factory setup parameters but preserves IP connectivity data and Craft settings from the current setup. Only users with admin privilege rights can perform this restart.
- **Restart with Factory Setup:** Restarts the system with initial system factory setup parameters without preserving any management or service configurations. Only users with admin privilege rights can perform this restart.

NOTE: Restart suspends service.

System restart can be performed locally by turning power off and then on. All configuration parameters are preserved in this case.

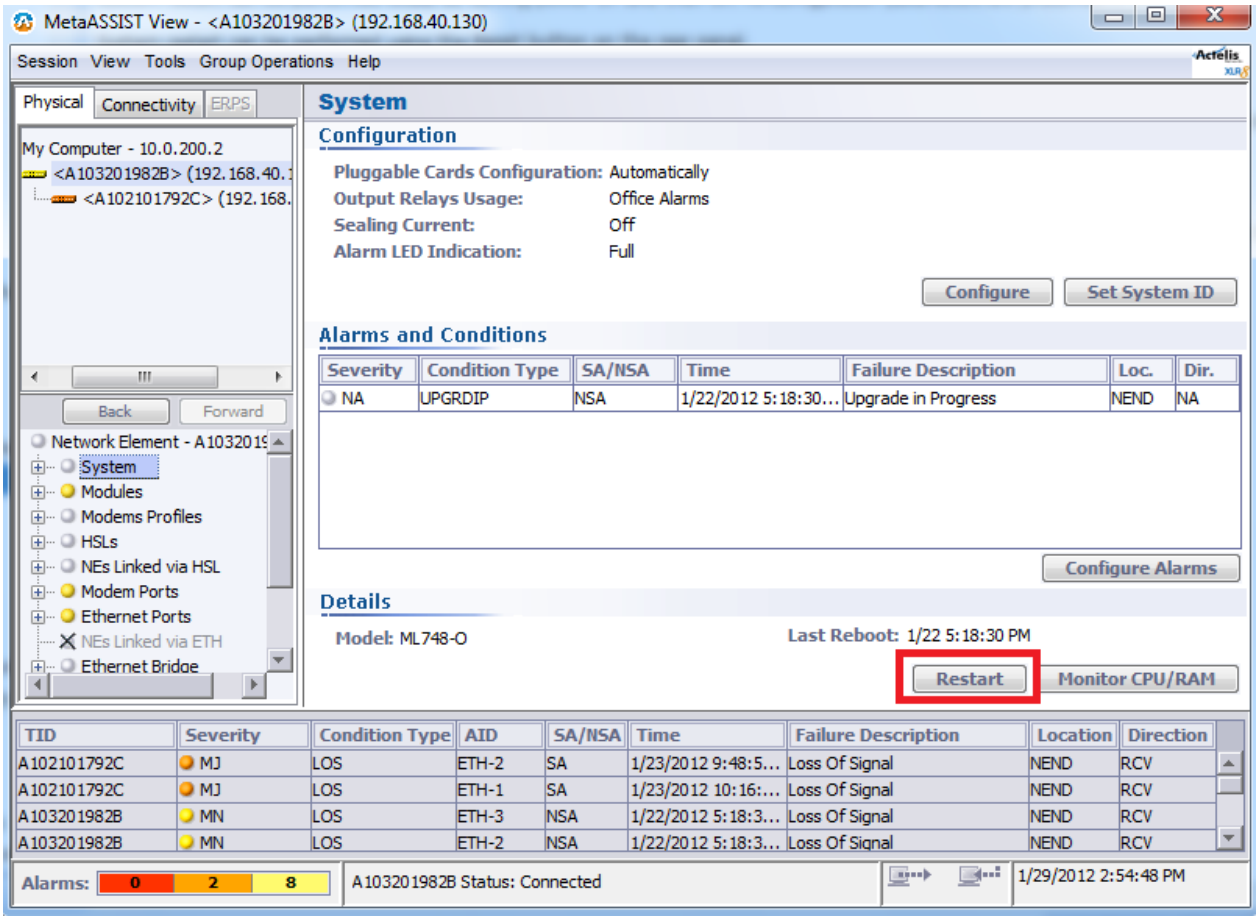
System restart can be performed using the Reset button on the rear panel.

System restart can be performed remotely using MetaASSIST View as follows:

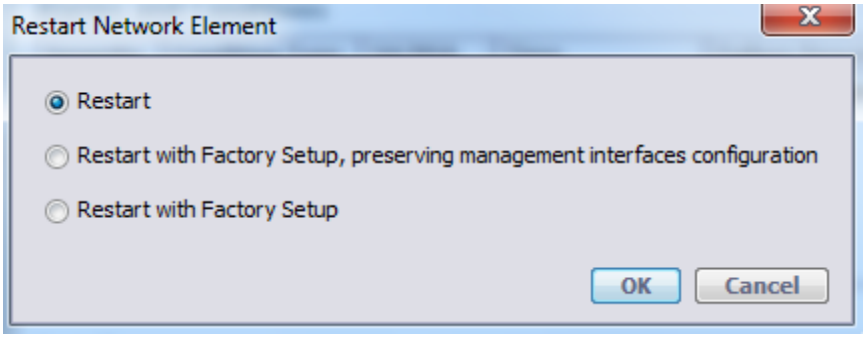
- For the ML device, which is directly accessible via craft port or via Management LAN by own IP address, use **System** pane accessible in the Network Element tree. Dialog box is opened.
- For the ML device, which is indirectly accessible through another NE:
  - For logged in system, use **System** pane accessible in the Network Element tree. Dialog box is opened.
  - For not logged in system (also without IP connectivity defined) use **NEs Linked via HSL** pane accessible in the Network Element tree. Dialog box is opened.

➢ ***To apply restart on either* directly or indirectly *accessible ML device:***

1. From the **Network Element** tree, select **System**



2. In the Details section click the **Restart** button. The **Restart Network Element** dialog appears.



3. Select a **Restart** option.
4. Click **OK**.
5. A warning message appears. Click **Yes** to restart.

Using Web Browser

The ML device Support Page option is used to open a Web browser session directly to a specified ML device and perform the following administrative operations on the specific ML device:

- **Accessing and Navigating the Support Page** (on page 14-21)
- **Configuration Backup and Restore** (on page 14-23)
- **Retrieving Logs** (on page 14-25)
- **Retrieving Files** (on page 14-26)
- **ML Software Control** (on page 14-27)
- **Displaying the TL1 / CLI Document** (on page 14-28)

Operations available on the Page are protected by TL1 User Account (User and Password) and are allowed for *Admin* or *Write* access privilege Users only.

Accessing and Navigating the Support Page

The Web support page is accessed by opening a Web session to a specific ML device.

➢ **To access the Web Support Page:**

1. Open any standard Web Browser available on your PC.
2. Type **http://<IP Address>/support** URL in the *Address* box in your Web browser; where the **<IP Address>** is the IP address of the ML device.

Tip:
To go directly to the TL1 Documentation, enter the above URL without the word **support**.
To go directly to the CLI Documentation, enter the above URL http://<IP Address>/ **CLI.html**.

The following figure shows the layout of the ML device Support Page:

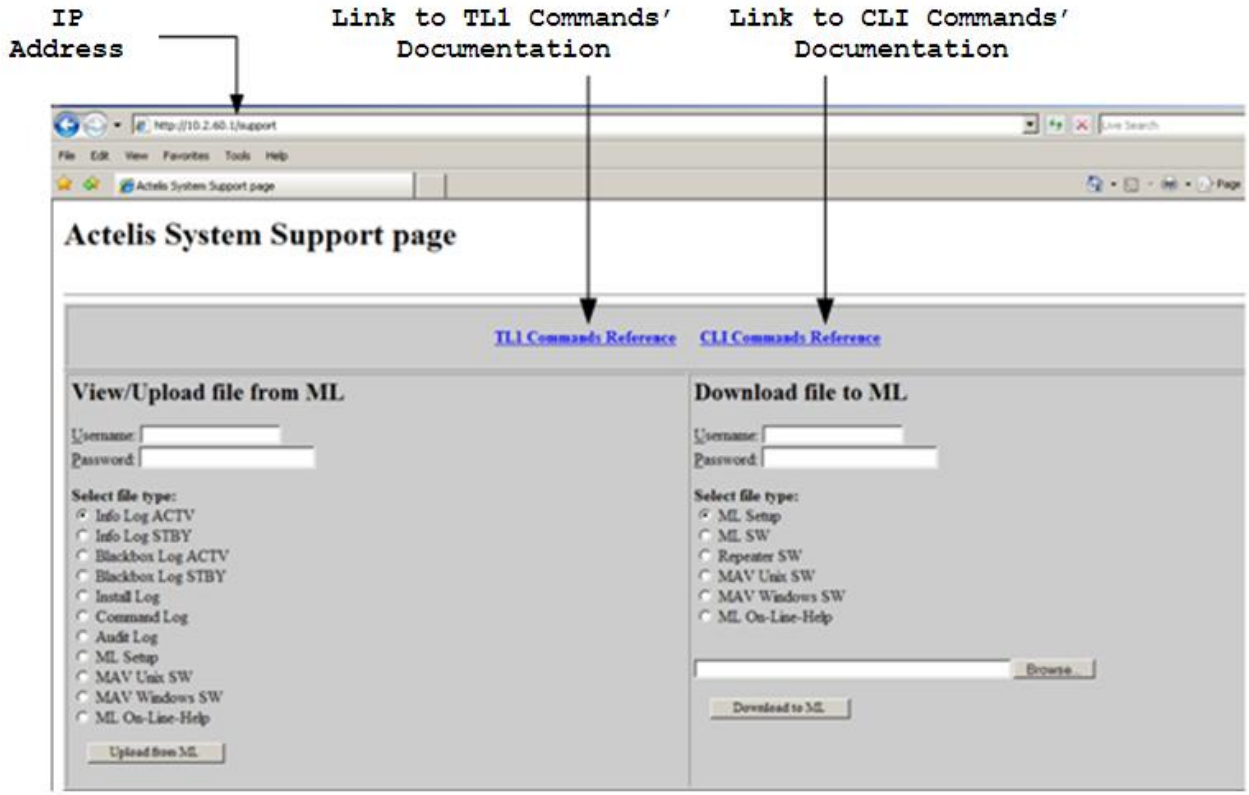


Figure 18: ML device Support Page

The Support page **Download** and **Upload/View** areas are described below:

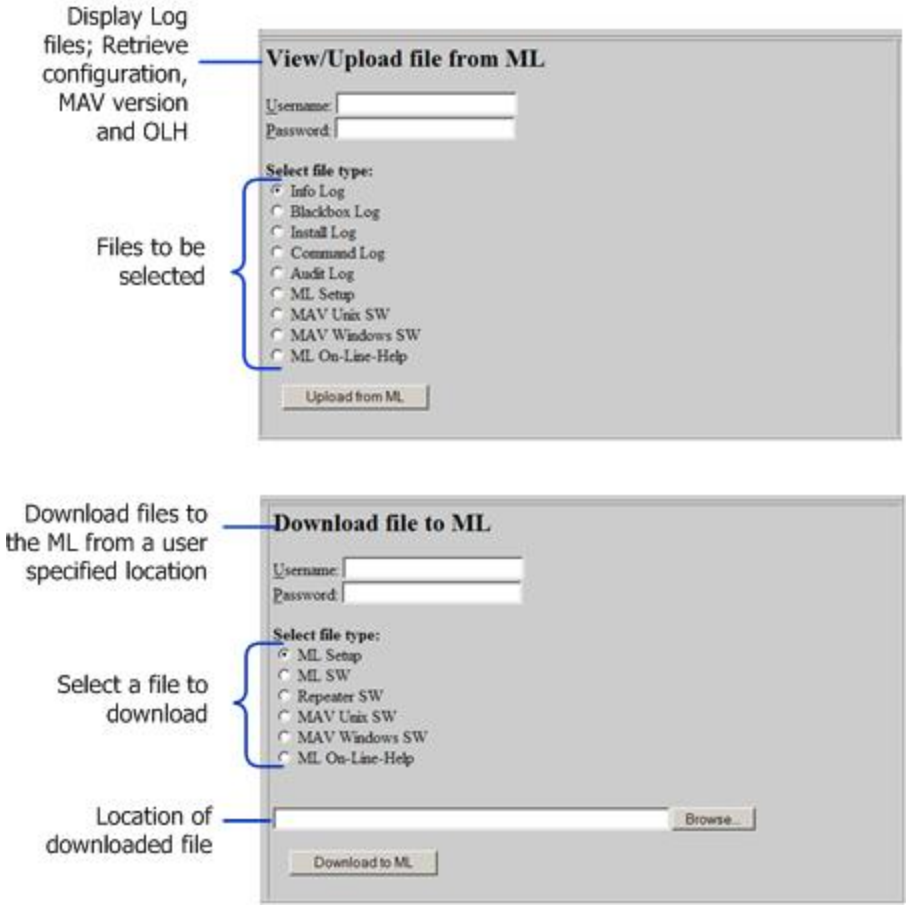


Figure 19: ML device Support Page Areas

Configuration Backup and Restore

This section describes how to:

- Backup the ML device configuration to a file
- Download a configuration file to the ML
- Restore the ML device configuration from the backup file

Backup ML Device Configuration

To enable rapid reconfiguration of the ML device after replacing it, it is recommended to retrieve the Configuration file from the ML device, and save it into a backup directory.

It is recommended to give the backup file indicative name in the following order:

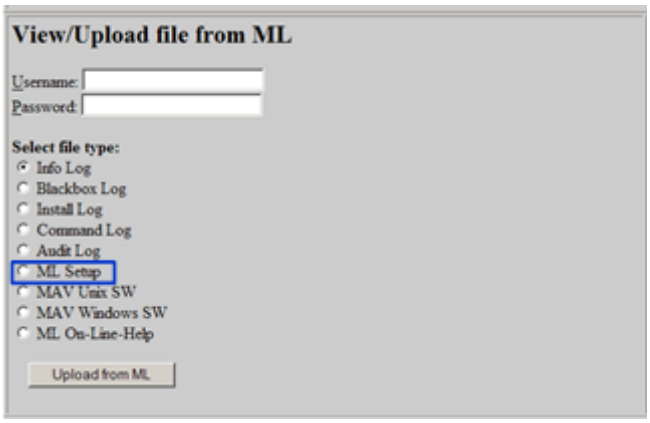
<prod name>-<file type>-<SW revision>-<Node IP address>-<TID>.dat

For example:

ML700-**setup-6_1_12-10_1_9_49-CO_49.dat**

➢ **To backup the Configuration file from the system:**

1. In the **Actelis System Support page**, under **View / Upload file from ML**, type the **Username** and **Password**.
2. Select **ML Setup**.



3. Click the **Upload from ML** button. A *File Download* dialog appears.
4. Click the **Save** button. A **Save As** dialog appears.
5. Choose the directory in which the file will be saved.
6. Type the file name as proposed or rename it if required and then click **Save**. The Configuration file is saved in the directory.

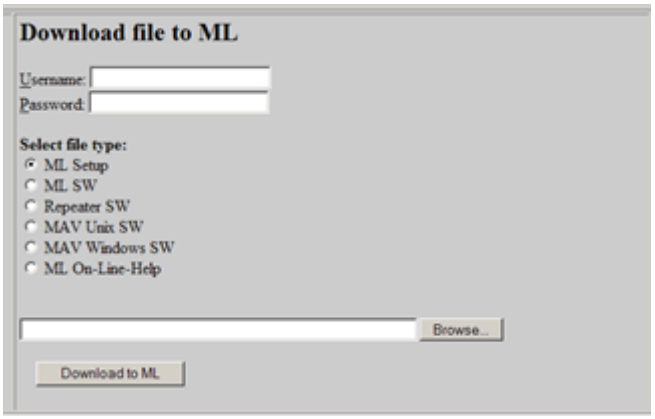
Download ML Device Backup File

When downloading a setup file to an ML, make sure that the Configuration setup file was previously captured from the same (or the same model) ML device and is stored in your PC.

➢ **To download the Configuration setup file:**

1. In the **Actelis System Support page**, under **Download file from ML,** type the **Username** and **Password**.

2. Select **ML Setup**.



3. Type in the path or use the Browse button to specify the Configuration file that was previously saved at a backup location in your PC.
4. Click the **Download to ML** button.
5. After the file was successfully downloaded to the ML device it can be restored as explained in **Restore ML Device Backup File** (on page 14-25).

   The Configuration setup file is checked for validity and then downloaded to the system. If the Configuration file is invalid or does not have the same version as the currently running software, an error message is displayed.

Restore ML Device Backup File

Prior to performing the following operations, verify that the ML device backup file is successfully downloaded as explained in Download ML Device Backup File.

➢ **To apply full Configuration setup data**

- This procedure requires opening a Telnet session. Log in to the system and enter the following TL1 command:
  init-sys:::::restore;
  The ML device restarts and then operates with the new configuration.

➢ **To apply provisioning data only (without TID, IP address, Craft port rate and Calibration data):**

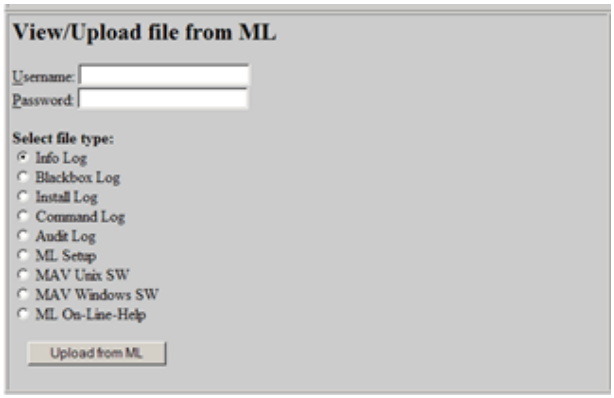
- Log in to the system and enter the following TL1 command:
  init-sys:::::duplicate;
  The ML device restarts and then operates with the new configuration. Continue with configuration of the TID, IP address and HSL calibration, if required.

Retrieving Logs

➢ **To access the logs (Command and System Info):**

1. In the **Actelis System Support page**, under **View / Upload file from ML**, type the **Username** and **Password.**

2. Select a log option by checking its bullet.



3. Click the **Upload from ML** button. The relevant log will be displayed.

For more details about the available logs and their content, see **Support Log File Management** (on page 14-10).

Retrieving Files

The MetaASSIST view running files and an OLH version of the system user manual are stored on every ML system.

These files can be retrieved and saved on your PC or other storage location and later be downloaded to other devices of the same model.

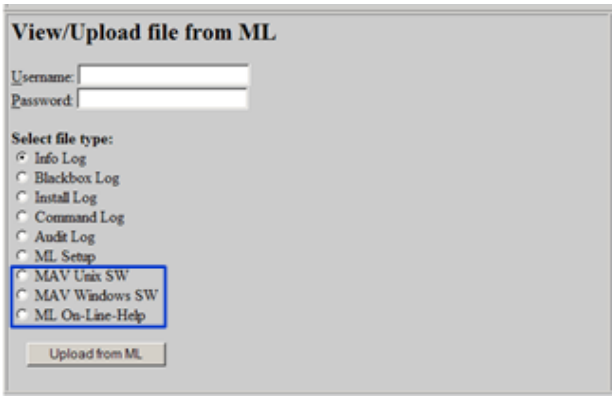
➢ **To retrieve a file**

1. In the **Actelis System Support page**, under **View / Upload file from ML**, type the **Username** and **Password**.
2. Select a file by checking its bullet. The available files are:

   MAV Unix SW - a MetaASSIST view version for UNIX

   MAV Windows SW - a MetaASSIST view version for Windows

   ML On-Line-Help - an On Line Help file of the system User Manual



3. Click the **Upload from ML** button. A **Save** window will appear.
4. Select the location where the file will be saved and name it. It is recommended to select an indicative name as explained in Backup ML Device Configuration . Click **Ok**.

ML Software Control

The process consists of:

1. Downloading the software from the Host
2. Activating the new software
3. Committing the software

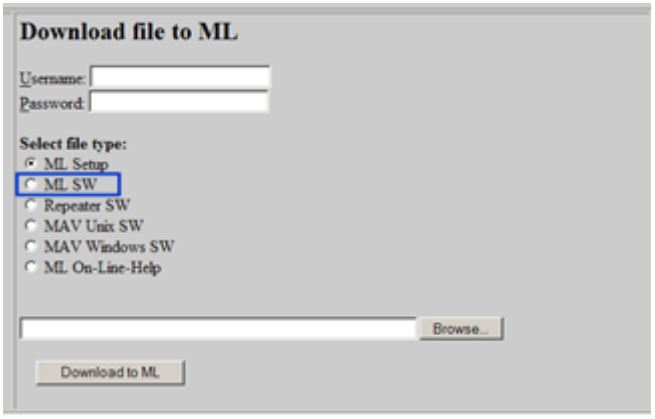
The first step can be performed via the web browser from the support page.

For detailed explanations about this procedure and how to perform it via the MetaASSIST view, see **Updating Software Versions** (on page 14-13).

Download ML Device Software

➢ **To download the software for a system upgrade:**

1. In the **Actelis System Support page**, under **Download file from ML,** type the **Username** and **Password**.
2. Select **ML SW**.



3. Type in the path or use the **Browse** button to specify the SW upgrade file location in the local PC or LAN.

NOTE: The file structure of the software consists of the NE type, release number and build number followed by the extension **mft**.
For example, the file **ML700-r714-18.mft** refers to ML700, Release 7.14 and build 18.

4. Click the **Download to ML** button. The upgrade software is downloaded to the ML device.

Activating the New Software

This procedure requires opening a Telnet session to the ML device.

➢ **To activate the new software**

1. To change the status of the downloaded software from **pending** to **running,** complete the following step:

- Log in to the ML device and enter the following TL1 command to activate the ML device:
  invk-sw;
  The ML device reboots and the upgrade software status changes from pending to running.

2. To commit the SW enter the following TL1 command:
   commit-sw;
   - or -
   To cancel the action enter the following TL1 command:
   canc-sw;
   The ML device reboots and software downgrade is downloaded.

Displaying the TL1 / CLI Document

- To access the TL1 Documentation - click the **TL1 Commands Reference** hypertext link. The TL1 Documentation page opens.
- To access the CLI Documentation - click the CLI **Commands Reference** hypertext link. The CLI Documentation page opens. The TL1/CLI documents explain the syntax for the TL1/CLI commands used in the Actelis ML customer interface. It also defines the Access Identifiers (AIDs) for the Managed Objects in these commands, as well as the required parameters and associated error codes. See the next section for more details regarding CLI usage.

CLI Usage Guidelines

This section provides basic guidelines for CLI usage on ML systems.

A CLI session can be accessed via craft port (RS-232), via telnet and via SSH. Login to CLI sessions is secured via the **ACL** (on page 12-21) (Access Control List) mechanism which - when enabled - allows access only to explicitly defined IPs and protocols.

Up to five simultaneous CLI sessions (in addition to craft port session) are supported per ML NE. The sessions can be originated from different or from the same IP, using different or the same user accounts.

A list of the supported CLI commands is provided in the **CLI document** (on page 14-28) (accessed through the Web support page).

NOTE: CLI is supported in ML700 and ML2300 (with SDU-400 cards) models, for sw release 7.0 and higher. VT100/ANSI terminal types are supported.

Accessing the CLI

CLI interface can be accessed via craft port interface or via telnet.

➢ **To access the CLI interface**

- On **Craft port** interface, the CLI and the TL1 mode are alternated, where TL1 is accessed by default. TL1 or CLI mode can be recognized according to the command line prompt:
  - '**TID**>' is the TL1 prompt
  - '**TID#**' is the CLI prompt

  To toggle between TL1 and CLI, click Ctrl-W (Ctrl-W does not logout the user from the session).
- On **telnet** and **SSH,** CLI is accessed by default when Telnet/SSH port is omitted or specified as 23 (for Telnet) or 22 (for SSH).

CLI Syntax

CLI commands' syntax consists of the following generic structure:

verb element operand value [optional-**operand** optional-**value**]

- **verb** examples: show, config, etc.
- **element** is an optional system element, e.g. card, service, etc.

➢ **CLI syntax guidelines and limitations**

- **verb, element, parameter** must use lowercase letters.
- **values** can use either lowercase or uppercase letters (as specified per each parameter in the CLI document and in-line in CLI help).

- User-defined *string* parameter can use any alpha-numeric values supported by VT100/ANSI terminal (UTF-7 127 codes).
- *String* which includes <Space> and <pound #> symbols should appear between double quote marks.
- *Password* characters are not echoed, although each character typed is prompted with an asterisk.
- *Password* can only use alphanumeric characters keys, <Backspace> and <Enter>.

CLI Function Keys

The following table describes the function keys that are available when using CLI.

Table 87: CLI Function Keys

By pressing or Typing...	Performed action	Comments
Pressing '?' on an incompletely typed word	Shows all valid competitions of that prefix	
Pressing <space> and '?' after a typed word	Shows a list of the words that can follow it	
Pressing <TAB> on an incompletely typed word	Completes the word if it is unique.	Auto-complete (without TAB) is also available.
Pressing the Up and Down arrow cursor keys	Moves back and forward through the command history.	
Pressing the Left and Right arrow cursor keys	Can be used for in-line command editing.	
Typing 'help' on each level shows the relevant information	• For incomplete command - all valid operands on current level • for a sub-level - additional available operands • for complete commands - all input parameters format	
Typing 'help commands'	Shows all auxiliary commands that are executable on any hierarchical level.	
Typing 'help edit'	Shows all keystrokes supported for CLI editing.	
Typing <space> and 'help' after a word	Shows a list of the words that can follow it.	

Using the CLI Document

The CLI document explains the syntax of CLI commands used in the Actelis ML customer interface. It also defines the Access Identifiers (AIDs) for the Managed Objects in these commands, the required parameters and associated error codes. The CLI document is accessed via the web interface (see **Displaying the TL1 / CLI Document** (on page 14-28)).

➢ Using the CLI commands document

The CLI document provides the supported commands with their following attributes:

- **NAME** – full command path to be typed (case-sensitive) to execute the command.
- **SECURITY** – the minimal privileges (read/ write/ admin) required for executing the command.
- **DESCRIPTION** – brief description of command usage.
- **FORMAT** – syntax of input command.
- **PARAMETERS** – input parameters' name, description, type and valid values.

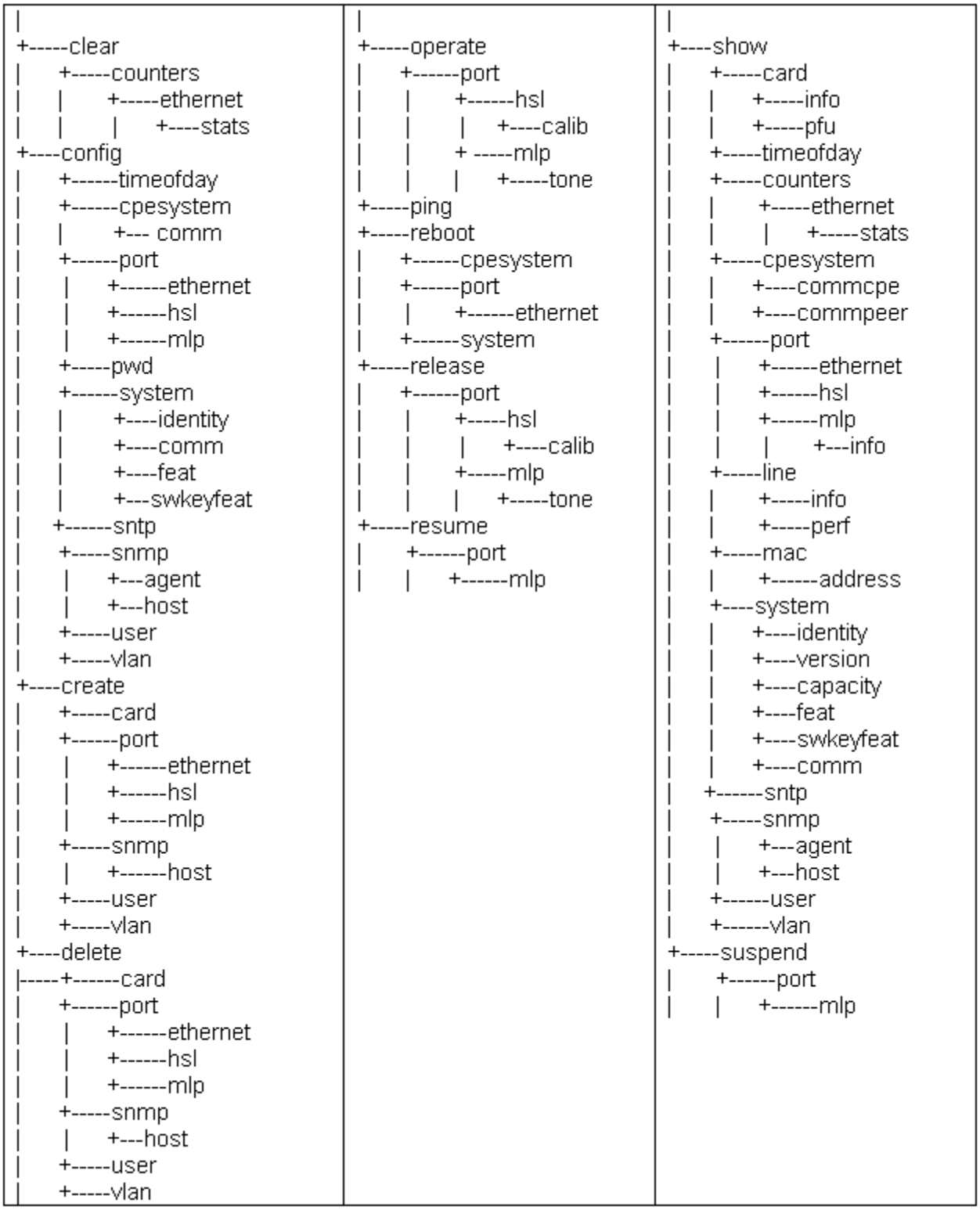
NOTE: Output parameters' Name, Description and Values are provided in-line via *show CLI* commands.

➢ CLI syntax notation used in the document (describing CLI commands' information):

- aaaaaa - mandatory parameter name
- [bbbbb] - optional parameter name
- <x> - parameter's single value
- { x-y } – parameter's range of values
- < x | y > - list of valid values

CLI Commands Tree

The following figure provides the CLI commands tree available in ML systems.



Auxiliary Commands

The following table details the auxiliary commands that are available on any hierarchical level.

Table 88: Auxiliary Commands

Command Name	Command Description	Parameters
logout	Logout from the current user session.	**No input / output parameters.**
whoami	Displays the name and privilege level of the current user.	**No input parameters.** **Output parameters**: username: <> privilege: <>
who	Displays a list of active CLI users.	**No input parameters.** **Output parameters:** Table of Username | Host Interface <username> <IP>/ "CRAFT"
help	Displays context sensitive help for commands.	**Input parameters:** [verb] [element] [keyword] When all parameters are omitted – only list of verbs is provided. When verb is specified (the rest is omitted) – list of element supported for this verb is provided. When verb and specific element are provided – list of keywords for this verb/element is provided. **Output parameters:** List of <name> < description>
clearscreen	Clears the CLI screen. Does not remove history.	**No input/output parameters.**
history	Displays a list of the last 30 commands typed at the CLI prompt.	**No input parameters.** **Output parameters:** <#> <verb element keyword>
exit	Moves up to previously entered level in the CLI tree. Does not logout from the CLI when typed at the CLI main (root) level.	**Input optional parameter** [all] moves up to root.
end	Moves to root without logout. The same should be provided by keystroke <Ctrl-Z>.	**No input/output parameters.**
tree	Display a hierarchical list of all commands or selected commands.	**No input parameters.** **Output parameters:** Hierarchal ASCII tree with 3 columns compact presentation.

Command Name	Command Description	Parameters
echo	Echoes input text to the CLI screen.	**Input parameter:** <text string up to 256 chars length>. If the string contains spaces, the string must be enclosed in quotation marks.
alias	Creates an alias (a character string) for a command.	**Input parameter:** aliasname "command [element[keyword]] to be replaced" If contains spaces, must be enclosed in quotation marks Aliasname – up to 64 chars (alphanumeric). e.g.: <TID.#alias marina "show cpesystem all"
stty	Terminal setting management (number of rows, characters in columns).	**Input parameters:** stty [rows <rows>] | [columns <columns>] Rows –screen height, default is 80 Columns – screen width, default is 80
stty hardwrap	Hardwrap command toggles (on and off) the hard wrapping of output. Terminals usually wrap at the screen width without truncating output, but turning on hard wrapping ensures this.	**No input parameters.**
stty info	Info – display the status of STTY, Namely: Terminal Type (ANSI, VT-100), Screen width (columns), Screen height (rows). Hardwrap (On or Off status)	**No input parameters.**
write	Write message to specific user session.	**Input parameters:** userName textString If the string contains spaces, the string must be enclosed in quotation marks.
broadcast	Write message to all opened sessions.	**Input parameters:** textString If the string contains spaces, the string must be enclosed in quotation marks.

15 Troubleshooting

ML products perform an extensive Self-test during power up, checking the installed hardware, data paths and system configuration. In addition, an in-service diagnostic test is periodically performed during normal operation, ensuring system sanity. In case of an alarmed condition, an indication of the event is given through:

- Front panel LEDs
- Office alarms transmitted via the alarm relays
- Autonomous TL1 reports, alarms and non-alarmed conditions
- SNMP traps

For more information or if you are unable to resolve a problem using these procedures, contact Actelis Networks customer support at techsupport@actelis.com.

In This Chapter

Recommended Test Equipment

To ensure successful troubleshooting of the ML device, the following test equipment is recommended:

- PC with MetaASSIST View
- Line test equipment, such as HP Transmission Impairment Measurement Set (HP TIMS), for testing the copper pairs if required
- DVM for measuring the power supply voltages

LED Fault Indications

ML700 Models do not contain any user replaceable parts. Any hardware faults on the models require the unit to be replaced. Faults due to incorrect facility connections can be detected and corrected.

The following figure shows the front panel of ML700 model:

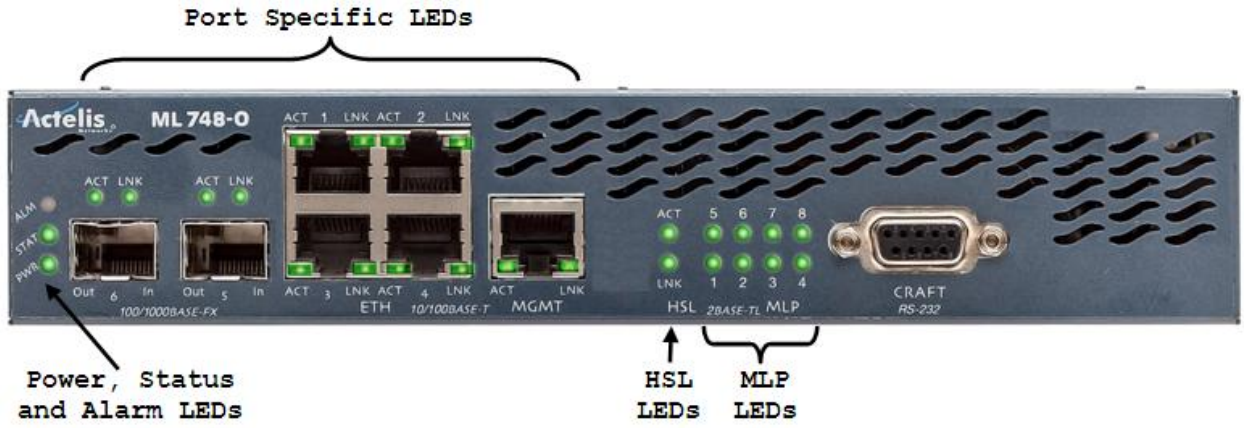


Table 89: ML700 LED Indicators

LED	Status	Recommended Responses
Power	ON - Normal. Power input OK.	--
	OFF - Faulty power input.	Check DC input voltage (-40 VDC to -60 VDC); If there is no DC and AC adapter is used, check if the AC adapter is properly connected to the AC supply; If the problem is not resolved, replace the AC adapter; If the problem is not resolved, replace the ML device unit.
Status	Indicates general status of unit.	
	GREEN - Steady. Normal. No hardware errors.	--
	GREEN - Blinking. Initialization in progress.	Wait for Power on sequence completion. If blinking continues for more than 10 minutes, replace the unit.
	RED - Hardware error detected.	Replace the unit.
Alarm	Indicates alarm on head-end or remote unit.	
	OFF - Normal condition. No alarm is detected.	--
	YELLOW- Minor alarm indication.	Faulty. See **Alarmed Conditions** (on page 15-6).
	RED - Major alarm indication.	Faulty. See **Alarmed Conditions** (on page 15-6).

LED	Status	Recommended Responses
LNK (ETH/HSL port)	Link status: up or down.	
	GREEN - Steady (Normal state), Link up and not blocked by STP.	--
	YELLOW - Steady. Link up but blocked by STP	Check for redundant Ethernet routes
	YELLOW - Blinking. HSL only. HSL calibration or recovery in progress.	Wait for HSL calibration or recovery termination. If calibration or recovery fail. See **Alarmed Conditions** (on page 15-6).
	OFF - Normal if link is down or port is disabled. - Otherwise, refer to recommended actions.	If Normal conditions are not relevant, check the following: 1. Port configuration. 2. Verify that the Port is not administratively removed from service (by disable or suspend operations). 3. Ethernet cables. 4. That external switching equipment is on.
ACT	Link activity (sending or receiving frames) state. An ACT indicator is provided for each of the Ethernet and HSL ports.	
	GREEN - Blinking (Normal). Data activity	--
	OFF - SW initialization in progress - Port is idle (no data transmission) - Port is disabled	Check if external switching equipment is on; Check if port was administratively removed from service.
MLP	Synchronization status of corresponding modem.	
	GREEN - Steady (Normal). Modem is synchronized.	
	OFF - Corresponding modem not in use - Configuration or signal loss.	If the modem is in use, then verify that it was not deleted in the head-end unit or is disconnected (copper loop connections).
	BLINKING - Modem is attempting to synchronize.	Wait for MLP synchronization, typically 1 minute. If HSL is up, and the modem failed, e.g. the line has been permanently cut (also alarmed). The LED will blink until the line is repaired.

Dry Contact Alarm Indications

Critical or Major fault (including power input failure) activates (closes) the corresponding alarm output of the device. The device is normally open and close in case of failure.

Alarmed Conditions

This section describes the recommended Troubleshooting Workflow to follow when an alarm is generated and provides information for analyzing the alarms.

This includes:

- Viewing the system front panel alarm LEDs (and/or the MetaASSIST View system pane), indicating the highest alarm severity that presently exists in the system.
- Analyzing the raised alarm information (detailed in **Field Descriptions** (on page 15-7)). Alarms are provided with a set of attributes that describe the alarm severity, condition type, Service affecting or not, etc.
- Troubleshooting according to the specific Alarmed Conditions Tables (system, equipment, Modem ports, etc.).

  NOTE: The alarms and recommended troubleshooting procedures are described in detail in Appendix F - Alarms Troubleshooting (on page F-1).

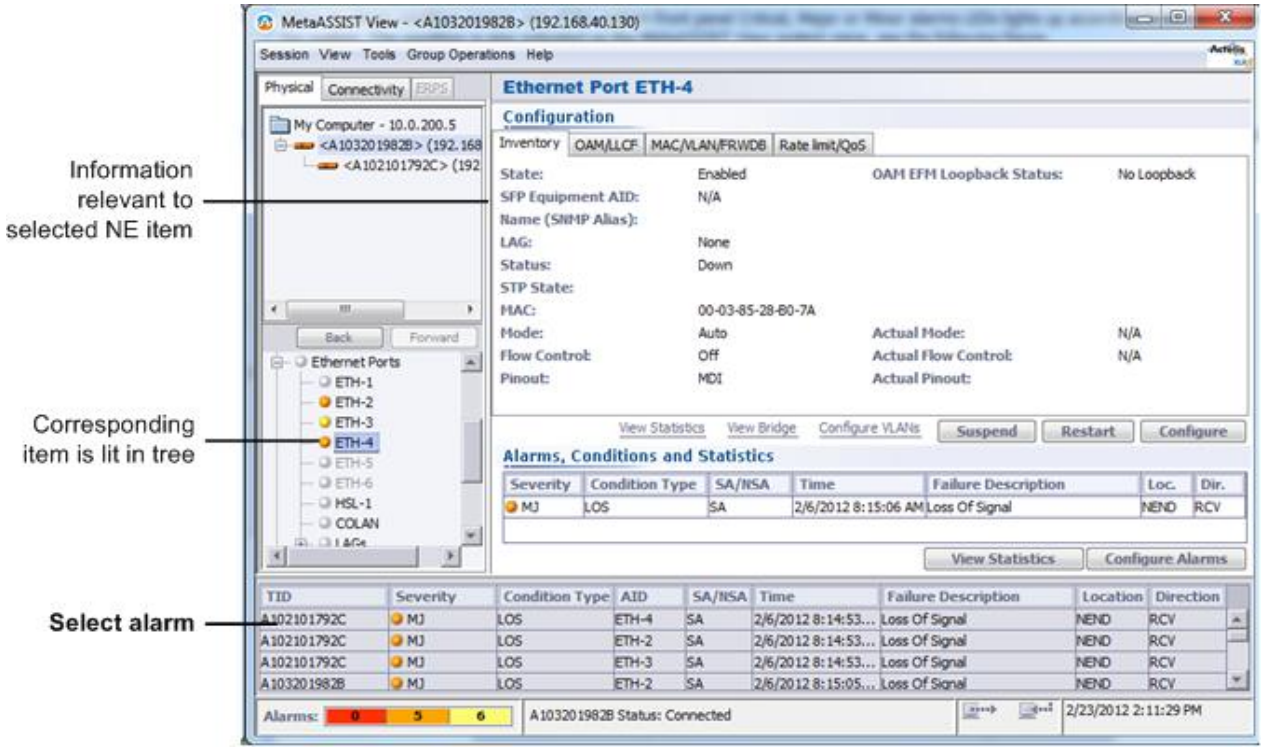
Troubleshooting Workflow

When an alarm condition occurs, one of the system front panel Critical, Major or Minor alarms LEDs lights up according to the highest alarm severity that presently exists in the system. The condition is also indicated on the MetaASSIST View system pane, see the following figure.

➢ **To troubleshoot the alarm using MetaASSIST View:**

1. As illustrated in the following figure, in the system alarms and conditions table (at the bottom of the window), double-click the alarm (any where in the row). As a result:
   - The pane corresponding to the selected component is invoked. The pane provides detailed information on the item.
   - The relevant item is indicated in the Network Element tree.

2. Follow the troubleshooting procedures described in the troubleshooting tables.



Field Descriptions

The following table provides the field descriptions for the alarms and conditions table for both the system pane and component pane.

*Table 90: Field descriptions for **alarms and conditions** table*

Field Name	This field provides ...
Severity	The Notification code of the alarm or message and the MTTR (Mean Time To Repair) requirement according to GR-474-CORE is as follows: • **CR**—Critical - 45 minutes MTTR; • **MJ**—Major - 90 minutes MTTR; • **MN**—Minor - 120 minutes MTTR; • **NA**—Not Alarmed; • **NR**—Not Reported. For additional details on notification codes, see **About Alarm Severity and Conditions** (on page 13-8). *NOTE: NA and NR are not displayed in MetaASSIST View unless their status is change to CR, MJ or MN.*
Condition Type	The condition that caused the alarm or message. As will be explained later in this section, the **Condition Type** field plays a key role in determining the troubleshooting procedures.

Field Name	This field provides ...
AID	The Access Identifier of the component (entity) involved with the alarm or message. The components can be one or more of the following: • System: COM; • Equipment: ML700; • Ethernet ports: ETH-<AID>, COLAN (MGMT); • High Speed Links: HSL-<AID> • Modem Line Ports: MLP-1-{1-8}; • Environmental Alarm Input: EC-1/2; • External Controls: CC-1.
SA/NSA	The effect that reported event has on system operations. Possible values are: • **SA** means event is Service Affecting (i.e., it caused part or all traffic to be dropped); • **NSA** means event is Not Service Affecting (e.g., redundant power input failure).
Time	The date-and-time when the event occurred. Date format is MM-DD; Time format is HH-MM-SS.
Description	Text description of the event.
Location (Loc.)	The event location. Possible values are: • **NEND** - (Near End), the problem is in the monitored ML device; • **FEND** - (Far End), the problem is in the external system attached to the monitored ML device; • **BOTH** - the problem is both in the monitored ML device and in the external system attached to the monitored ML device.
Direction (Dir.)	The direction related to the event. Possible values are: • **TRMT** — the component was transmitting; • **RCV** — the component was receiving; • **BTH** — the component was transmitting and receiving; • **NA** — Not Applicable.

Copper Line Troubleshooting

ML systems provide several tests to assist the technician in troubleshooting copper-pairs:

Copper Lines Installation Problems

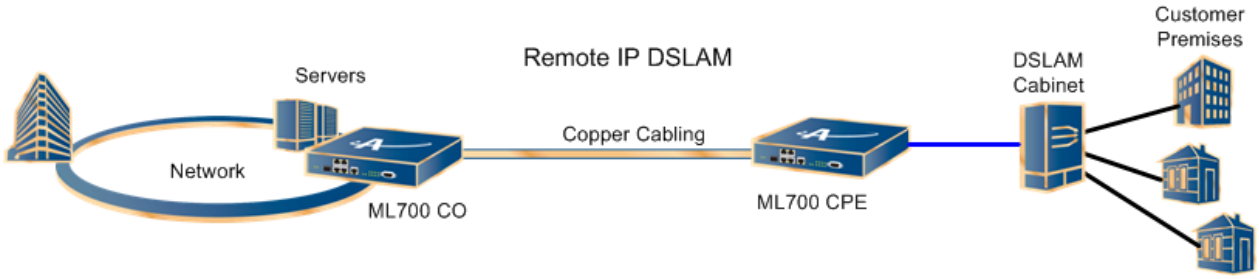
A Copper Lines installation problem could be caused due to inconsistent ML700 Topology: installations where HSL -O is terminated on multiple -R (Customer) destinations, resulting with Ethernet service and in-band management traffic not available.

Inconsistent ML700 Topology

Two ML700 systems connected via copper lines (even a single line) and properly configured will automatically detect the connection.

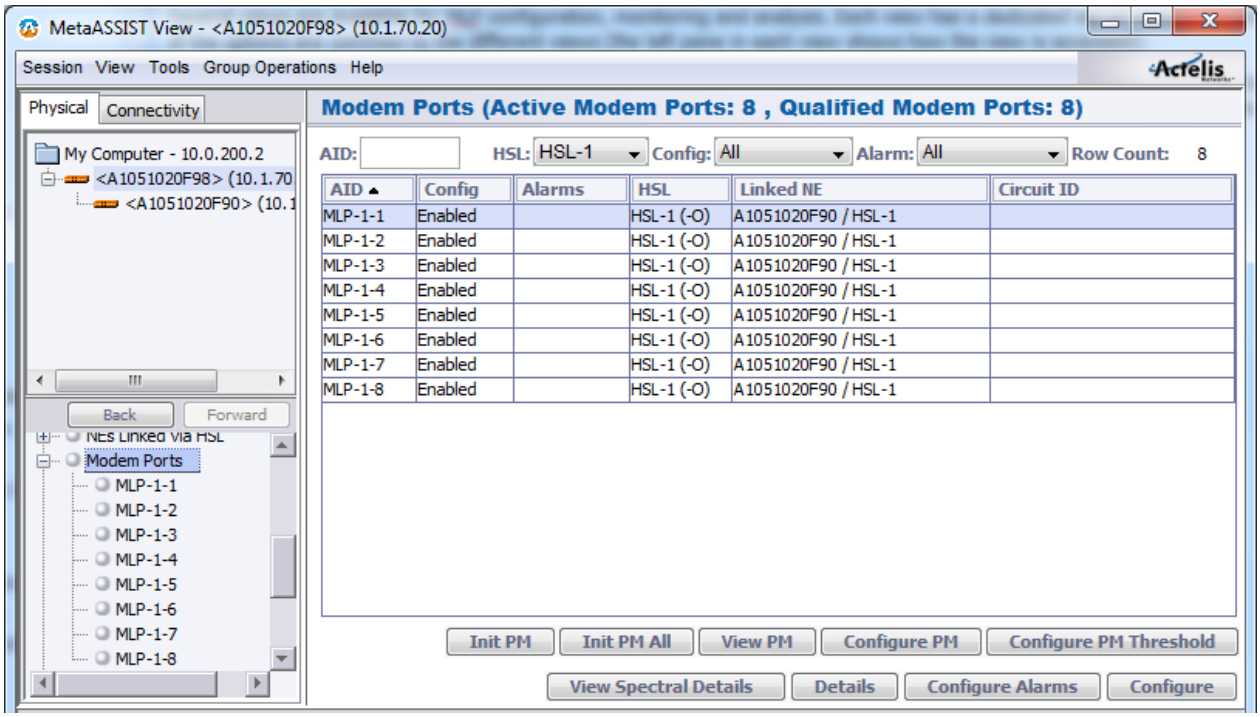
ML700 system with HSL in -O (Office) mode provides automatic discovery of linked ML700 system (with HSL in mode -R (Customer)). It can be monitored using MetaASSIST View panes "HSL port" and "MLP ports" if all Copper Lines bonded within the HSL are terminated on the same system.

The Serial Number of the STU-R system is used to identify the linked ML system. In installations where HSL -O is terminated on multiple -R (Customer) destinations, Ethernet service and in-band management traffic will not be available. The problem is reported by **COPPERMIS** Alarm on a specific HSL, which discovers the mismatch.



Troubleshooting copper mismatch connections (**COPPERMIS**) is allowed from ML device system with HSL in -O (Office) mode only.

The table in the **Modem Ports** pane provides unique identification (Serial Number) of each copper line termination. The table column - "Linked NE" provides Serial Number(s) of the discovered linked by HSL ML device system(s).



➢ To resolve the HSL COPPERMIS problem

Reconnect each copper line with a different Serial Number discovered on distant end. The MLP provides Serial Number discovery immediately after synchronization.

➢ To work around the HSL COPPERMIS problem

1. Reconfigure the HSL (on local side) to exclude the incorrectly terminated copper lines.
2. Cancel HSL Calibration.
3. Delete the MLPs from the HSL.
4. Re-calibrate the HSL.

Modem Suspension and Restoration

ML700 allows you to suspend or restore traffic on a particular MLP port, preserving configuration setup of the port.

➢ **To Suspend or Restore a Modem Port:**

1. In the Network Element tree, open **Modem Ports**. The **Modem Ports** pane opens.
2. From the table, double-click a row. The **Modem Port MLP** pane opens in the work area.
3. To suspend the modem port, select **Suspend**. A warning message appears. Click **Yes**.
4. To restore the modem port, select **Resume**.
5. Repeat steps 1-4 for additional modem ports.

NOTE: You also have access from the Navigation tree as follows: Open **Modem Ports**, **MLPs**. The **Modem Port MLP** pane opens in the work area.

Line Quality Test

Copper lines can be tested by external line test equipment as specified in **Copper Line Testing** (on page 15-11) and by ML system as specified in Qualification by ML system.

Copper Lines Testing

This section contains the procedures and specifications for verifying the quality of the used lines (copper pairs).

Test Prerequisites

To perform the procedures in this section, you need the following test equipment:

- Line tester, such as Transmission Impairment Measurement Set (TIMS);
- Digital Volt Meter (DVM).

For detailed information on how to use the line tester to perform the procedures in this section, refer to your line-tester documentation.

Table 91: Descriptions

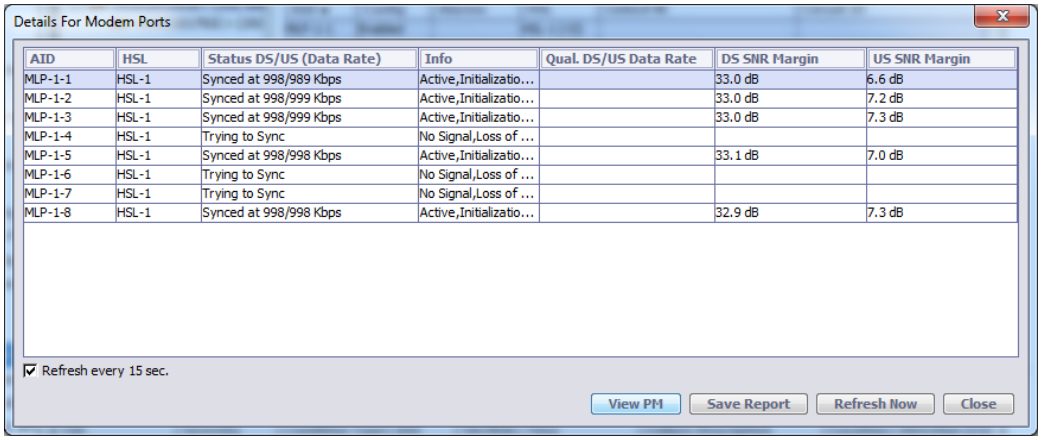
<table>
<tr><th>Test</th><th>Description</th></tr>
<tr><td>Line-impairment Test</td><td>It is always a good practice to verify that all cable pairs are fault free. Good continuity between the two Actelis systems ensures optimal performance of the system.
Procedure: Use TIMS and follow standard telco operating procedures to ensure that all copper facilities are free from physical and electrical faults, such as: opens, splits, grounds, and load coils.</td></tr>
<tr><td>Crosstalk Test</td><td>Use the line tester to transmit a signal with the following characteristics over one of the lines and examine the signal on all adjacent lines:
• Transmit level +13 dBm;
• Transmit frequencies 80 kHz, 160 kHz, 196 or 320 kHz;
• Transmit and receive impedance 135 Ohm.
• Test the lines at any required frequency.
Expected results: For optimum HSL performance, the crosstalk test results should be for twisted pairs (not Quad cables) as follows:
If the test result is 10 dB less than the level specified in the previous table, the line should not be used.
<table><tr><th>Transmit Frequency (kHz)</th><th>Isolation (Attenuation)</th></tr><tr><td>80</td><td>≥ 67 dB</td></tr><tr><td>160</td><td>≥ 60 dB</td></tr><tr><td>196</td><td>≥ 58 dB</td></tr><tr><td>320</td><td>≥ 53 dB</td></tr></table></td></tr>
<tr><td>Noise-to-ground Test</td><td>This test ensures that the lines can withstand signal interferences from electrical sources, such as radio stations, transformers, electric motors and power lines.
Procedure: Follow the instructions in your line-tester documentation to test the lines for an input impedance of 135 Ohm. Make sure that the sleeve or shield of the cable for the lines you are testing is grounded to an earth-ground point.
Expected result: The noise-to-ground test result should be ≤ 54 dBrn.</td></tr>
</table>

Qualification by ML NE

The line qualification routines are part of the calibration process. The results are reported in the **Modem Port Details** pane (see the following figure). This report provides the information for determining whether a line should be dropped or included in the HSL.

➢ To display the Modem Port Details

1. From the navigation area, select **Modem Ports**. The **Modem Ports** pane opens.



2. In **Modem Ports** pane, click **Details (All Modems)** button and check the values in the **Status and Info** columns. The following results can appear:
   - **Synced at ... kbps** - Normal operation expected result;
   - **Trying to Sync** – Modem initialization not completed yet;
   - **Qual. Failed: not used** – Modem failed–insufficient modem rate (i.e. not compliant with EFM modem ratio requirements), see the following table for troubleshooting.
   - **Quarantine**: modem suffer from CRC errors and thus excluded (quarantined) from HSL

Table 92: Possible causes for failures reported in Details for Modem Ports pane

If the Qualification parameter indicates this failure type...	Then the possible causes are...
Quarantine	• Noise margin too low; • Impulse noise; • high external noise; • malfunction in cable (for example, improper twisting).
Qual. Failed: not used (Qualification failed–insufficient modem rate)	• damaged splice; • loop length too long; • bridged tap out of spec; • high external noise; • malfunction in cable (for example, improper twisting).

Data Errors on Modems

To detect data errors on modems link use the **PM counters.** (on page 13-13) Data errors on modems may be due to the following:

1. **Insufficient noise margin** – check the noise margin in the Modem Port Details.
   - Noise margin may be restored automatically if SRA (Seamless Rate Adaptation) is enabled. (SRA may be limited to restore all lost noise margin due to other modem settings such as modem latency that needs to be kept.)
   - If noise margin degrades below minimal value the modem performs auto initialization.
   - If noise margin stays too low (e.g. <3dB) but still above minimal value, consider performing manual modem initialization (HSL recalibration for all modems re-init or single modem Delete and Add)
2. **Impulse Noise** – check the **INM histograms** (on page 6-29). In case that the INP settings are not sufficient, re-calibrate the link with the required INP settings (either increase INP protection or use retransmission mode).

   In case that the INP settings are correct but the link is suffering from many errors (and thus modem is quarantined), check copper pair quality: external noise, damaged splicing, etc.
3. **Non stationary noise source** (e.g. activation of peer xDSL links). Usually link stabilize after a while, if not consider activating the link with higher NM.

   Modem rate degradation may be due to the following:
   - high external noise - use SC graphs (e.g. bit loading, SNR per subcarrier) to find disturbers impact;
   - poor splicing – use attenuation measurements (e.g. Hlog);
   - copper leakage to ground – use external MLT tester to check lines quality

Troubleshooting link with BBA

BBA Amplifier auto tunes to link topology and thus its amplification on Downstream and Upstream directions varies with topology and with spectral regulations (in case of SC type BBA).

BBA is an unmanaged device and its characteristics may be evaluated via the ML unit.

BBA link additional parameters

The following parameters may assist in understanding the topology and the BBA amplification parameters

Table 93: Parameters in link with BBA

Parameter.	Parameter Meaning
EWL	EWL parameter is available in case of regular link without BBA and in case of link with BBA. EWL value may be calculated if overall span loop length is known and cable type is known (for details refer to the Table 78: HSL Details). In case of BBA the difference between calculated EWL and the EWL that the system provides is the BBA gain.
IL300k	Downstream Insertion Loss (measured at 300kHz) is provided only in case of link with BBA. The measured attenuation is composed of the two segments attenuation (ML700-O to BBA and BBA to ML700-R) minus BBA's gains. Link Insertion Loss may be calculated if overall span loop length is known and cable type is known. In case of BBA the difference between calculated Insertion Loss and the Insertion Loss that the system provides is the BBA gain.
IL100k	Upstream Insertion Loss (measured at 100kHz) is provided only in case of link with BBA. The measured attenuation is composed of the two segments attenuation (ML700-O to BBA and BBA to ML700-R) minus BBA's gains. Link Insertion Loss may be calculated if overall span loop length is known and cable type is known. In case of BBA the difference between calculated Insertion Loss and the Insertion Loss that the system provides is the BBA gain.

Ethernet Service Troubleshooting

This section describes:

- Ethernet Service problems that are **Non-Alarmed** (on page 15-16)
- The **Ethernet Service Fault Isolation Tools** (on page 15-20) provided by the system (in addition to the alarm indications)

Non-Alarmed Service Problems

Handling Service problems that are not alarmed is described in this section and includes:

- Guidelines for checking that a service's basic traffic is available (**Verifying Service Traffic and Connectivity** (on page 15-16)).
- Recommended steps to be performed when traffic does not pass through the system (**No Ethernet Traffic** (on page 15-17)).
- A list of the common reasons for Service Traffic Frames dropping (**Insufficient Quality of Traffic** (on page 15-18)).

Verifying Service Traffic and Connectivity

This section provides guidelines for checking that a service's basic traffic is available, allowing the user to check the definitions and to continue with the service fine adjustments, troubleshooting and configurations of required control parameters.

The first step is to check the service connectivity, as described below.

VLAN-based Ethernet Service configuration is available on each NE participating in Ethernet Traffic switching. The configuration of each ML NE should correspond to the equipment attached on both sides of the L2.

Please note the following guidelines for Ethernet Service Configuration checking:

1. Ensure that the planed Ethernet topology done prior to the configuration was implemented correctly. Especially check and implement the following:
   - Ethernet Type of SE-VLAN tag (default 0x8100 Q-n-Q Cisco) can be changed, but should be acceptable by equipment attached.
   - MTU size of frames – each new SE-VLAN tag adds to the frame another 4 bytes. Calculate the largest expected frame and check that it is acceptable in a whole Switching Network.
   - Handle the No-Loop Ethernet Topology - use Spanning Tree Protocol if there are redundant connections. Separate Customer and Provider Bridges Control planes – configure rules of L2CP.
2. Remember that Management traffic plane may be affected by the Service traffic plane you select. Start with Management plane, not Traffic plane configuration.
3. Start from the most remote NE (from the Management Host).

4. If Management connection is lost, restore the connection using Non-IP access to Linked by HSL NEs. The channel works from CO to CPE direction and allows Management LAN connectivity restore.
5. Management LAN connectivity does not guarantee the particular Service connectivity.

No Ethernet Traffic

When Traffic does not pass through the system and there are no alarms or conditions raised in the system, then perform the following in the recommended order:

1. Check if any required by deployment managed entity (equipment and facilities) is disabled (grayed-out in MetaASSIST View). Enable the disabled entities and check for alarms. To resolve alarms, see **Troubleshooting Alarmed Conditions** (on page 15-6).
2. Check if any required by deployment managed entity (equipment and facilities) is not in maintenance mode (when alarms and conditions are not monitored). Restore the managed entities from maintenance mode, see **Operating Alarms** (on page 13-11). For facilities (MLP, ETH, HSL), you can also refer to **Service Suspension and Restoration** (on page 15-10). Check for alarms. To resolve alarms, see **Troubleshooting Alarmed Conditions** (on page 15-6).
3. Check if some SA (Service Affecting) Alarm/Condition are configured with Severity NA (Not Alarmed). Check and reconfigure each SA alarm to appropriate severity, see Modifying Alarm. Check for alarms. To resolve alarms, see **Troubleshooting Alarmed Conditions** (on page 15-6).
4. The **Ethernet Bridge (on page 5-3)** of all NEs in the working topology must be configured as 802.1Q (VLAN aware). Note that for some models, 802.1Q is the only available setting.
5. Check the system for Ethernet Loop:
   - Enable STP on the system, see **STP Configuration** (on page 5-20);
   - Check if STP is also enabled on each ETH/HSL port, see **STP Configuration** (on page 5-20);

   The system will automatically suspend redundant links, the LNK LED will turn Amber.

   To resolve the Ethernet loop, perform one of the following:
   - Keep STP enabled;
   - Disconnect redundant links and disable STP;
   - Resolve Ethernet loop on the external network equipment.
6. Check the system for incomplete VLAN configuration:
   - Make sure that traffic VLANs are configured and match with VLANs defined in all Actelis systems and adjacent WAN and LAN network;
   - You can use 802.1D (VLAN unaware) mode to circumvent incomplete VLAN configuration problems.

Insufficient Quality of Traffic (Frame Drop)

Service Traffic Frames may be dropped due to various reasons. The common reasons are listed in this section.

Note that In-band Management Traffic may affect Service Traffic, since it is given high priority. For this reason, operations applied on indirectly connected NEs may temporarily disrupt the service. For example, SW file transfer to NE, Log files transfer from NE, Configuration Setup Backup and Restore files transfer, or continuous monitoring of NE by multiple operators.

Table 94: Common Problems Related to Dropping Service Traffic Frames

Fault	Description	Corrective action
Oversized Packets Occurrence	Oversized packets are dropped by the ML device system. ML device MFS (this is the Maximum Ethernet Frame size) that can be transferred by the ML device is 1632 Bytes. In case a 4-Byte VLAN tag is inserted by the ML device (on untagged or stacked Ethernet port), the maximum allowed frame size of the customer traffic decreases to 1628 Bytes.	Reconfigure adjacent network equipment (e.g. router) with Maximum Ethernet Frame size of 1632 Bytes or less.
Adjacent Ethernet Port Configuration Mismatch	ML device system and its adjacent network equipment Ethernet port's parameters are mismatched.	Reconfigure Ethernet ports on either ML device or the adjacent network equipment to match.
ML devise Ethernet Port Configuration Inconsistency	WFQ conflicts with Flow Control feature enabled on a particular port.	Disable Flow Control feature to allow WFQ to work properly.
Downstream to Customer Site Traffic is Congested	Congestion on a ML device NE Ethernet port occurs when the HSL BW is greater than the Ethernet port BW (configured to 10MBps, Half or Full). Congested frames are then dropped by L2 priority classification.	Resolve the congestion by configuring the Ethernet port to 100Mbps on the external equipment (if adjacent network equipment allows it).
Upstream from Customer Site Traffic is Congested on HSL	Congestion on HSL port occurs when HSL BW is less than Ethernet port BW (usual 100MBps). Congested frames will be dropped according with selected Port priority classification type. The incoming frame in ML device can be classified by L2 or by L3 priority bits of customer traffic.	Apply L2 or L3 priority classification on Customer LAN Adjacent Actelis system port to drop packets with selective precedence.

Asymmetric Ethernet Traffic	In case of two different Actelis system models used in any topology, you may have asymmetric Ethernet traffic, due to different Egress (Tx) or Ingress (Rx) Rate limit configuration on ports of adjacent Actelis systems (via HSL or Ethernet).	To resolve the problem configure the systems equally
Forwarding By L2 Priority works improperly	Original traffic L2 prioritization can be enforced by Port Priority or higher layers priority configuration (i.e. configured other than by L2 priority) or be affected by improper configuration of L2 classification table.	Set Port Priority to By L2 Priority to classify packets according to their VLAN tag (802.1p priority field) and configure L2 classification tables properly.
Original traffic L2 priority is changed	In those VLAN configurations, where Ethernet port is defined as a stacked port (on Customer LAN Adjacent Actelis system), additional external VLAN tag is added to the original frame, forwarded in upstream to CO. New VLAN tag priority is assigned according with result of Priority-to-Traffic Class classification, applied on the port. Original priority is translated to Traffic Class using Classification table rules (configurable) and then new priority is applied according with resulted Traffic Class (non-configurable). The following Traffic Class-to-Priority rules are applied: Highest traffic class - Priority value 6-7, High - 4-5, Medium - 2-3, Low - 0-1.	There are either forcefully applied per port traffic class (Highest/High/Medium/Low), or "By L2 priority"/"By L3 Priority" Priority-to-Traffic Class classification. Use "By L2 Priority" classification to use original traffic VLAN tag for traffic classification. Also check that L2 Priority classification table (which consist of Priority-to-Traffic Class rules) is configured properly.
Forwarding By L3 Priority works improperly	If original L3 traffic is not pure IP V4/V6 over Ethernet (VLAN tagged or untagged) but is additionally encapsulated (L2TP, PPPoE, etc.), then improper L3 classification is applied. Also, L3 prioritization can be enforced by Port Priority configuration (is configured as other than by L3 priority) or be affected by improper configuration of L3 classification table.	If original traffic is not pure IP V4/V6 over Ethernet (VLAN tagged or untagged) then reconfigure Ethernet Ports priority (do not use L3 priority). If original traffic is pure IP V4/V6 then set Port Priority to "By L3 Priority" to classify packets according to ToS/DSCP field and/or configure L3 classification tables properly.

Ethernet Service Fault Isolation Tools

The ML device system provides the following tools for Ethernet troubleshooting in addition to alarm indications:

- Ping for verifying IP connectivity from the ML device system to a particular (specified) system on your network;
- Ethernet Port Statistics providing standard Ethernet counters per port. For details, see Ethernet Statistics or **Ethernet BW Monitoring** (on page 13-28).

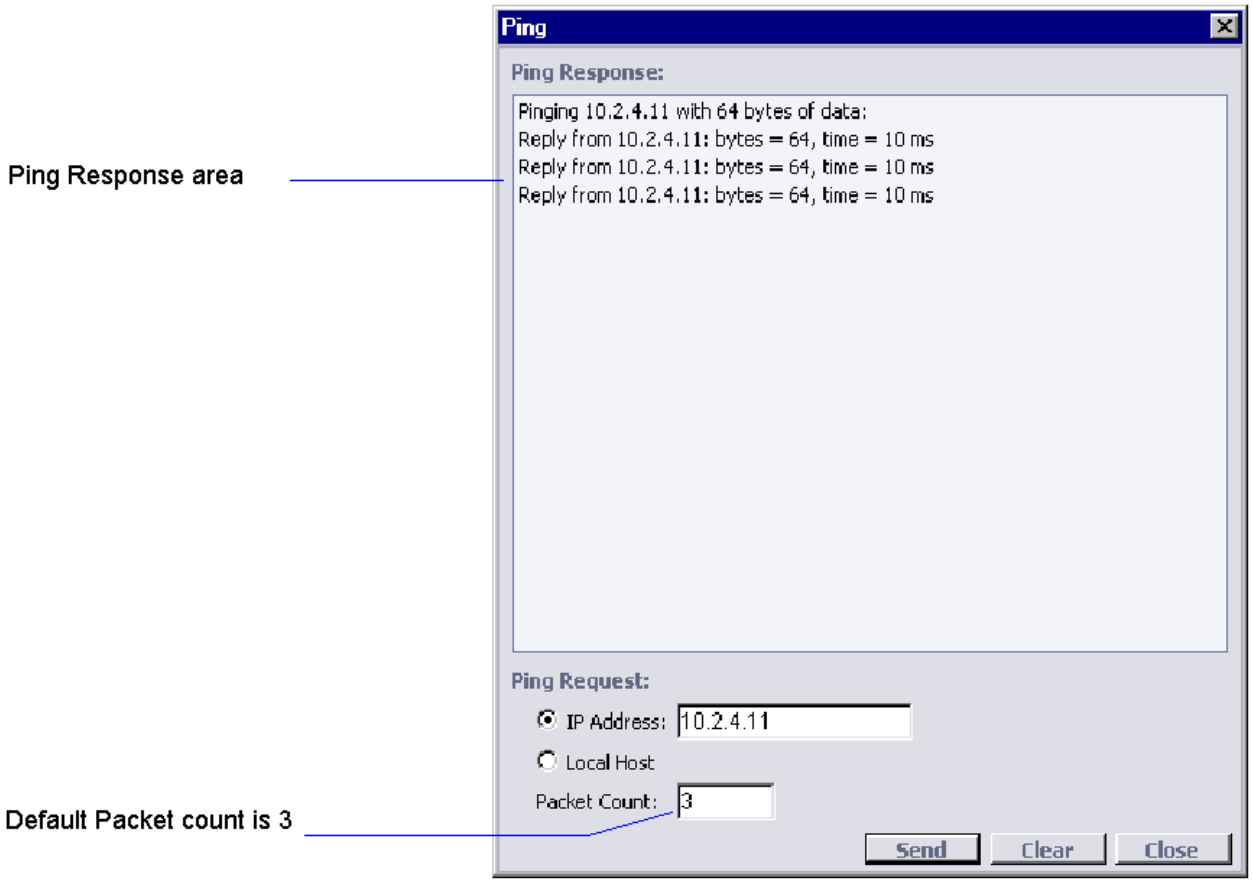
Ping

The Ping dialog box is a network diagnostic tool interface used to verify connectivity to a particular system on your network. For example, you can check if the customer premises equipment is connected to the Actelis system and is online. Ping sends ICMP *echo requests* in the form of a data packet to a remote destination and displays the results for each *echo request*. This exchange is referred to as *pinging*. The Ping command also displays the time for a response to arrive in milliseconds and packet size.

➢ To send a Ping request:

1. In the Network Element tree, open **Management Interfaces.** The **Management Interfaces** pane opens.
2. Click **Ping**. The **Ping** dialog appears. See the following figure.
3. In the **Ping Request** area, select the destination of the required NE: IP Address or Local Host. Type the Host IP address if selected.
4. In the **Packet Count** box, you can set the number of data packets sent by the ping command (default is 3).
5. Click the **Send** button.
   The Ping tool sends an echo request and waits for the echo reply. If the ping was successful, summary lines are displayed in the Ping Response area, indicating the result of the ping. A response message appears after less than a second.
6. During pinging, the **Send** button toggles to **Stop**. You can click **Stop** at any time to stop the ping.

7. Click **Clear** to erase the results from the Ping Response area.



Troubleshooting using Ping

To check if IP stack works properly on ML device system itself

8. Click **Ping**.
9. Select the **Local Host** option.
10. Click **Send**.
11. Check that Ping successfully replied 3 times.
12. Click **Close**.

To check IP connectivity between ML device system and Remote Management Network:

13. Click **Ping**.
14. Select the **IP Address** option.
15. Type in the IP address (any known IP in Management Network).
16. Click **Send**.
17. Check that Ping successfully replied 3 times.
18. Click **Close**.

802.3ah Ethernet OAM Tools

The 802.3ah standard or OAM for Ethernet in the First Mile is limited to managing and troubleshooting the single-hop from the closest access platform to the customer's premise, improving service reliability in this part of the network that often is problematic. As a link level standard operating on a port by port basis, this standard cannot monitor an end-to-end link or EVC or a particular application.

To enable and configure 802.3ah

802.3ah is enabled and configured on CO and CPE Ethernet Port Configuration dialog on either side of the link (by default, the option is *disabled* on all ports).

Since EFM OAM can only monitor a single hop (i.e. from CO to CPE), messages are contained in the link. OAM information is not passed to other network elements and alarms and info messages are extracted from or sent to the operators access platform.

Key functions include:

- **EFM OAM Discovery.** Enables ML device systems to identify the OAM capability of other ML device systems (such as CPE) and exchange state and configuration information such as Mode, Vendor, Unit ID, loopback support, and more. The MAX OAM MFS size =1518 bytes. The transmit OAM size is optimized to the content (minimum 64 bytes).
- **Remote Loopback** (on page 15-22) with timeout test - a simple port-level end-to-end test function to check traffic transmission performance.
- **Remote Failure Indication (RFI)** - provides indication of loss of signal (LOS). On ETH Optical Ports (100FX and 1000FX) with 802.3ah option enabled, when a loss of signal is detected by the receiver, LOS alarm is raised on a local port and OAMPDU frames with "link failure" bit set to 1 are transmitted back towards the opposite port. When OAMPDU frames with "link failure" bit set to 1 are received from a peer port, the RFI alarm is raised on a local port.

  NOTE: RFI origination is unsupported on port configured in MODE=AUTO (auto-negotiation) or HALF-DUPLEX, as specified in IEEE 802.3ah clause 22.2.4.1.12.

Performing Remote Loopback

This OAM option is used for link level testing between 802.3ah OAM-capable devices. This test is used to compare TX/RX on the local port and ensure quality (frame loss) and throughput (speed and duplex) of the link between two ports (local and remote). The process is performed as follows:

- Configuration is applied on the *local port* (the port that will forward through test traffic).
- The local port will automatically (by special OAM PDU) configure the remote port (the port that will perform a loopback of test traffic).
- After configuration is completed, every Ethernet frame received on the remote port will be transmitted back to the local port, without frame modification.

Note the following:

- The local port can be *manually* operated to resume remote loopback (special OAM PDU will be sent toward remote port automatically).
- In addition, each port can be locally configured to resume the remote loopback applied after a timeout of 5 to 30 minutes. The Timer is started upon initial remote loopback request OAMPDU arrived and is not reset upon follows OAMPDU, i.e. loopback cannot be applied longer then predefined time. For infinite loopback (until manual resume), timeout option should be turned Off.

➢ To perform Remote Loopback:

NOTE: Test traffic is to be provided by an external device.

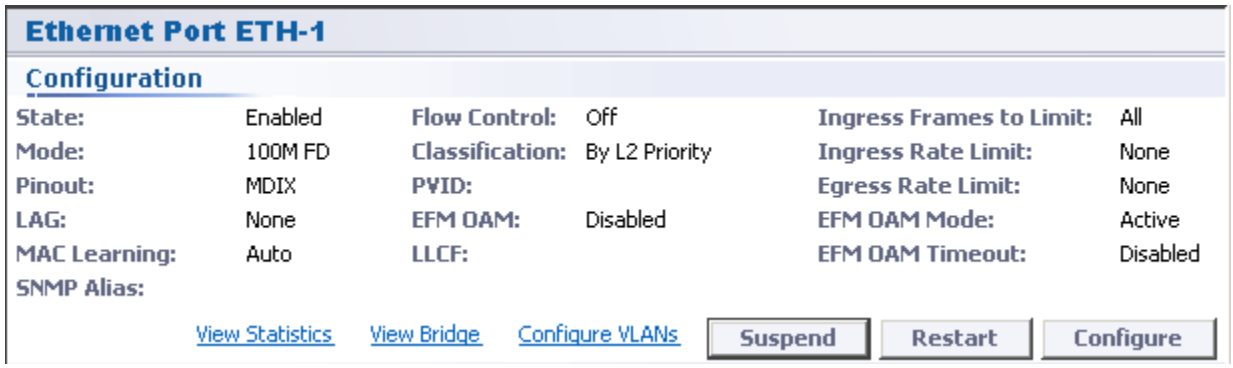
1. In the Ethernet port configuration dialog:
   - Enable 802.3ah OAM on the link ports on which the test will be performed.
   - Configure the Loopback Timeout parameters.
2. Interconnect the ports using a standard Ethernet cable.
3. Verify the connection as follows:
   - Access the Ethernet pane of one (or both) of the interconnected ports ((in the **Network Element** tree, under **Ethernet Ports,** click the Ethernet port - the relevant Ethernet port appears).
   - In the **EFM OAM** area, click **Details** and verify that **Peer Capabilities Loopback** is enabled; otherwise, check the connection.
4. In the port pane, **EFM OAM** area, click the **Operate Loopback** button to perform the loopback test.
5. In the port pane, EFM OAM area, click the **Loopback Statistics** button. The EFM OAM Statistics window appears.
6. Use the window to analyze the Loopback test results.

Ethernet Service Suspension and Restoration

In order to ensure that Ethernet Port setting (provided on local or peer port) is successfully applied or in order to re-initiate link negotiation, it is recommended to either Restart the Port or Suspend and then Resume the port.

➢ To Suspend or Restore a service via an Ethernet Port

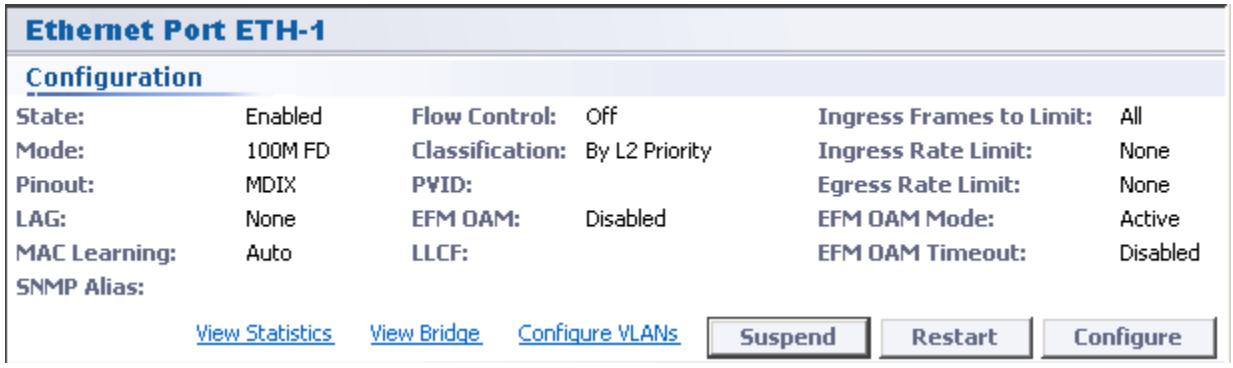
1. In the Network Element tree, expand **Ethernet Ports** and select the relevant port. The corresponding Ethernet Ports pane appears.



2. To suspend the service:
   - In the configuration area, select **Suspend**. A warning message appears.
   - Click **Yes**. The port is down.
3. To restore the service:
   - In the configuration area, select **Resume**. The port is Up.

➢ To Restart a service via an Ethernet Port

1. In the Network Element tree, expand **Ethernet Ports** and select the relevant port. The corresponding Ethernet Ports pane appears.



2. To restart the service:
   - In the configuration area, select **Restart**. A warning message appears.
   - Click **Yes**. The port will be re-started.

Management Connection Problems

Unsuccessful connections can be due to configuration or login problems as follows:

Configuration Problems

Craft Port Access problems:

- Local Craft port setting (baud rate) specified in MetaASSIST View, configured on ML device and configured on your management host serial port (COM1/COM2) do not match. In this case, MetaASSIST View tries to reconnect indefinitely. It is recommended to check the connection parameters. If local craft connection cannot be established, configure your PC Baud Rate according to ML definitions, change the Baud Rate in the Connect dialog box, and try to re-connect.
- If connection was not established at any of the baud rates this implies that the Craft port was disabled. Try one of the following:
  - On Actelis system, try to use IP access (via COLAN (MGMT) or ETH-<ID>) if IP address was already configured beforehand;
  - Replace the Actelis system with another one (with factory setup).
  - Serial port connector or cable is damaged. It is recommended to check physical connectivity;

Ethernet Port Access problems:

- **Out-of-band management problems:** In all of the following cases, MetaASSIST View tries to reconnect indefinitely. Resolve the problem and MetaASSIST View will reconnect automatically.
- Verify that the ML device COLAN (MGMT) port is enabled (using a craft connection). By factory setup, ML device COLAN (MGMT) is disabled;
- COLAN (MGMT) port settings do not match PC port configurations. This can be due to the following:
  - Cable configuration does not match the attached cable. The COLAN (MGMT) MDI pinout is by default MDIX and requires an RJ45 connector with a crossover cable;
  - Speed and Duplex between the PC and COLAN (MGMT) do not match. By default, the Speed and Duplex mode of the COLAN (MGMT) are auto-negotiated. If your PC or workstation port does not support this feature, then speed and duplex mode should be manually configured on the ML device via Craft;
  - Connector or cable is damaged. It is recommended to check physical connectivity.
- **In-band management problems:**
  In all of the following cases, MetaASSIST View tries to reconnect indefinitely. Resolve the problem and MetaASSIST View will reconnect automatically.
- You may have an Ethernet loop. Resolve the problem and re-connect;

- If service traffic passes through the Actelis system, but management traffic does not, then please check that the Management VLAN is configured correctly;
- Management traffic (defined to be forwarded with HIGHEST priority) fails when HSL is congested by service traffic. Check that Ingress Traffic limiting is not enabled on HSL (in ML700 only). To resolve the problem, disable the feature via TL1.
- If both Management and Service traffic do not pass through the Actelis system then probably the Ethernet port setting does not match with network configurations:
  - The ETH-<ID> port MDI pinout is by default MDI and requires an RJ45 connector with straight-through cable;
  - Speed and Duplex mode of ETH-<ID> by default are auto-negotiated. You can connect via Craft port and configure ML device Ethernet port according to your network setting;
  - Connector is damaged. It is recommended to check physical connectivity.

IP connectivity parameters problem

- Incorrect IP address was typed in the "Connect" dialog box. In this case, MetaASSIST View tries to connect to the NE and displays the following tooltip when the cursor is located on the NE: 'Started Connecting...'. Re-connect with correct IP address.
- Invalid IP attributes (i.e., Incorrect or duplicated IP address, incorrect subnet mask or gateway address) configured on ML NE.
  - On directly accessed NE, MetaASSIST View tries to connect to the NE and displays the following tooltip when the cursor is located on the NE: 'Started Connecting...'. Re-connect with correct IP address.
  - On in-directly accessed NE (subtended via HSL NE), MetaASSIST View tries to connect to the NE but fails to connect. In this case, the NE will be displayed in the **NEs linked via HSL** pane. Reconfigure the parameters on the ML NE using this pane and then re-connect via this pane.

Access is not granted by IP Access Control feature

In this case, MetaASSIST View tries to reconnect indefinitely. Resolve the problem and MetaASSIST View will reconnect automatically.

- In this case, you need to add your IP address to the IP Access Control List with the Telnet protocol specified as enabled for connection or connect through the Craft port and disable IP Access Control. IP Access Control feature is enabled on ML device and the IP address of your host (PC/Workstation) is not in the IP Access Control List.

SSH Authentication Failures and Warnings (optional - for secure version only)

- **Private Key file not found.**
  If the Private Key cannot be found in the workstation file system, you will receive the following error message: '*Private Key file cannot be found.*'
- **Public Key of the Management Host not found.**
  If the Public Key of the Network Element cannot be found in the workstation file system, you will receive the following warning message: '*Accept Key <Signature> for Host <IP Address>*.' Click **Yes** to continue with the login and save it for the next login.

- **Public Key of Management Host changed.**
  If the Public Key of the Network Element was found in the workstation file system but it is not the same as the Network Element actual key (was changed), you will receive the following warning message: '*Host Identification has changed. Do you want to replace existing key with: <Signature>*'. Click **Yes** to accept.
- **Authentication Failed, Management Host does not have the ML device Public Key or Passphrase is incorrect.**
  If the Public Key of the MetaASSIST View was not entered into the Network Element, the Passphrase is incorrect, or user did not accept the public key of the Network Element, you will receive the following error message: '*Authentication Failed*'. Ask the system administrator for a new Public Key.
- **3 SSH sessions are already opened.**
  If 3 SSH sessions are already in progress and you try to open a fourth one, you will receive the following error message: '*Authentication Failed*'.

Login problems (common for all interfaces)

MetaASSIST View displays the error message '*Login failed*.' in the following cases:

- **User Account Does Not Exist.**
  In this case, an incorrect User Name was typed in. Click **Close** and type a different user name.
- **Illegal Password was typed.**
  In this case, an incorrect Password was typed in. Click **Close** and type a correct Password. MetaASSIST View can be configured for IP Access Control. See **IP Access Control** (on page 12-21).
- **User account is locked.**
  Administrator can lock user account manually. Also, the system can be configured to provide automatic control on number of failed attempts (configurable) that should cause the user account to be locked automatically. Only the administrator can unlock the user account (locked automatically or manually).

MetaASSIST View displays the error message: "*Currently too many sessions are open on the Actelis system*" in the following case:

- **Too many users.**
  The Actelis system can support up to 20 concurrent management sessions on the Head-end (19 remotely (via LAN) and 1 locally (via craft port) connected management hosts). If more users try to connect, then the error message appears.
- **Auto-discovered Actelis NEs auto-login failed.**
  Attempt of the system to access TL1 agent on linked Actelis NE using the same user/password as on manually connected Actelis NE failed, due to possible difference in user accounts on various Actelis NEs.

Resolving MetaASSIST View / Actelis System Software Problems

Software version problems can be due to partial or fully incompatible SW versions between MetaASSIST View and the Actelis System.

Partially Incompatible MetaASSIST View vs. Actelis System Version: MetaASSIST View notifies the user about partially incompatible MetaASSIST View vs. Actelis System Version (for example unknown version of known product line) with the following notification:

"Unknown S/W version of the Actelis System. Some functionality would be unavailable or may work improperly. An upgrade of MetaASSIST is recommended. Would you like to continue anyway?"

In this case, the user can open the MetaASSIST View application and connect with the Actelis System of an unknown version of a known product line but will have the following notification displayed on all panes:

"Unknown Actelis System S/W. Please upgrade MetaASSIST View."

Fully Incompatible MetaASSIST View vs. Actelis System Version: MetaASSIST View notifies the user about fully incompatible MetaASSIST View vs. Actelis System Version (unknown/unsupported version of unknown/unsupported product line) with the following notification:

"Incompatible S/W version of the Actelis System. An upgrade of MetaASSIST is required."

In this case, the user cannot open MetaASSIST View for Actelis Systems of unknown/unsupported version of unknown/unsupported product line.

Resolving Management Connection Problems

Unsuccessful connections can be due to configuration or login problems as follows:

Configuration Problems

Craft Port Access problems:

- Local Craft port setting (baud rate) specified in MetaASSIST View, configured on ML device and configured on your management host serial port (COM1/COM2) do not match. In this case, MetaASSIST View tries to reconnect indefinitely. It is recommended to check the connection parameters. If local craft connection cannot be established, configure your PC Baud Rate according to ML definitions, change the Baud Rate in the Connect dialog box, and try to re-connect.
- If connection was not established at any of the baud rates this implies that the Craft port was disabled. Try one of the following:
  - On Actelis system, try to use IP access (via COLAN (MGMT) or ETH-<ID>) if IP address was already configured beforehand;
  - Replace the Actelis system with another one (with factory setup).
  - Serial port connector or cable is damaged. It is recommended to check physical connectivity;

Ethernet Port Access problems:

- **Out-of-band management problems**: In all of the following cases, MetaASSIST View tries to reconnect indefinitely. Resolve the problem and MetaASSIST View will reconnect automatically.
- Verify that the ML device COLAN (MGMT) port is enabled (using a craft connection). By factory setup, ML device COLAN (MGMT) is disabled;
- COLAN (MGMT) port settings do not match PC port configurations. This can be due to the following:

  - Cable configuration does not match the attached cable. The COLAN (MGMT) MDI pinout is by default MDIX and requires an RJ45 connector with a crossover cable;
  - Speed and Duplex between the PC and COLAN (MGMT) do not match. By default, the Speed and Duplex mode of the COLAN (MGMT) are auto-negotiated. If your PC or workstation port does not support this feature, then speed and duplex mode should be manually configured on the ML device via Craft;
  - Connector or cable is damaged. It is recommended to check physical connectivity.

- **In-band management problems**:
  In all of the following cases, MetaASSIST View tries to reconnect indefinitely. Resolve the problem and MetaASSIST View will reconnect automatically.
- You may have an Ethernet loop. Resolve the problem and re-connect;
- If service traffic passes through the Actelis system, but management traffic does not, then please check that the Management VLAN is configured correctly;
- Management traffic (defined to be forwarded with HIGHEST priority) fails when HSL is congested by service traffic. Check that Ingress Traffic limiting is not enabled on HSL (in ML700 only). To resolve the problem, disable the feature via TL1.
- If both Management and Service traffic do not pass through the Actelis system then probably the Ethernet port setting does not match with network configurations:
  - The ETH-<ID> port MDI pinout is by default MDI and requires an RJ45 connector with straight-through cable;
  - Speed and Duplex mode of ETH-<ID> by default are auto-negotiated. You can connect via Craft port and configure ML device Ethernet port according to your network setting;
  - Connector is damaged. It is recommended to check physical connectivity.

IP connectivity parameters problem:

- Incorrect IP address was typed in the "Connect" dialog box. In this case, MetaASSIST View tries to connect to the NE and displays the following tooltip when the cursor is located on the NE: 'Started Connecting...'. Re-connect with correct IP address.
- Invalid IP attributes (i.e., Incorrect or duplicated IP address, incorrect subnet mask or gateway address) configured on ML NE.

- On directly accessed NE, MetaASSIST View tries to connect to the NE and displays the following tooltip when the cursor is located on the NE: 'Started Connecting...'. Re-connect with correct IP address.
- On in-directly accessed NE (subtended via HSL NE), MetaASSIST View tries to connect to the NE but fails to connect. In this case, the NE will be displayed in the NEs linked via HSL pane. Reconfigure the parameters on the ML NE using this pane and then re-connect via this pane.

Access is not granted by IP Access Control feature

In this case, MetaASSIST View tries to reconnect indefinitely. Resolve the problem and MetaASSIST View will reconnect automatically.

- In this case, you need to add your IP address to the IP Access Control List with the Telnet protocol specified as enabled for connection or connect through the Craft port and disable IP Access Control. IP Access Control feature is enabled on ML device and the IP address of your host (PC/Workstation) is not in the IP Access Control List.

SSH Authentication Failures and Warnings (optional - for secure version only)

- **Private Key file not found.**
  If the Private Key cannot be found in the workstation file system, you will receive the following error message: 'Private Key file cannot be found'.
- **Public Key of the Management Host not found.**
  If the Public Key of the Network Element cannot be found in the workstation file system, you will receive the following warning message: 'Accept Key <Signature> for Host <IP Address>.' Click Yes to continue with the login and save it for the next login.
- **Public Key of Management Host changed.**
  If the Public Key of the Network Element was found in the workstation file system but it is not the same as the Network Element actual key (was changed), you will receive the following warning message: 'Host Identification has changed. Do you want to replace existing key with: <Signature>'. Click Yes to accept.
- **Authentication Failed, Management Host does not have the ML device Public Key or Passphrase is incorrect.**
  If the Public Key of the MetaASSIST View was not entered into the Network Element, the Passphrase is incorrect, or user did not accept the public key of the Network Element, you will receive the following error message: 'Authentication Failed'. Ask the system administrator for a new Public Key.
- **3 SSH sessions are already opened.**
  If 3 SSH sessions are already in progress and you try to open a fourth one, you will receive the following error message: 'Authentication Failed'.

Login problems (common for all interfaces)

MetaASSIST View displays the error message 'Login failed.' in the following cases:

- **User Account Does Not Exist.**
  In this case, an incorrect User Name was typed in. Click Close and type a different user name.
- **Illegal Password was typed.**
  In this case, an incorrect Password was typed in. Click Close and type a correct Password. MetaASSIST View can be configured for IP Access Control. See IP Access Control.
- **User account is locked.**
  Administrator can lock a user account manually. The system may also be configured to provide automatic control on a number of failed attempts (configurable) that should cause the user account to be locked automatically. Only an administrator can unlock the user account (locked automatically or manually).

MetaASSIST View displays the error message: "Currently too many sessions are open on the Actelis system" in the following case:

- **Too many users.**
  The Actelis system can support up to 20 concurrent management sessions on the Head-end (19 remotely (via LAN) and 1 locally (via CRAFT port) connected management hosts). If more users try to connect, then the error message appears.
- **Auto-discovered Actelis NEs auto-login failed.**
  The system's attempt to access a TL1 agent on a linked Actelis NE using the same user/password as on manually connected Actelis NE failed, due to possible difference in user accounts on various Actelis NEs.

Resolving MetaASSIST View / Actelis System Software Problems

Software version problems can be due to partial or fully incompatible SW versions between MetaASSIST View and the Actelis System.

Partially Incompatible MetaASSIST View vs. Actelis System Version: MetaASSIST View notifies the user about partially incompatible MetaASSIST View vs. Actelis System Version (for example unknown version of known product line) with the following notification:

"Unknown S/W version of the Actelis System. Some functionality would be unavailable or may work improperly. An upgrade of MetaASSIST is recommended. Would you like to continue anyway?"

In this case, the user can open the MetaASSIST View application and connect with the Actelis System of an unknown version of a known product line but will have the following notification displayed on all panes:

"Unknown Actelis System S/W. Please upgrade MetaASSIST View."

Fully Incompatible MetaASSIST View vs. Actelis System Version: MetaASSIST View notifies the user about fully incompatible MetaASSIST View vs. Actelis System Version (unknown/unsupported version of unknown/unsupported product line) with the following notification:

"Incompatible S/W version of the Actelis System. An upgrade of MetaASSIST is required."

In this case, the user cannot open MetaASSIST View for Actelis Systems of unknown/unsupported version of unknown/unsupported product line.

Appendix A - Technical Specifications

This appendix contains the following ML700 specifications:

- General Specifications
- Supported SNMP MIBs
- **Customer Logs** (on page A-6)

ML700 Specifications

Table 95: ML700 Specifications

Interfaces

Ethernet Service

• 10/100Base-TX IEEE 802.3	4 ports, RJ45, Auto-MDIX
• 100/1000Base-Fx (option)	2x 100/1000Base-FX - SFP based, MSA compliant

High Speed Link (Bonded copper Pairs)

• Number of HSL Ports	1
• Protocols	IEEE 802.3ah 10Pass-TS; ITU-T G.998.2 (G.Bond/Ethernet)

• Modem Line code and supported profiles	• ADSL2 (ITU-T G.992.3): Annex A and Annex M
	• ADSL2+ (ITU-T G.992.5): Annex A, B, J and Annex M
	• VDSL2 (ITU-T G.993.2):
	  ○ VDSL2 profiles: 8a, 8b, 8c, 8d, 12a, 12b, 17a
	  ○ Region A (North America): D32, D48, D64 and D128
	  ○ Region B (Europe):
	  • B8_1 (998-M1x-A)
	  • B8_2 (998-M1x-B)
	  • B8_3 (998-M1-NUS0)
	  • B8_4 (998-M2x-A)
	  • B8_5 (998-M2x-M)
	  • B8_6 (998-M2x-B)
	  • B8_7 (998-M2x-NUS0)
	  • B8_8 (998E17-M2x-NUS0)
	  • B8_9 (998E17-M2x-NUS0-M)
	  • B8_10 (998ADE17-M2x-NUS0-M)
	  • B8_11 (998ADE17-M2x-A)
	  • B8_12 (998ADE17-M2x-B)
	  • B8_17 (998ADE17-M2x-M)
	• Vectoring (ITU-T G.993.5) - ML740-R only

• Bandwidth	Downlink - up to 500 Mbps Uplink - up to 250 Mbps
• Number of Copper Pairs	2, 4 or 8 (model dependent)
Connector:	RJ45 (per modem/pair)
• Modem rates	192kbps to 100Mbps (depending on loop and spectral regulations).
• End-to-end Delay	• Fast mode: 2-4ms (typical) • Interleaved: up to 63ms interleaving delay • G.inp (G.998.4 retransmission): depending on settings, configurable up to 63ms retransmission delay
• Impulse Noise Protection	Depending on settings, configurable up to 16 symbols (4ms) in Interleaved mode and >20ms in G.998.4
• Sealing Current Sourcing	48VDC/1.5mA nominal (On/Off settable)
• BER	10E-10 (typical);10E-7 (guaranteed)
• Modem Profiles	According to default/user-defined DMT profiles as stated in BBF TR-165 to comply with ITU-T G.997.1 standards

• Copper Pairs Test Tools	• Graphs for: QLN, SNR, bit loading and TX PSD • Impulse Noise Monitoring (INM) histograms • Performance Monitoring (PM) counters • Modem Status: Rate, Attenuation, Noise Margin

Management (Out-of-Band)

• 10/100Base-TX	1 port (dedicated) - port may be used as service port as well
Connector:	RJ45, Auto-MDIX
• Craft	EIA RS-232 (DCE) port
Connector:	DB9

Ethernet Bridge Features

• Speed/duplex mode	Auto-negotiation or manually 10/100/1000(option) HALF/FULL
• Flow control	IEEE 802.3x (pause frames for FULL/back pressure for HALF DUPLEX modes)
• Link Aggregation	IEEE 802.3ad
• EFM OAM	IEEE 802.3ah clause 57
• Bridging	IEEE 802.1d/p/q
• Min tagged frame size	64 bytes
• Maximum Frame Size	1630 bytes
• Forwarding Database size	8K
• Double Tagging	Q-in-Q , Ethernet Type 0x8100 (configurable)
• VLANs	255 user defined Traffic VLANs + 1 user defined MGMT VLAN, for VIDs in range from 1 to 4094
• Maximum Burst Size	~250 frames for 64-byte length frames; ~60 frames for 1532-byte length frames;
• RSTP, STP	IEEE 802.1d compliant
• Provider Bridge	IEEE 802.1ad compliant
• CFM / MEF OAM	IEEE 802.1ag compliant / Y.1731 compliant
• LLDP	IEEE 802.1ab compliant
• IGMP Snooping	For IGMPv1/v2, RFC4541 - for RFC 1112/2236

Quality of Service Features

• Class of Service (Queues)	8
• Scheduler	WFQ, SP or Hybrid

MEF Services

• MEF Compliancy	MEF9 & MEF14 certified, MEF10 compliant
• EVCs	8
• Classification Rules	32 ingress rules (Port/VLAN/L2/L3/L4 Flexible)
• BW control	32 profiles, each one with CIR, CBS, EIR, EBS configurable
• Ingress policing	Two rates/3 color ingress traffic metering (green (CIR+CBS), Yellow (EIR+EBS), red (exceeds BW profile)
• Scheduler	SP, WFQ or Hybrid, Weights 1:15 configurable
• Egress limiting and shaping	Shaping per service Flow and Egress limiting per HSL port

Management

Management Applications

• EMS	MetaASSIST EMS
• Craft GUI	MetaASSIST View

Protocols

• SNMP	SNMP v1 and v2c
• Command Line Interface	TL1, CLI

• Remote Access	Telnet
• Secure Access (option)	SSH v2
• Time Synchronization	SNTP v3
• Web Access	HTTP
• File Transfer	FTP, TFTP
• Syslog	RFC 3164

Front Panel Indicators (LEDs)

• Power • Status • Alarm	
• MLP	per modem/pair
• ACT (Activity) and LNK (Link)	per Ethernet/HSL port

Alarm Contacts

• Interface Connector	Terminal Block: 2 Input, 1 Output (not supported by ML620i models)
• Alarm Output voltage/current	60VDC/120mA max
• Alarm Input voltage/current	±20VDC/3.5mA max

Physical

• Dimensions	Height: 1.6" / 40mm (1U) Depth: 11.0" / 280mm Width: 8.4" / 213mm
• Weight:	3.75 lbs / 1.7 Kg
• Mounting	Rack: 2 units in 19", 23" or ETSI racks Desktop and Wall Mount

Power

• DC:	-48 to -60 VDC nominal 22 Watt (model dependent)
• AC:	External adapter 90 to 264 VAC, 47-63 Hz 17 to 28 Watt (per model)

Environmental

• Operating Temp.	-40° to +65°C
• Storage Temp.	-40° to +70°C
• Relative humidity	Up to 95%, non-cond.

Certification and Compliancy

• Safety	UL 60950-1, EN 60950-1, CSA C22.2 60950-1, IEC 60950-1
• EMC	FCC Part 15 Class A, ICES-003 Class A ETSI EN 300 386 Class A ETSI ETS 300 132-2
• CE certified	EMC and Safety
• Environmental	GR-63-CORE ETSI ETS 300 019

ML700 Supported SNMP MIBs

The following SNMP MIBs are supported:

- System group [RFC-1213]
- Interface ifTable [RFC-1213/RFC-2863]
- IfInvertedStack MIB [RFC-2864]
- Bridge MIB [RFC-1493] and [RFC-4188]
- Extended Bridge MIB [RFC-4363]
- RSTP MIB [RFC-4318]
- Entity MIB [version 2, RFC-2737] and [RFC-4133]
- Entity State MIB [RFC-4268]
- DOT3-OAM-MIB [RFC 4878]
- RMON MIB [RFC-2021]
- IEEE8021-CFM-MIB(IEEE draft 8)
- Radius Client Authentication MIB [RFC2618 and RFC4668]
- ACTELIS ALARM MIB (proprietary)

Customer Logs

- Customer Logs - 2x1Mbyte:
  - COMMAND (Collect all TL1 commands) - 1 Mbyte
  - AUDIT (Collect all attempts to connect to ML device: HTTP, TL1/telnet, TL1/SSH, SNMP, SNTP, etc.) - 1Mbyte.
- Support Logs (for internal use) - 3x1Mbyte:
  - INSTALL
  - INFO
  - BLACKBOX

Appendix B - Parts List

This appendix summarizes the items which can be ordered from Actelis, including:

SFP Modules

Table 96: SFP Modules

Item	Description	Part Number	CLEI Code
1000Base-LX SMF SFP module	1.25Gbps, Single Mode, 1310nm, 10 km, LC connector, Bail de-latch	506R00002	M3C1HH0BAA
1000Base-SX MMF SFP module	1.25Gbps, Multi Mode, 850nm, 500m, LC connector, Bail de-latch	506R00012	M3C1HG0BAA
100Base-FX MMF SFP module	125 Mbps, Multi Mode, 1310 nm, 2km, LC connector, Bail de-latch option	506R00022	COUIABEGAA
100Base-FX SMF SFP module	125 Mbps, Single Mode, 1310 nm, 15km, LC connector, Bail de-latch	506R00032	COUIABDGAA
1000Base-T SFP module	Rate 1.25Gbps, 100m, RJ45 connector	506R00042	COUIABCGAA
Ethernet over T3 SFP module, 1000Base-TX version 2.0	GFP (G.7041) encapsulation, 44.736 Mbps, Gigabit Ethernet port based MSA compliant SFP, 75Ohm, unbalanced, 275m (900ft), DIN 1.0/2.3 connector. Shipped with two 30 cm (11.8 in) DIN 1.0/2.3-to-BNC cable adaptors	506R00072	N/A
Ethernet over T3 SFP module, 1000Base-TX version 2.5	GFP (G.7041) encapsulation, 44.736 Mbps, Gigabit Ethernet port based MSA compliant SFP, 75Ohm, unbalanced, 275m (900ft), DIN 1.0/2.3 connector. Shipped with two 30 cm (11.8 in) DIN 1.0/2.3-to-BNC cable adaptors	506R61156	N/A
Ethernet over T3 SFP module, 100Base-FX - version 2.0	GFP (G.7041) encapsulation, 44.736 Mbps, Fast Ethernet port based MSA compliant SFP, 75Ohm, unbalanced, 275m (900ft), DIN 1.0/2.3 connector. Shipped with two 30 cm (11.8 in) DIN 1.0/2.3-to-BNC cable adaptors	506R00082	N/A
Add Drop Module 1310nm/1550nm (LADM-1310-1550)	2-wavelength (1310 nm and 1550 nm) CWDM Add and Drop MUX plug-in module, compatible with SP40 chassis	506R51510	N/A
CADM Coarse Add Drop Module, 1610nm (CADM-1610)	1610 nm wavelength CWDM Add and Drop MUX plug-in module, compatible with SP40 chassis	506R51511	N/A
CWDM Mux/Demux - Band2	Coarse Mux/Demux Four Channel Wavelengths Band 2, 1570-1550-1530-1510nm	506R51612	N/A
CADM Coarse Add Drop Module, 1550nm (CADM-1550)	1550 nm wavelength CWDM Add and Drop MUX plug-in module, compatible with SP40 chassis	506R51514	N/A
SFP 1310nm Single mode Transceiver GbE IR 40Km	Broadband Long Reach Optical Transceiver, up to 2.125Gbps bi-directional data link, Single Mode, 1310 nm, 40 km	506R51750	N/A

T3/E3 over Ethernet SFP - 100Base-FX	T3/E3 over Ethernet SFP. Configurable for supporting E3/T3 and a number of encapsulation protocols.	506R61151	N/A
BiDi SM CWDM SFP Transceiver for GE port, 40km, TX=1490nm/Rx=1310nm	Bi-directional Single Mode CWDM SFP Transceiver for GE port, 40km, TX=1490nm/Rx=1310nm Note: requires P/N 506R61169 at the other side	506R61170	N/A
CSFP Transceiver 1610nm, GbE, 80km	CWDM Pluggable SFP Transceiver, 1610nm, up to 1.25 Gb/s bi-directional data links, 80km	506R51711	N/A
CSFP Transceiver, 1550nm GbE, 80km	CWDM Pluggable SFP Transceiver, 1550nm, up to 1.25 Gb/s bi-directional data links, 80km	506R51712	N/A
CSFP Transceiver, 1570nm GbE, 80km	CWDM Pluggable SFP Transceiver, 1570nm, up to 1.25 Gb/s bi-directional data links, 80km	506R51713	N/A
CSFP Transceiver, 1550nm GbE, 80km	CWDM Pluggable SFP Transceiver, 1550nm, up to 1.25 Gb/s bi-directional data links, 80km, LC Connector	506R51714	N/A
CSFP Transceiver, 1530nm GbE, 80km	CWDM Pluggable SFP Transceiver, 1530nm, up to 1.25 Gb/s bi-directional data links, 80km, LC Connector	506R51715	N/A
CSFP Transceiver, 1510nm GbE, 80km	CWDM Pluggable SFP Transceiver, 1510nm, up to 1.25 Gb/s bi-directional data links, 80km	506R51716	N/A
CSFP Transceiver, 1610nm GbE, 120Km	CWDM Pluggable SFP Transceiver, 1610nm, up to 1.25 Gb/s bi-directional data links, 120km	506R61120	N/A
Stackable Chassis, 4 slot, 1RU 19 or 23 (SP40)	4-slot chassis for CWDM MUX plug-in modules	502R60510	N/A

Cables

Table 97: Service, Alarm, Clock cables

Item	Description	Part Number	CLEI Code
CRAFT i/f cable, DB-9 con. both ends	Craft management cable, DB-9 connectors on both sides, 3m/10ft	504R20010	N/A
Eth (crossed), stranded STP 12ft/3.6m, RJ45 both ends	Eth crossed cable, strand. 12ft/3.6m, RJ45 both ends	504R20025	N/A
Eth straight, strand. 12ft/3.6m, RJ45 both ends	Shielded Eth straight cable. 12ft/3.6m, RJ45 both ends. Can be used for DSL connections as well.	504R20030	N/A

Table 98: Power and Grounding Cables

Item	Description	Part Number	CLEI Code
20ft/6m open ended, 48VDC 18AWG, Gnd 14AWG	Power harness for DC power	504R20043	N/A
AC Power cord, Australian type	Australian power cord, 3x 1mm wires, 1.8 meters, BLACK	199A10040	N/A
AC Power cord, Italian type	Italian power cord, 3x 1mm wires, 1.8 meters, BLACK	199A10050	N/A
AC Power cord, Swiss type	Swiss power cord, 3x 1mm wires, 1.8 meters, BLACK	199A10060	N/A
AC Power cord, UK type	UK power cord, 3x 1mm wires, 1.8 meters, BLACK	199A10070	N/A

Table 99: ML700 DSL Cables

Item	Description	Part Number	CLEI Code
12ft/3.6m straight, solid wires, RJ45 both ends	DSL connections; Solid wires enable connection to terminal block. Use as External Clock cable for ML 1500/150.	504R20020	N/A
10ft/3m, 4xRJ45 to open end, solid wires	For connecting ML700 DSL lines to a terminal block	504R20110	N/A
50ft/15m, 4xRJ45 to open end, solid wires	For connecting ML700 DSL lines to a terminal block	504R20130	N/A
100ft/30m, 4xRJ45 to open end, solid wires	For connecting ML700 DSL lines to a terminal block	504R20140	N/A
150ft/50m, 4xRJ45 to open end, solid wires	For connecting ML700 DSL lines to a terminal block	504R20170	N/A
10ft/3m, 8xRJ45 to open end, solid wires	For connecting ML700 DSL lines to a terminal block	504R20120	N/A
50ft/15m, 8xRJ45 to open end, solid wires	For connecting ML700 DSL lines to a terminal block	504R20150	N/A
100ft/30m, 8xRJ45 to open end, solid wires	For connecting ML700 DSL lines to a terminal block	504R20160	N/A

Item	Description	Part Number	CLEI Code
150ft/50m, 8xRJ45 to open end, solid wires	For connecting ML700 DSL lines to a terminal block	504R20180	N/A
1ft/30cm, 4xRJ45/P to 1xRJ45/J, stranded wires	For connecting ML700 DSL lines to a Cat-5 reel	504R20090	N/A

Accessories

Table 100: Kits

Item	Description	Part Number	CLEI Code
Accessories Kit	Accessories Kit for ML700	510K00060	N/A
European AC-DC Adapter	AC-DC Adapter with European cord	506R00006E	N/A
North American AC-DC Adapter	AC-DC Adapter with North American cord	506R00006	N/A
UK AC-DC Adapter	AC-DC Adapter with UK cord	506R00006U	N/A
Sleeve Extension Slide Kit Installation	Sleeve Extension Slide Kit	502R05080	N/A
Rack Mount Kit	Rack Mount Kit	510R21070	COMNH00DRA
Wall Mount Kit	Wall Mount Kit	510R21080	N/A
Wall Mount Kit, Flat faced	Wall Mount Kit, flat faced	510R50955	N/A

Appendix C - Step-by-Step Commissioning Procedures

- **Workflow of commissioning procedures for ML700**

CO Site Installation

Before you begin the commissioning procedure, verify that the *ML system at the CO site* is installed properly according to the instructions in the Installation Guide:

1. System is mounted at the appropriate location (i.e. in the rack mount).
2. Ventilation on the ML device is unobstructed.
3. System is properly grounded.
4. Copper lines are connected to the ML CO device.
5. GPI/GPO dry contacts are connected to Environmental Controls/External Alarms or External Controls.
6. Power connections and relevant issues (AC/DC or DC power, installation of fuses, etc.) are implemented properly.
7. ML unit is powered up, and power on sequence is completed.

This completes the physical installation of the ML device in the Central Office environment.

CO Configuration - for Link Verification

This procedure sets up the ML CO for communication with the ML CPE.

1. Open a local session to the MetaASSIST View (see **Craft Connection to the ML** (on page 2-3)).
2. Verify that there are *no* HWFLT or PROGFLT alarms on the ML700 -O (CO). Any other alarms are not relevant at this point.
3. In the **HSLs pane** (on page 4-20) select the desired HSL, click on **Configure** and set the required configuration.

   For VDSL2 only if installed at the cabinet:

   - Set the Exchange Side Electrical Length (ESEL) for VDSL2 if installed at the cabinet.

   For link with BBA (Broadband accelerator):

   - Set the **Broadband Accelerator Support** to Checked.
4. All MLPs are enabled by default. To prevent alarms on unused MLP the ports should be disabled. To disable the unused MLPs uncheck the MLPs in the **MLPs configuration pane** (on page 4-16).
5. Prior to **calibrating the HSL** (on page 4-21), verify that the defined **Rate,** (on page 6-4) **Spectral** (on page 6-7) and **Quality** (on page 6-23) profiles meet your needs and that the template is configured with the appropriate profiles (on page 6-31). Create new profiles and template if necessary.

   On the **Spectral Profiles** pane you may use **Load DMT SMODEs** for a country of choice. At the end of the process, check available or create new template, using available profiles. For more details see **Modem Profiles Management Model** (on page 6-1).
6. Calibrate the HSL by choosing the appropriate Profile template.

Note: CO modems will not achieve synchronization until CPE installation is complete.

CPE Physical Site Installation

1. The CPE site installation procedure is similar to the CO site installation procedure.
2. If you configured the ML CO device according to *CO Configuration - for Link Verification*, then the copper connectivity can be verified by ensuring the MLP and HSL LEDs will be blinking or steady GREEN, indicating the modems of ML devices on CO and CPE sites are synchronizing (blinking) or synchronized (steady). In case of using auto-mode the MLP LEDs on CPE might not lit. In such case user may need to re-calibrate the HSL from the CO site.
3. Optionally disable all unused MLP ports.
4. This completes the physical installation of the ML device in the Customer Premises / Remote Terminal environment.

ML CO - Service Configuration

Determine the relevant Ethernet traffic topology for your site prior to the Actelis systems configuration, see **L2 Network configuration in various topologies** (on page G-1). All steps should be implemented starting from the most remote ML device, to avoid Management LAN integrity loss during configuration.

1. Configure Ethernet bridge-wide options. If STP is to be used, note the following:

   If enabled at bridge level, STP is also enabled per port. To keep HSL out-of autonomous STP decision to block the port , ensure that STP is disabled on HSL port of CO.
   To separate Customer LAN STP, ensure that STP is disabled on ML NE.

2. Configure Ethernet ports:
   - Ethernet ports are auto-entered and immediately monitored for alarm conditions. Alarms on ETH<ID> show that adjacent equipment is not connected yet or physical interface configuration does not match. Connect Ethernet cables and if required, adjust the configuration. Disable unused Ethernet ports to omit their LOS alarm.

3. Configure VLANs:
   - 5 Traffic VLANs are provided by default. These stack (push additional external VLAN tag to traffic toward HSL and strip this VLAN in opposite, toward Ethernet ports direction) and tunnel Ethernet traffic between each Ethernet port and HSL port.
   - To define or change traffic behavior VLAN should be re-configured according to the required topology.
   - To decide about Service Traffic Topology to use, see **L2 Network configuration in various topologies** (on page G-1).

4. Configure Quality Of Service parameters, applicable per Ethernet port, or Ethernet Virtual Connection (SERVICE flows). For more information refer to **Ethernet Service Configuration** (on page 10-1).

ML CO - Administration Configuration

The following steps enable remote Management Access and the configure security policy. Implement this procedure for all units, starting from the most remote ML device, to avoid Management LAN connectivity loss during configuration.

NOTE: Use a local CRAFT port connection to avoid Management LAN connectivity loss during configuration.

1. Set System ID to provide unique identification of System and its location for managing via TL1 (applied as TID) and SNMP (applied as System Name) interfaces. TL1 and SNMP identification can be applied equally or differently. By factory setup, each ML device Serial Number is reported as TID/System Name.
2. Set Date and Time (manually or enable SNTP) to provide correct timestamp of alarm conditions reported from the Actelis systems.
3. Configure Management LAN connectivity according to installed Ethernet Service traffic topology and use guidelines for MGMT traffic in various topologies, see **L2 Network Configuration in Various Topologies** (on page G-1).
4. Set User Accounts. Enable Password control (complexity, history, failed login, etc.), if required by Provider Management access policy.
5. If required, configure SSH and ACL according to Provider Management access policy.
6. If required, block non-IP access on ML device installed on CO to avoid insecure access to CO NE from remote NEs.

ML CO - Configuration Backup

The following steps complete the configuration by service validation and capturing the backup file of the approved configuration of each ML device involved in the deployment scenario.

1. Verify Ethernet connectivity between all Actelis systems: Ping the IP Address of each ML device. Apply Ping on any IP known in the Customer site if MGMT is not terminated on CPE.
2. Backup the configuration of each ML device, starting from the most remote system. See Configuration Backup and Restore.

Appendix D - Ethernet Service Configuration Step-by-Step

Ethernet services are defined by a range of attributes, some of which are applied at the UNI while others are applied at the EVC or service itself, to provide end-to-end provisioning. This chapter describes how to implement service attributes at the EVC (or service).

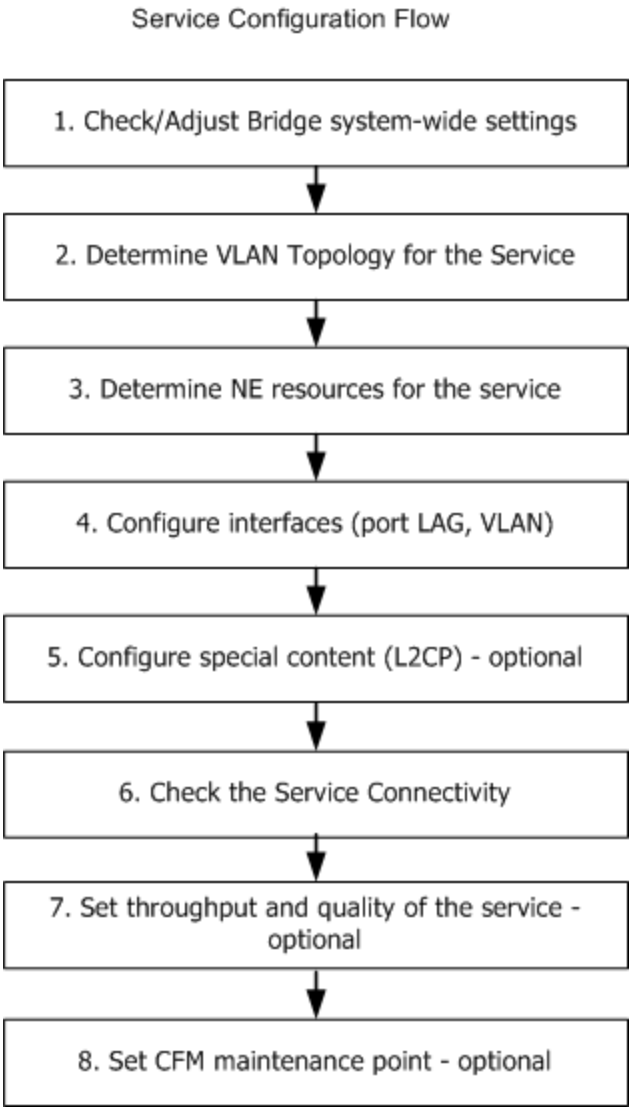
EVC service attributes can be defined by following the step-by-step detailed instructions according to the steps provided in this chapter.

Service Configuration Procedure

This section provides step-by-step instructions on configuring a service on ML700.

The Service Configuration procedure is performed after ensuring that the initial setup has been successfully completed (i.e. performing CO and CPE equipment configuration and control, MLP configuration and HSL calibration), and after ensuring that the management plane (allowing access to the CO and to the particular CPE(s)) has been set.

The service configuration consists of the following steps:



Service Configuration Details

Step 1: Check and Adjust Bridge system-wide settings

- System-wide configurable parameters affect all services at once, so it is crucial to determine these configurations, which are applied system-widely, in advance and before any Ethernet Service is assigned.
- For ML700 bridge system-wide configuration, follow **Ethernet Bridge and STP/RSTP Configuration** (on page 5-1) instructions.

Step 2: Determine VLAN topology for the Service

- To determine the Service Topology, use VLAN schemes as shown in the **VLAN Configuration** (on page 8-1) chapter.
- In order to determine the correct topology, consider the needs of the L2 Priority CoS bits preservation or modifications.
- Assuming that only external VLAN tag is accessible on the CO NE, the topology should be selected to either propagate CoS bits to additional external VLAN tag or to modify the CoS bits according to the classification result on either CO or CPE.
- For ML700 L2 Priority CoS bits control capabilities, refer to L2 Priority CoS bits Re-Marking.

Step 3: Determine NE Resources for the Service

- Allocate the physical interfaces (ports/LAGs) to be assigned for the Service on the CPE and the CO.
- Determine media characteristics of the customer's equipment attached through the UNI (User-Network Interface) to the CPE NE and through the NNI (Network–Network Interface toward WAN/LAN) beyond the CO NE.
  These parameters include: electrical or optical cable type, MDI/MDIX connection to the router/hub or End-Station, interface speed, Auto-negotiation capabilities, LAG needs, LAG load sharing scheme, etc.
- Verify that the OAM, LLCF and STP configuration is compatible with the service provider's Network definitions.

Step 4: Configure Ports, LAGs and VLAN for the Service

After making the above steps' configuration decisions, the CPE and the CO NEs (each NE separately) should now be configured according to the steps listed below.

NOTE: To avoid management connectivity loss with the CPE, it is recommended to first configure the CPE and then the CO.

1. To configure a LAG (if used):
   - Generate the LAG entity first.
   - Enable and add the new LAG to the LAG Ethernet Ports.

- Verify that all of the Ethernet ports which will be assigned to the LAG are adjusted with the same Speed attributes.

  NOTE: the auto-mode cannot be used, and VLANs should not be assigned.

- Configure the VLAN to be applied to the LAGs.

2. To configure the Ports see Ethernet Port Configuration. To configure the LAGs, see **Static Link Aggregation (LAG) Configuration** (on page 4-39).
3. To configure the VLANs see **VLAN Configuration** (on page 8-1)

Step 5: Control special content (L2CP) of the service

- Configure the method in which the system handles L2CP frames (Eliminate / Handle / Tunnel), according to the Customer Service Requirements.
- For more information see **L2CP Processing** (on page 9-1).

Step 6: Check the Service Connectivity

After completing the above steps, the Ethernet Service traffic is configured. At this phase, the Service Connectivity should be verified, and handled if needed, by performing the following tests:

- **Send a Ping** either to the CPE IP or to an IP beyond the CPE (if the customer LAN IPs are known) from the WAN Management host. In addition check Ping to the CO.
  If the ping fails, see **Verifying Service Traffic and Connectivity** (on page 15-16).
- Check the CPE ETH port (which was previously configured to support the service traffic) response to the commands: Suspend and Resume (the traffic should be stopped/resumed). For more information see **Ethernet Service Suspension and Restoration** (on page 15-24).

Step 7: Set Throughput and Quality of the Service

The service throughput and quality should be configured separately on the CPE and on the CO NE.

- Depending on the CPE and CO NE models, throughput control can be applied as follows:
  - Basic (per port, using ingress/egress rate limiting)
  - Advanced (per flexibly identified flow – using rules of EVC services)
- When planning the network service flow, note that the Ethernet service throughput of the ML NEs (any model) is calculated as "Net" traffic; i.e. without the 20 bytes of the Ethernet media overhead (Inter-frame-Gap and Preamble) added to each Ethernet frame, but rather with the L2 frame content only.
- For Configuration instructions see **Quality of Service (QoS)** (on page 7-1), Rate Limit Configuration, and **EVC Configuration** (on page 10-1).

Step 8: Set CFM Maintenance Point

- To complete the service provisioning, a CFM option can be enabled per EVC service flow, controlling end-to-end consistency of Ethernet Service configuration, and providing continuous connectivity check of Service traffic.
- For more information about configuring the CFM Maintenance Point (either MIP or MEP) on CO and CPE NEs, see **Ethernet CFM Configuration** (on page 11-1).

Appendix E - Factory Setup Content

This appendix describes the factory setup for the ML700 models, where the factory setup for each model is described in the appropriate sub-section.

Factory Setup

Table 101: ML700 Units Factory Setup Content

Management

TL1 access	Default User (Admin/Admin, Write/Write, Read/Read) accounts, Local DB of user accounts is in use (not Radius).
Access From Peer (via HSL)	Enabled - relevant to non-IP (Fast OAM) access. Management control via EOC from STU-R to STU-C modem is permanently disabled. Management control via EOC from STU-C to STU-R modem is permanently enabled.
CRAFT	Enabled, with 9,600-baud rate
IP access	IP address = 0.0.0.0, Subnet mask = 255.255.0.0, Gateway = 0.0.0.0.
Radius Client	Disabled , no Radius Server is Configured
LLDP (Link Layer Discovery Protocol)	Disabled system-wide. When enabled, applicable on ETH-x/COLAN ports only.
System identification	Unique TL1 TID and SNMP System ID, initialized by serial number of ML system
SNMP access	Default read access string is set to "public". Default write access string is set to "private". SNMP Traps are on, but Destination Addresses are empty. Trap Source OID is set to MIB-II.
Security	All security features are OFF (ACL, Radius Client, SSH, PWD complexity, failed login control, etc.). Local User Accounts in use (Radius Server is not used).
Log files	All are enabled, Command log Level =2
PM counters	Enabled, PM day start time is 0 (00-00); Thresholds on PM counters are disabled.
Time of Day	No time is set. TOD = Local, Time Zone=0, DST is Off, SNTP Client is Off.
Alarm led	Fully enabled

10Pass-TS bonding

HSL	Enabled
HSL LOWBW alarm threshold	Disabled
MLP	All MLPs are enabled and assigned to HSL-1.
Sealing current	Disabled

Ethernet Port Physical

ETH-x	ETH-{1-4} - enabled. Mode=Auto, Pinout =MDI, Flow control=OFF. ETH-{5-6} (option on some models) disabled (When enabled and only if SFP is entered, Mode=Auto, Flow control=OFF).
COLAN	Disabled. When enabled, Mode=Auto, Pinout =MDIX, Flow control=OFF.
HSL-1	Enabled.
LAG-x	Not entered
Ethernet Ports EFM OAM	EFM OAM is OFF. When enabled (per port) is set to ACTIVE mode

Ethernet Bridge

VLAN awareness	Enabled (by 802.1Q mode)

VLAN Tag type	0x8100
PPPoE tunnel forwarding	Disabled.
FRWDB learning	Enabled
FRWDB aging	Enabled, 300 sec
IGMP Snooping	Bridge Level ON, per VLAN OFF

VLANs

VLANs	Simultaneous support up to 256 VLANs, in range {1-4095}. *NOTE: VID=4093 is permanently reserved (for PPPoE feature), VID=4092 is permanently reserved*
MGMT VLAN	VID= 100 is set for CPU, COLAN (untagged), and all HSL (tagged), even not entered
Service VLAN	VID=101: ETH-1/S + HSL-1/T VID=102: ETH-2/S + HSL-1/T VID=103: ETH-3/S + HSL-1/T VID=104: ETH-4/S + HSL-1/T VID=105: ETH-5/S + HSL-1/T Where S - Stacked, T- Tagged

Ethernet Bridge CoS

Scheduler type	2 SP (Strict Priority) – 6 WFQ (Weighted Fair Queue), 6 queues with weights (configurable): H-8, MH-4, ML-2, L-2, LL-1, LLL-1
WFQ	CLASS weights un-configurable Highest (HH) -8, High (MH)-4, Medium (L)-2, Low (LLL)-1
L2Prio-to-CLASS classification	COS bits {0,1} – Low (LLL), COS bits {2,3} – Medium (L), COS bits {4,5} – High (MH), COS bits {6,7} – Highest (HH).
L3Prio-to-CLASS classification	TOS bits {0-15} – Low, TOS bits {16-31} – Medium, TOS bits {32-47} – High, COS bits {48-63} - Highest.
L2Prio Translation	(HSL ingress applicable) transparent (L2Prio is unchanged)
CLASS-to-L2Prio mapping	(HSL egress applicable) HHH - 7, HH - 6, H - 5, MH - 4, ML - 3, L - 2, LL - 1, LLL - 0

Ethernet Port QoS

Classification	on ETH-x – "by L2PRIO", on COLAN – HH (Enforced)
Ingress rate limiting	OFF on all allowed ports (allowed on ETH-x, HSL, COLAN)
Egress rate limiting	OFF on all allowed ports (allowed only on HSL)
Ingress Limit burst	Not allowed (per bridge configured)

Ethernet Services (BW limiting)

EVCs	not entered
CFM / MEF OAM	Y.1731 compliant
IGMP Snooping for IGMPv1/v2	RFC4541 for RFC 1112/2236

STP

STP system-wide	Disabled. When enabled, protocol type is set to RSTP by default.
Port setting	ON in all ETH ports (ETH-x, COLAN and HSL).

STP path costs defaults set for RSTP	20,000,000 on COLAN/MGMT port 2,000,000 on HSL port
STP path for configured ETH	
If AUTO	ETH-1-4: 2,000,000, ETH-5/6 - 200,000
If 10Mbps	2,000,000
If 100Mbps	200,000
If 1000Mbps	20,000

L2CP

Cisco Reserved MACs:	
01-00-0C-00-00-00 (Cisco ISL), 01-00-0C-CC-CC-CC (Cisco CDP), 01-00-0C-CC-CC-CD (Cisco PVST+)	L2CP disabled -bypass L2CP control
MAC 01-80-C2-00-00-00 (STP)	PEER on all Ports
MAC 01-80-C2-00-00-01 (Pause Frames)	PEER on all Ports
MAC 01-80-C2-00-00-02, subtype=2 (OAM)	PEER on all Ports
MAC 01-80-C2-00-00-02, subtype=3 –10 (UNKNOWN)	DISCARD on all Ports
MAC 01-80-C2-00-00-02, subtype=0 or >11	permanently dropped as illegal
MAC 01-80-C2-00-00-0E (LLDP)	PEER on ETH-x and COLAN Ports, DISCARD on HSL Ports
MAC 01-80-C2-00-00-{03-0F}, 10, {20-21}	DISCARD on all Ports

Rules and Services

Table 102: Services and Rules Factory Setup

Ethernet Services (BW limiting and CLASS of Service)

EVCs	not entered
EVC Services	
SERV-1:	EVC AID= "", DESCR = "INTERNAL HIGH", BWPROFILEID = 0, QUEUE=HHH
SERV-2:	EVC AID= "", DESCR = "INTERNAL LOW", BWPROFILEID = 0, QUEUE=LLL
SERV-3:	EVC AID= "", DESCR = "DEFAULT MGMT", BWPROFILEID = 0, QUEUE=HHH
SERV-4:	EVC AID= "", DESCR = "HIGHEST SERVICE UNLIMITED QUEUE", BWPROFILEID = 0, QUEUE=H //scheduled as WFQ with weight=8
SERV-5:	EVC AID= "", DESCR = "HIGH SERVICE UNLIMITED QUEUE", BWPROFILEID = 0, QUEUE=MH //scheduled as WFQ with weight=4
SERV-6:	EVC AID= "", DESCR = "MEDIUM SERVICE UNLIMITED QUEUE", BWPROFILEID = 0, QUEUE=L//scheduled as WFQ with weight=2
SERV-7:	EVC AID= "", DESCR = "LOW SERVICE UNLIMITED QUEUE", BWPROFILEID = 0, QUEUE=LLL//scheduled as WFQ with weight=1
Identification Rules	
RULE-1: not editable	Default Template, All Values, except MACDST, =ANY, MACDST = 01-80-C2-00-00-00, MASKMACDST=FF-FF-FF-FF-FF-F0, PASSTOMETER=Y, SERV-1, MARKING=NONE, DESCR = L2CP MAC=0x0180C200000*
RULE-2: not editable	Default Template, All Values, except MACDST, =ANY, MACDST = 01-80-C2-00-00-10, PASSTOMETER=Y, SERV-1, ORDERNUM=-1, MARKING=NONE, DESCR= " L2CP MAC=0x0180C2000010".
RULE-3: not editable	Default Template, All Values, except MACDST, =ANY, MACDST = 01-80-C2-00-20,MASKMACDST=FF-FF-FF-FF-FF-FE, PASSTOMETER=Y, SERV-1, MARKING=NONE, DESCR= "L2CP MAC=0x0180C20020/1".
RULE-4: not editable	Default Template, All Values, except MACDST, =ANY, MACDST =01-00-0c-00-00-00, MASKMACDST=FF-FF-FF-FF-FF-FF, PASSTOMETER=Y, SERV-1, MARKING=NONE, DESCR="ISL MAC=0x01000C000000".
RULE-5: not editable	Default Template, All Values, except MACDST, =ANY, MACDST =01-00-0c-cc-cc-cc/D, MASKMACDST=FF-FF-FF-FF-FF-FE, PASSTOMETER=Y, SERV-1, MARKING=NONE, DESCR= "CDP/PVST+ MAC=0x01000 CC-CC-CC-C/Dl".
RULE-6: not editable	Default Template, All Values, except MACDST, =ANY, MACDST = 01-80-C2-00-00-30, MASKMACDST=FF-FF-FF-FF-FF-F0, PASSTOMETER=Y, SERV-1, MARKING=NONE, DESCR= "CFM MAC=0x0180C200003*".
RULE-7:	Default Template, All Values, except VID, =ANY, EXTTAGVID = 100 (MGMTVID), PASSTOMETER=Y,SERV-3, MARKING=NONE, DESCR= "MGMT VLAN".

RULE-8:	Default Template, All Values except EXTTAGTYPE and EXTTAGCOS, =ANY, EXTTAGTYPE =8100,EXTTAGCOS = 0, EXTTAGCOSMASK = 110, PASSTOMETER=Y, SERV-7, MARKING=CLASS-TO-COS,DESCR= "L2PRIO COS ={0-1}".
RULE-9:	Default Template, All Values except EXTTAGTYPE and EXTTAGCOS, =ANY, EXTTAGTYPE =8100,EXTTAGCOS = 2, EXTTAGCOSMASK = 110, PASSTOMETER=Y, SERV-6, MARKING= CLASS-TO-COS,DESCR= " L2PRIO COS={2-3}".
RULE-10:	Default Template, All Values except EXTTAGTYPE and EXTTAGCOS, =ANY, EXTTAGTYPE =8100,EXTTAGCOS = 4, EXTTAGCOSMASK = 110, PASSTOMETER=Y, SERV-5, MARKING= CLASS-TO-COS,DESCR= " L2PRIO COS={4-5}".
RULE-11:	Default Template, All Values except EXTTAGTYPE and EXTTAGCOS, =ANY, EXTTAGTYPE =8100,EXTTAGCOS = 6, EXTTAGCOSMASK = 110, PASSTOMETER=Y, SERV-4, MARKING= CLASS-TO-COS,DESCR= " L2PRIO COS={6-7}".
RULE-32: not editable	Default Template, All Values =ANY, PASSTOMETER=Y, SERV-2, MARKING=NONE, DESCR= " ALL THE REST traffic tunnel".

BW Profiles

BWPROFILE-0	Description="UNLIMITED TRAFFIC
BWPROFILE-1	CIR=200 kbps, CBS=99999 bytes , EIR=0, EBS=0, Description="200kbps LIMIT for MGMT TRAFFIC"

Appendix F - Alarms Troubleshooting

The troubleshooting procedures are described in the following tables. They include troubleshooting:

NOTE: The severity of a condition type is user configurable. The severity of each condition type, mentioned in the following troubleshooting tables, is according to factory setup.

System Alarms Troubleshooting

*Table 103: **System** troubleshooting table*

Condition Type	Description	Recommended Troubleshooting Procedure
NOSETUP	No initial setup; System is in Factory setup..	Configure the system. The alarm is cleared immediately after the first configuration command. If you have a backup file of the configuration, reload the setup. See **Reverting to Backup Software** (on page 14-18). If the alarm is not cleared or reappears later on even if the system is configured, then this is probably due to a faulty unit. Replace the ML device unit.
UPGRDIP	Software Upgrade in Progress; The alarm is raised when download of the new SW is initiated.	Commit SW operation should be provided to clear the alarm. Commit SW operation is enabled regardless of new SW status. It is recommended to Activate new SW and ensure that Service is OK before Committing the new SW. Refer to **Updating the System Software** (on page 14-13) for details.

Equipment Alarms Troubleshooting

Table 104: Equipment alarms troubleshooting table

Condition Type	Description	Recommended Troubleshooting Procedure
HWFLT AID ML700	Hardware fault; Indicates a card failure..	Replace unit.
PROGFLT AID ML700	Program store failure; Software release in the ML device is corrupted and cannot be automatically repaired. On nearest reboot the system may not respond.	The corrupted file must be replaced as soon as possible (downloaded from a server) as follows: View the software revision of the unit. In the Network Element tree, click **System Administration, SW Release**. Download the correct software version. In the SW Release pane, perform all the Software Update procedures. If problem is not resolved, replace ML700.
UEQ AID SFP	Unequipped module; The SFP module is configured but not present in its socket. Alarm is reported as Not Service Affecting (NSA) and Minor when Ethernet port associated with the SFP module is not part of any VLAN or this Ethernet port is either not enabled or removed from Service intentionally. Otherwise Alarm is reported as Service Affecting (SA) and Major.	Make sure specified module is installed properly. If necessary, replace the module.
HWFLT AID = SFP	SFP hardware failure; Indicates that plugged-in SFP module is unreadable (either MSA non-compliant or faulty SFP module). Alarm is reported as Not Service Affecting (NSA) and Minor when Ethernet port associated with the SFP module is not part of any VLAN or this Ethernet port is either not enabled or removed from Service intentionally.	Perform one of the following: Replace SFP module. If problem is not resolved, replace ML700.

Condition Type	Description	Recommended Troubleshooting Procedure
UNKNOWN AID = SFP	SFP module of Unsupported SFP interface type is inserted (for supported types, see **Pluggable Equipment Control** (on page 4-8)). In this case service is blocked. Not listed in the Parts List SFP module, which is also non-compliant to Multiple Source Agreement (MSA), is inserted. Service is not blocked. Alarm is reported as Not Service Affecting (NSA) and Minor when Ethernet port associated with the SFP module is not part of any VLAN or this Ethernet port is either not enabled or removed from Service intentionally. Otherwise Alarm is reported as Service Affecting (SA) and Major (can be changed).	If non-compliant to MSA SFP is in use, set the alarm to NA, see Modifying Alarm Severity. For Unsupported SFP type, replace with an appropriate SFP type module.
EQPTMIS AID = SFP	SFP module of inserted does not match the manual configuration of ETH-5/6 MODE (see Configuring Ethernet Ports)	Check the ETH-5/6 port configuration and either replace the SFP module to match it or reconfigure ETH-5/6 port.
DDMALERT AID = SFP	Digital Diagnostic Memory Alert. The SFP module reports about one of 10 possible environmental or hardware problems. Alarm is reported as NSA (Not service Affecting), with Minor default (unless severity is modified) if the Ethernet port associated with the SFP module: Is not part of any VLAN or is not enabled or removed from Service intentionally. Otherwise the alarm is reported SA (Service Affecting), with Major default (can be changed) severity	Replace SFP if its parameters degraded due to MTBF (low laser BIAS, etc.) or check environment to change (high temperature).

Modem Ports Alarms Troubleshooting

Table 105: Modem Ports alarms troubleshooting table

Condition Type	Description	Recommended Troubleshooting Procedure
HIATTN	High loop attenuation; Current loop attenuation on MLP is equal or exceeds a threshold value configured for this MLP. Alarm condition is cleared when loop attenuation drops below the threshold value by at least 1dB.	The condition is used as a system performance analysis tool. Loop attenuation is a product of SNR margin and BER. The HSL automatically maintains control on SNR Margin in order to provide sufficient BER level in the copper loop. To eliminate the condition, reconfigure the condition threshold. Do not re-calibrate the HSL, since HIATTN is not a fault condition.
LOSW	Loss of Synchronization Word; The MLP has lost synchronization. This condition is MJ, SA if modem belong to the HSL with LOWBW Threshold Control enabled and crossed. The condition is applicable on HSL in -O (Office) mode only. In all other cases this condition is MN, NSA.	This problem is typically caused by temporary disturbances, such as micro-interruptions or transient noise. To determine whether problem is temporary or persistent, perform the following: In **Modem Ports** pane, click **Details (All Modems)** button. **Details For Modem Ports** pane opens. Check the details for the specified MLP for the system. If the problem persists, try the following procedures in the suggested order: Follow the instructions in Analyzing Results of the Line Qualification Routines to eliminate a modem mismatch as a possible cause. Check the copper pairs (lines). Repair/replace lines, as necessary; check out RJ45 connectors. ⚠ When replacing pairs, be careful **not** to disconnect adjacent pairs.
LOWSNRM	Low SNR margin; Current SNR margin on MLP is equal or less than a threshold value configured for this MLP. Alarm condition is cleared when SNR margin returns to +1 dB above the threshold value.	The condition is used as a system performance analysis tool. The HSL automatically maintains control on SNR Margin in order to provide sufficient BER level in the copper loop. To eliminate the condition, reconfigure the condition threshold. Do not re-calibrate the HSL, since LOWSNRM is not a fault condition.

Condition Type	Description	Recommended Troubleshooting Procedure
QUALFLT	Qualification fault; Modem failed qualification during calibration due to insufficient transmission rate, noise margin or excessive cross-talk.	This condition is most likely caused by cut or bad lines. In case of enhanced calibration (1:4 ratio), this alarm indicates that this modem is removed during the HSL calibration process because the modem either: Limits the upper rates on other MLP(s) OR Failed / Low Rate compared to other MLP(s). Perform the following procedures in the suggested order: Analyze the qualification test routine results. Use the procedures to check the copper pairs (lines) for the MLPs specified by the QUALFLT alarm. Repair/replace lines, as necessary; check out RJ45 connectors. ⚠ When replacing pairs, be careful **not** to disconnect adjacent pairs. De-calibrate (Cancel Calibration) the HSL where MLPs belong. In **Modem Ports** pane, click **Details (All Modems)** button and determine MLPs are synchronized at minimum rate. In **High Speed Link** pane, click **Calibrate** to calibrate the HSL (allow a few minutes for downtime). Ensure that there are no QUALFLT modems. If you are sure about line quality, and QUALFLT still exists, replace the unit.
QUARANTINE	Applicable on ML700-O model MLP-AID only . Modem with errors during several seconds is quarantined to prevent the errors from the HSL. Modem is restored to normal operation automatically after one minute free of errors. Alarm is raised as SA (service affecting), if HSL is calibrated and at least one of LOWBWUS or LOWBWDS thresholds was crossed, otherwise alarm shall be raised as NSA (non service affecting). Alarm severity defaults: MN (minor) for NSA and MJ (major) for SA condition	This condition is most likely caused by bad/cut lines, faulty ML device and/or mis-configured ML. Check the copper pairs connection. If problem is not resolved, check if ML device linked by HSL is powered up, correctly installed (copper loop connections), not alarmed and MLP and HSL are configured properly; If problem is not resolved, replace linked ML device.

Condition Type	Description	Recommended Troubleshooting Procedure
BADRATIO	Applicable on ML700-O model MLP-AID (or on ML600 MLP-AID assigned to HSL in –O mode (Office)) . Alarm is raised on modems which are excluded from HSL operation, as cannot be kept due to slower versus other modems rate in ratio above then 1:4 EFM-bond ratio allowed. Alarm is raised as SA (service affecting), if HSL is calibrated and at least one of LOWBWUS or LOWBWDS thresholds was crossed, otherwise alarm is raised as NSA (non service affecting). Alarm severity defaults : MN (minor) for NSA and MJ (major) for SA condition.	ML CO , when rate ratio between modems assigned to HSL rates is above 1:4, will stop use of slow rate modems and will keep operational only highest rate modem(s), calculating best cumulative BW achievable (it may happen that 1 modem will stay , while 7 other will be suspended). If more robust behaviour (more modems involved) is required, modems can be limited by MAXRATE specified via RATEPROFILE used in DMTTEMPLATE of calibration.

HSL Alarms Troubleshooting

Table 106: HSL alarms troubleshooting table

Condition Type	Description	Recommended Troubleshooting Procedure
COPPERMIS	Copper mismatch connection; There is no Ethernet service and in-band management traffic. Applicable on HSL configured in -O (Office) mode.	The ML device with HSL in -O (Office) mode can detect and report that this HSL is terminated on multiple -R (Customer) destinations. The table in the **Modem Ports** pane provides unique identification (Serial Number) of each copper line termination. The table column - "Linked NE" provides Serial Number (s) of the discovered linked by HSL ML device system(s). To resolve the problem: Re-connect each copper line with different Serial Number discovered on distant end. MLP provides Serial Number discovery immediately after synchronization. To work around the problem: Reconfigure HSL on local side to exclude incorrectly terminated copper lines from HSL. De-calibrate (Cancel Calibration) the HSL; then delete MLPs from HSL, re-calibrate HSL once more.
HSLDIAG	High Speed Link is Up, but not calibrated yet. Up, not calibrated status can appear when the system is powered for the first time or when you click the **Cancel Calibration** button in HSL pane. Applicable on HSL configured in -O (Office) mode.	In **High Speed Link** pane, click the **Calibrate** button to calibrate the HSL (allow a few minutes to complete the process).
HSLDWN	HSL is down; Temporary alarm resulting from HSL initialization or recovery process (secondary state is HUNT, CALIB or RCVRY). Applicable on HSL configured in -O (Office) mode.	There is a temporary alarm. Verify in the **HSL** pane, Details section, that after a few minutes the HSL status is changed to one of the following: UP with the appropriate alarm or no alarms; HSLDIAG with the appropriate alarm; HSLFLT with the appropriate alarm. If problem is not resolved, check if linked by HSL ML device is powered up, correctly installed (copper loop connections), not alarmed and MLP and HSL are configured properly.

Condition Type	Description	Recommended Troubleshooting Procedure
HSLFLT	HSL is faulty; High Speed Link has failed and cannot be recovered automatically due to one of the following: The copper pairs are disconnected; Linked by HSL Actelis system is faulty. Applicable on HSL configured in -O (Office) mode.	Check the copper pairs connection. See the table for possible causes; If problem is not resolved, check if linked by HSL ML device is powered up, correctly installed (copper loop connections), not alarmed and MLP and HSL are configured properly; If problem is not resolved, replace linked ML device.
LOWBWDS/ LOWBWUS	Configured HSL BW Threshold is crossed, for US and DS separately. By factory default, HSL BW threshold is disabled. Applicable on HSL configured in -O (Office) mode.	To avoid LOWBWDS/US alarm: Disable Threshold control or reduce Threshold value in accordance with available HSL BW. To resolve insufficient available HSL BW, troubleshoot Modem Ports (repair/replace/add) and then re-calibrate HSL.
NOTRFC	Applicable on ML700-O model HSL-AID only. No Traffic; Alarm raised if there are some quarantined modems and all Non-quarantined modems have failed. NOTRFC is raised unconditionally SA (service affecting), by default NA.	Differently from HSLFLT which require technician involvement in copper lines/equipment repairing, NOTRFC alarm indicates temporary operational state, which most likely will be automatically resolved (quarantined modem will be automatically released for HSL operation).

Ethernet Port Alarms Troubleshooting

Table 107: Ethernet Ports Alarms Troubleshooting table

Condition Type	Description	Recommended Troubleshooting Procedure
LOS	Loss of Signal on the Ethernet Port. AID = ETH-<ID> or COLAN (MGMT). The Ethernet cable is unplugged or faulty or the Ethernet port on the remote equipment connected to the Service port is mis-configured or down. The alarm is MJ and SA if port is being used by traffic VLAN (always provided in 802.1d Bridge mode). If port is not used by traffic VLAN, the alarm is MN and NSA. Alarm will be masked if there is an existing Equipment alarm.	Use MetaASSIST View and do one of the following: From **Ethernet Ports** pane, select the Ethernet port and then click the **Configure** button. Verify that the port configuration matches the adjacent network equipment. If the port is unused/disconnected, disable it. Check cable connection to the Ethernet port, replace cable if required. Check the peer equipment (equipment linked by Ethernet), make sure the Ethernet port is enabled and configured to match Service port configuration.
RFI	Remote Fault Indication. AID = ETH. Remote Fault Indication is monitored and reported on optical interfaces only, if EFM OAM feature is enabled on a port. Unidirectional RX link failure is reported back on unidirectional TX link by "link failure" bit in EFM OAM PDU format. The alarm is Non Alarmed by factory setup, but can be configured to be reported with any severity. Alarm will be reported as SA if port participates in at least one VLAN, otherwise alarm will be reported as NSA.	Replace cable
INTRUDER	Raised immediately upon CPU detection of intruder condition (new unknown unicast not matching allowed MACs listed in FILTER table), informing about non-allowed traffic arrival, and possibility of traffic blocking through the port. Alarm will be unconditionally **MJ/SA**, cleared by **LOS** alarm. AID = ETH-<ID> or COLAN (MGMT).	To restore the port normal work, either restart the ML700 NE, or perform the following steps: Reset the port (either plug/unplug the cable *or* perform any of the following remote operations: **Reset Port, Suspend/Resume Port, Delete/Enter Port**) Restart the MAC Filtering mechanism: Click **Delete All View Dynamic Addresses** pane (accessed via the **Ethernet Bridge** pane).

MEP Alarm Troubleshooting

Table 108: Ethernet Ports Alarms Troubleshooting table

Condition Type	Description	Recommended Troubleshooting Procedure
RDI	RDI alarm , raised on MEP AID indicates that the last CCM received by this MEP from some remote MEP contained the RDI bit. AID = MEP Remote Defect Indication (RDI) bit informs that the MEP originating this indication doesn't receive CCM messages from at least one of the MEPs in the same MA (MEG). The absence of RDI in a CCM indicates that the transmitting MEP is receiving CCMs from all configured MEPs.	Use CFM loopback toward each MEP in MA/MEG to discover the problematic MEP. In some cases (i.e. Network load or NE load of the CCM messages originator/terminator), RDI is an indication of awkward CFM configuration (i.e. too heavy traffic is generated at end point, or CFM traffic is congested with Service traffic in network). For this case, increase CCM interval (up to 10 min) or increase CCM Priority (up to 7). This may help resolve the problem.

Condition Type	Description	Recommended Troubleshooting Procedure
SIGFLT	One of the problem defined in ITU-T Y.1731 detected and reported as Signaling fault on MEP (Maintenance End Point) AID. AID=MEP. SIGFLT supported in both Y.1731 and CFM modes of work. All possible defects (known in SNMP as: errmac, rmepccm, errccm, xconccm) , except RDI defect ,are reported as SIGFLT alarm	SIGFLT alarm is provided with additional information on a specific reason. The Boolean parameters ERRMAC, RMEPCCM, ERRCCM, XCONCCM, when set to Y (yes), indicate the following problems:
		ERRMAC: The last CCM received by this MEP from some remote MEP indicated that the transmitting MEP's associated MAC is reporting an error status via the Port Status TLV or Interface Status TLV. **Recommendation:** Access the NE where the remote MEP is set. Check the remote MEP's NE HW status; check HW problems with PHY or MAC component of the port on the remote NE switch. If no HW problems found, check the state of the remote MEP (i.e. local MEP on the remote NE) reported and the connectivity to the local MEP (i.e. remote MEP on the remote NE).
		RMEPCCM: This MEP is not receiving CCMs from some other MEP in its configured list. **Recommendation:** If changes in the network occurred (e.g. a MEP was deleted in MA), use Init MEP button on ML MEP pane to re-discover the new list of remote MEPs. If no changes in the network, check each remote MEP locally on it's NE (if they also have this Boolean set to Yes - the problem is bi-directional). Otherwise, if the problem is in a single direction, check all paths to the remote MEP.·
		ERRCCM: This MEP is receiving invalid CCMs or, in Y.1731 mode, ERRCCM is used to indicate UNEXPPERIOD defect , i.e. CCM is received with different then configured on the MEP interval (MA/MEG assumption is that all MEPs originate CCM using the same interval of time, 1sec by default) **Recommendation:** Check remote MEP CCM interval configuration or ensure CCM PDU interoperability between 2 NE, if possible customize CCM PDU format (for example SEQNUM=N) on one NE to match with another NE accepted format.
		XCONCCM: This MEP is receiving CCMs that could be from some other MA or, in Y.1731 mode, XCONCCM is used to indicate MISMRG or MEGLVL defects. **Recommendation:** Change configuration of MEG level, name, MEP(s) ID or Primary VLAN.
		UNEXPMEP: This MEP is receiving messages from unexpected (not-registered) remote MEP found in MEG . **Recommendation**: Add newly discovered MEP as an RMEP to the alarmed MEP or delete discovered MEP on its own location.
		General Note: Not all MEGLVL mismatches can be detected – this is due to CFM limitations on ML500/600/700 devices : "CFM Traffic of a layer lower than the lowest CFM Domain defined on NE is not dropped (as required by the standard) but behaves as a regular service traffic (dropped or passed as is or passed with VLAN encapsulation) depending on Port VLAN membership where CFM traffic appears. All indications above are Boolean and do not point to the specific RMEP but indicates the specific type of problem only.

Condition Type	Description	Recommended Troubleshooting Procedure
CFLT	Alarm was obsolete in R7.12. Connectivity Failure problem is detected and reported on MEP (Maintenance End Point) AID.Alarm indicates one of the any possible defects (known in SNMP as: rdi, errmac, rmepccm, errccm, xconccm). **AID=MEP**	

Appendix G - VLAN Topologies

Actelis equipment allows building various Ethernet topologies in Service and Management Traffic planes.

Prior to Ethernet topology planning verify and perform the following:

- Verify that there are no loops in the Ethernet Topology - use Spanning Tree Protocol if there are redundant connections;
- Check MFS (Maximum Frame Size) size of frames - each new S-VLAN tag adds to the frame an additional 4 bytes. Calculate the largest expected MFS size and check that it is acceptable in the whole Network;
- Ethernet Type of S-VLAN tag (default 0x8100 Q-n-Q Cisco) can be changed, but should be acceptable on each Hop device;
- Separate Customer and Provider Bridges Control planes - configure rules of L2CP.

This chapter provides examples of useful Ethernet topologies, with a description on how to configure Actelis NEs to achieve each of them.

The desired topology should be carefully planned prior to configuration, preventing Management LAN connectivity lost.

How to avoid L2 connectivity loss during Ethernet topology configuration:

- Plan or select one of proposed topologies prior to configuration;
- Remember that the Management traffic plane may be affected by the Service traffic plane you selected;
- Start from the most remote NE (from the Management Host);
- Start with the Management plane, not the Traffic plane configuration;
- If integrity is lost, restore connection using Non-IP access to Linked by HSL NEs. The channel works from the CO to CPE direction only and allows restoring the Management LAN integrity.

NOTE: All Actelis NEs may perform as VLAN-aware (Q-bridge) or VLAN-unaware (D-bridge) Ethernet Switches. Installations, which use different bridge modes (Q and D) on various NEs, are possible but are not described in the examples below, and should be carefully planned by the Providers' Ethernet Network Engineer.

Symmetric Topologies

In symmetric topologies, traffic beyond the ML edge devices (CO and CPE) is forwarded unchanged. The symmetric topology matches with P2P installation needs, where ML NE is used as a media converter only or where Customer and Provider site L2 plane is flatly merged.

The following configurations of the ML link work for symmetric topologies:

- HUB;
- TUNNELS;
  - Transparent for ANY Customer traffic;
  - Transparent for Untagged Customer traffic;
  - Transparent for Specified Tagged Customer traffic (CE-VID filtering);

HUB configuration is applicable in any deployment, providing VLAN-unaware (802.1D) behavior on each NE. Management traffic in this configuration can be either VLAN-tagged or VLAN-untagged, as desired.

TUNNELS configuration, which is suitable for P2P deployments, providing transparent (frames are unchanged beyond the ML systems) and separate (each port is protected from other ports by an internally applied VLAN) tunnels through the ML between the 10/100/100BT/FX Port connected to the PAF-2BaseTL Port. Management traffic in this configuration can be either VLAN-tagged or VLAN-untagged, as desired. There are 2 different configurations that can achieve Transparent behavior of service traffic, one allowing in-band and out-of-band management (with some limitations regarding Service Traffic), another allowing out-of-band management only (without limitations on Service Traffic).

Traffic Tunnels w/o VLAN Filtering

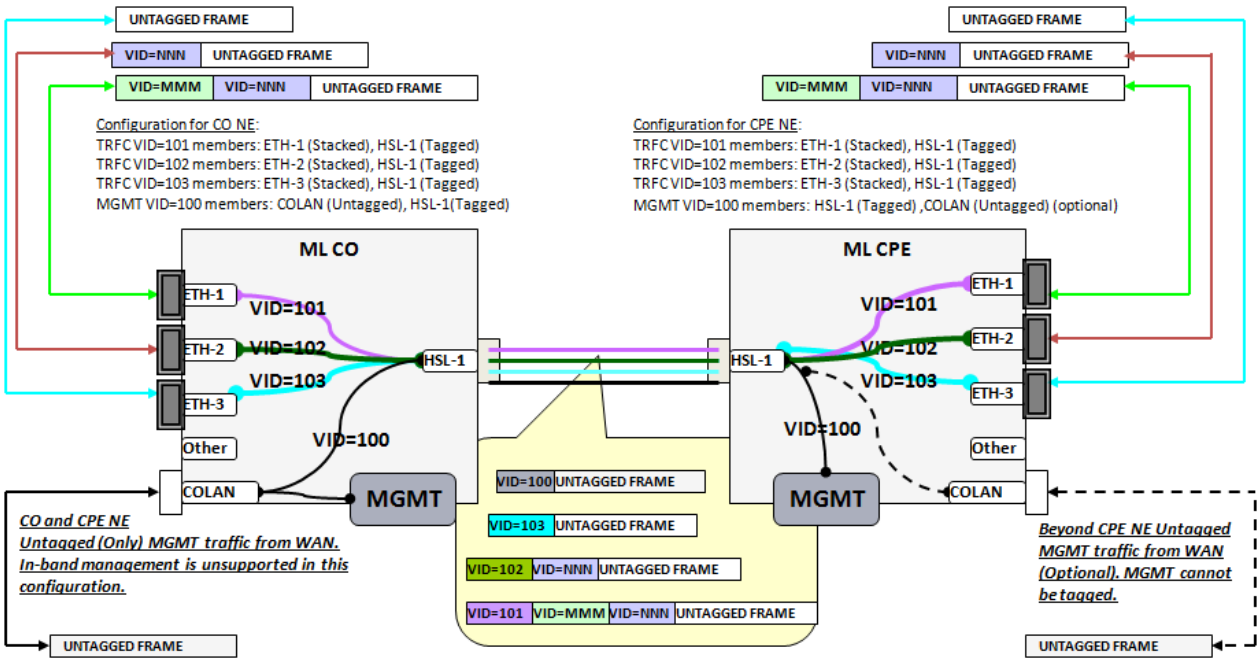


Figure 20: Tunnels for any type of Customer Traffic, without Out-of-Band Untagged MGMT traffic

Table 109: Configuration summary for "Tunnels for Any service traffic type:

CO NE	CPE NE
ETH-x [Stacked] for TRFC VID	ETH-x [Stacked] for TRFC VID
HSL-1 [Tagged] for TRFC VID and [Tagged] for MGMT VID	HSL-1 [Tagged] for TRFC VID and [Tagged] for MGMT VID
COLAN [Untagged] for MGMT VID	COLAN [Untagged] for MGMT VID (optional).

Traffic Tunnels with and w/o VLANs Filtering

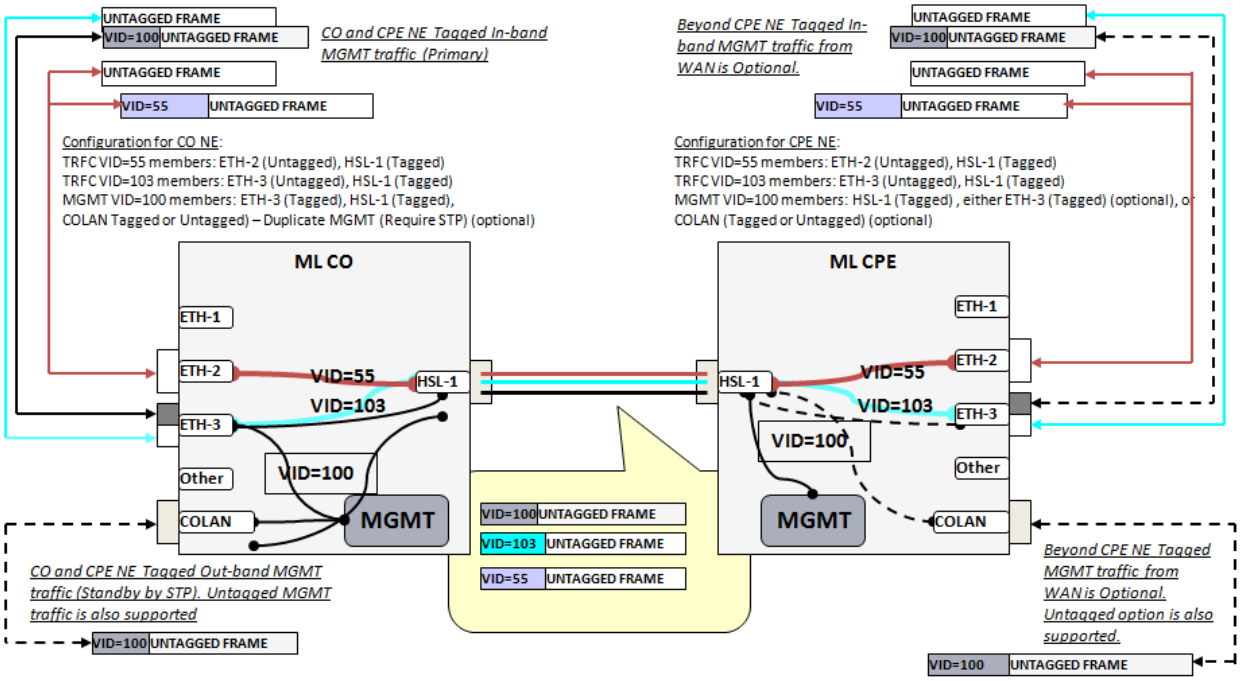


Figure 21: Tunnels for Untagged or Tagged with VID=PVID Customer Traffic, with In-band Tagged MGMT Traffic

Table 110: Configuration summary for "Tunnels for Untagged/Tagged with VID=PVID service traffic type":

CO NE	CPE NE
ETH-x [Untagged] for TRFC VID and [Tagged] for MGMT VID	ETH-x [Untagged] for TRFC VID and [Tagged] for MGMT VID (optional)
HSL-1 [Tagged] for TRFC VID and [Tagged] for MGMT VID	HSL-1 [Tagged] for TRFC VID and [Tagged] for MGMT VID
COLAN [Tagged or Untagged] for MGMT VID (require STP)	COLAN [Tagged or Untagged] for MGMT VID (optional) (require STP)

Traffic Tunnels with VLAN Filtering

This configuration, applicable in any deployment, uses the same encapsulation level (VLAN tag) for switching in Customer LAN and Provider WAN and between them. Management traffic in this configuration can be either VLAN-tagged or VLAN-untagged, as desired. In-band management traffic beyond the CO and the CPE is also available.

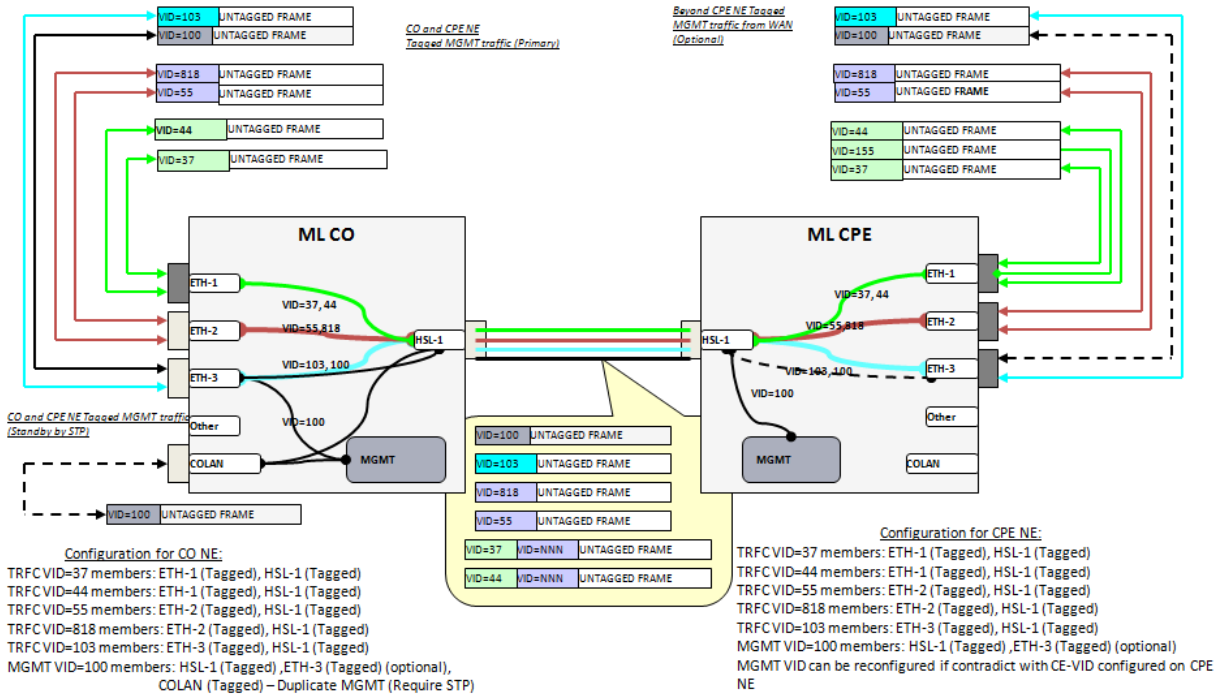


Figure 22: Tagged Customer Traffic filtering, with in-band or out-of-band Tagged MGMT Traffic available.

Table 111: Configuration summary for "CE-VID no filtering, without preserving"

CO NE	CPE NE
ETH-x [Tagged] for TRFC VID and [Tagged] for MGMT VID.	ETH-x [Tagged] for TRFC VID and [Tagged] for MGMT VID (optional).
HSL [Tagged] for TRFC VID and [Tagged] for MGMT VID.	HSL-1 [Tagged] for TRFC VID and [Tagged] for MGMT VID.
COLAN [Tagged or Untagged] for MGMT VID (optional, require STP).	COLAN [Tagged or Untagged] for MGMT VID (optional).

Asymmetric Topologies

In asymmetric topologies ML NEs change the traffic, allowing inter-connect Customer and Provider side L2 planes using VLAN stacking (adding SE-VLAN(s) in Provider direction and stripping the SE-VLAN(s) in Customer direction).

The following configurations of ML link work for asymmetric topologies:

- Stacked on CPE (per-CPE-port), no CE-VID filtering;
- Stacked on CO (per-CPE), CE-VID filtering is possible;
- Stacked on both CPE (per-CPE-port) and CO (per-CPE), no CE-VID filtering.

Stacked on CPE (per-CPE-port), no CE-VID filtering

This configuration applicable in any deployment, encapsulates all customers' frames (tagged and untagged, without filtering of CE-VID) using an additional SE-VID tag. This configuration also allows multiple SE-VIDs per CPE (one per port), supporting multiple customers per CPE. In addition, allows intra-switching between CPEs, using switching between HSL ports (belonging to the same SE-VID) on CO NE. Management traffic in this configuration can be either VLAN-tagged or VLAN-untagged, as desired. In-band management traffic beyond the CPE is unsupported in this case.

Stacked on CO (per-CPE), CE-VID filtering is possible

This configuration applicable in any deployment, allows filtering of CE-VID on CPE and on CO encapsulates all permitted customer frames by additional SE-VID tag (one per each CPE). This configuration also allows intra-switching between CPEs, using switching between HSL ports (belonging to the same SE-VID) on CO NE. Management traffic in this configuration can be either VLAN-tagged or VLAN-untagged, as desired. In-band management traffic beyond the CPE is also available. This configuration allows Management VID re-mapping (applicable in case when MGMT VID contradict with CE-VID on CPE).

NOTE: Switch from CPE stacking topology to CPE filtering topology requires to delete all current Traffic VLANs and create new Traffic VLANs instead.

Stacked on both CPE (per-CPE-port) and CO (per-CPE), no CE-VID filtering

This configuration applicable in any deployment, accepts all customer traffic, encapsulates it twice by External SE-VID and Inner SE-VID tags which are applied on CO NE and CPE NE accordingly. In case of tagged Customer traffic, triple-tagged frames should be processed (cause additional 6 bytes of MFS size required on WAN/MAN equipment).

Management traffic in this configuration has the following limitations:

- CO management traffic can be either tagged or un-tagged (in-band or out-of-band).
- CPE management traffic should be dual-tagged (with Inner SE-MGMT-VID (limitation of HSL port of CPE by ML700) and with External SE-TRFC-VID (to pass through CO)).

➢ **To configure the LAN topology:**

- Obtain the VID(s) (VID = 1 to 4095) to represent the Customer in Provider Network (by SE-VID). Service Edge VLAN (SE-VID) can be added on each NE (CO or CPE or both).
- Obtain the VLAN tag Ethernet type according to the Provider Network rules (default is 0x8100, like as in Cisco's Q-in-Q implementation);
- Launch MetaASSIST View Application and connect to the NE on CO via craft (recommended);
- Please use Online Help, available in MetaASSIST View, to get a detailed description on how to perform the following configuration;
- Configure obtained Ethernet Type as desired on CO and CPE NEs;
- Configure chosen VID on all NEs, starting from the most remote NE, using the guidelines for each topology, as described below.

The following sections provide the schemes and the configuration order for all listed topologies above.

SP-VID per CPE Port

This configuration applicable in any deployment, encapsulates all customers' frames (tagged and untagged, without filtering of CE-VID) using an additional SE-VID tag. This configuration also allows multiple SE-VIDs per CPE (one per port), supporting multiple customers per CPE. In addition, allows intra-switching between CPEs, using switching between HSL ports (belonging to the same SE-VID) on CO NE. Management traffic in this configuration can be either VLAN-tagged or VLAN-untagged, as desired. In-band management traffic beyond the CPE is unsupported in this case.

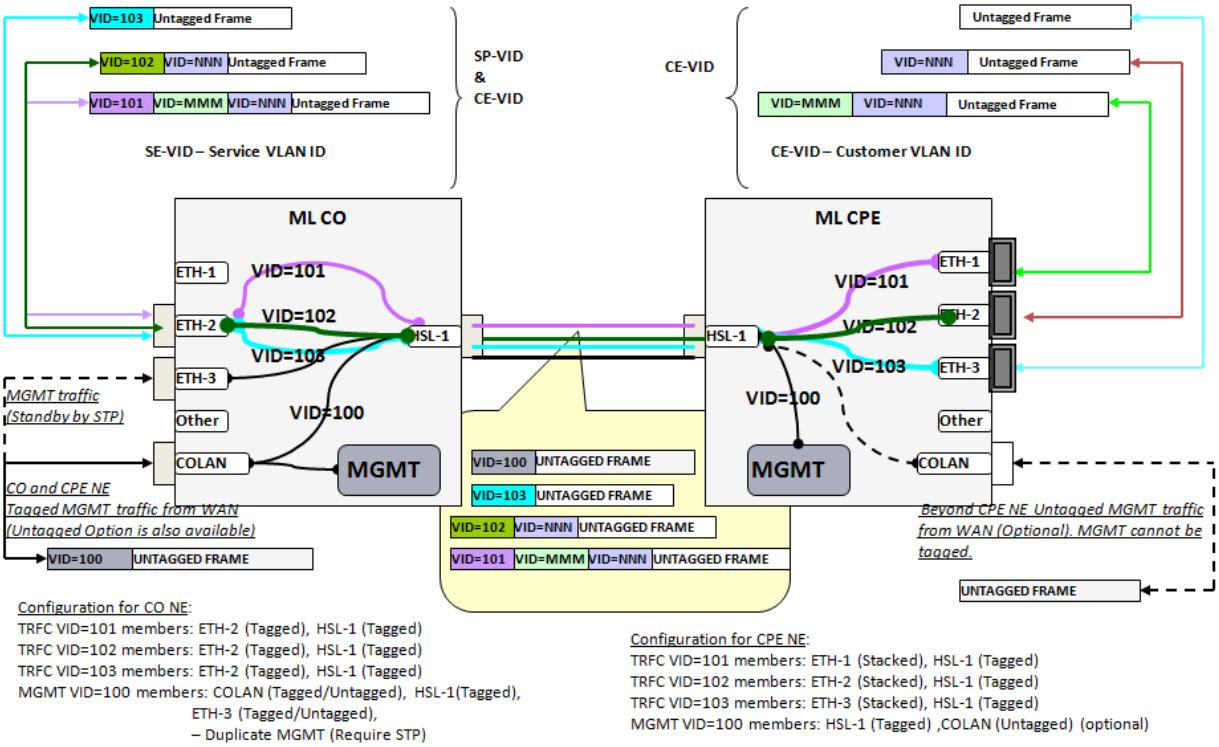


Figure 23: CE-VID preserving without filtering, stacked per each Port on CPE NE.

Table 112: Configuration summary for "CE-VID preserving/no filtering, with stacking per CPE port"

CO NE	Intermediate NE (optional)	CPE NE
ETH-x [Tagged] for TRFC VID and [Tagged] for MGMT VID (optional).	ETH-x [Untagged] for TRFC VID.	ETH-x [Stacked] for TRFC VID.
HSL-1 [Tagged] [1] for TRFC VID and [Tagged] for MGMT VID.	HSL-1 is [Tagged] for TRFC VID and [Tagged] MGMT VID.	HSL-1 [Tagged] for TRFC VID and [Tagged] for MGMT VID.
COLAN [Tagged or Untagged] for MGMT VID.	COLAN [Tagged or Untagged] for MGMT VID (optional).	COLAN [Tagged] for MGMT VID (optional).

[1] NOTE: Equal VID on multiple HSL provides intra-switching between appropriate ports of appropriated CPEs.

SP-VID per both CPE & CPE Port (non-IP CPE MGMT)

This configuration applicable in any deployment, accepts all customer traffic, encapsulates it twice by External SE-VID and Inner SE-VID tags which are applied on CO NE and CPE NE accordingly. In case of tagged Customer traffic, triple-tagged frames should be processed (cause additional 6 bytes of MFS size required on WAN/MAN equipment). Management traffic in this configuration has the following limitations. CO management traffic can be either tagged or un-tagged (in-band or out-of-band). CPE management traffic should be dual-tagged (with Inner SE-MGMT-VID (limitation of HSL port of CPE by ML700) and with External SE-TRFC-VID (to pass through CO).

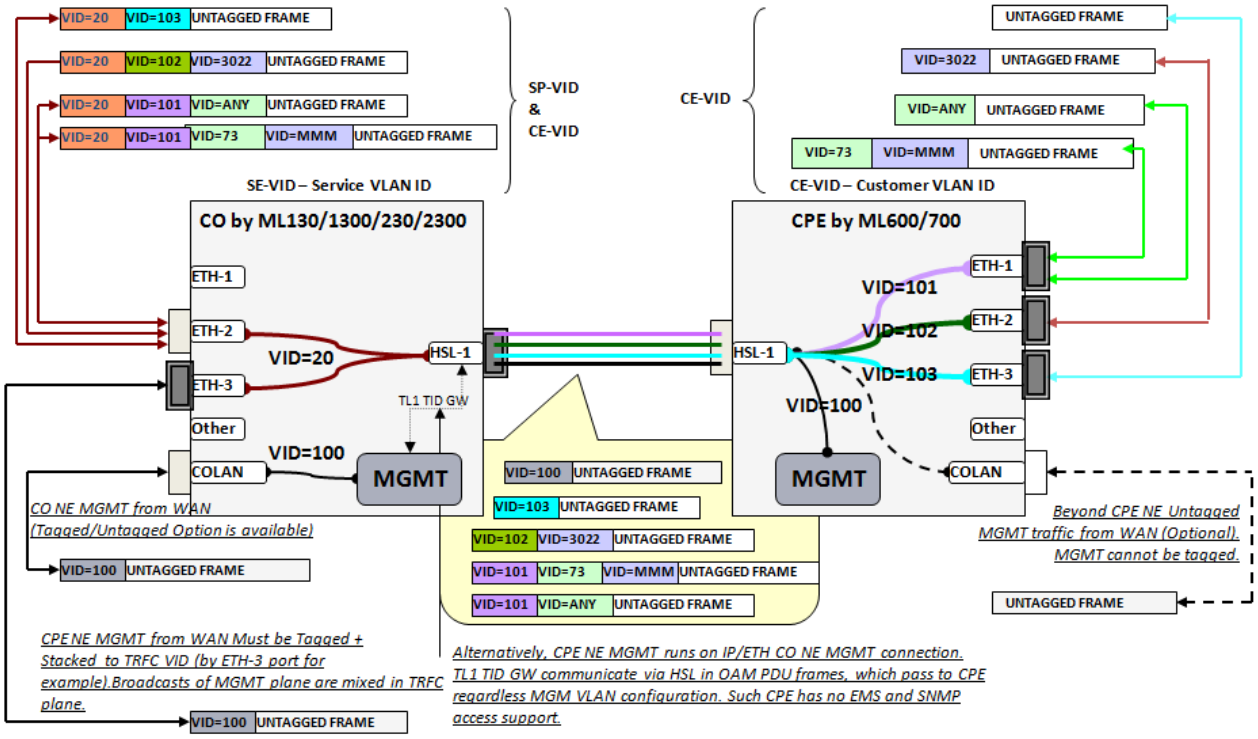


Figure 24: CE-VID preserving without filtering, VLAN dual stacking (per CPE port and per whole CPE)

Table 113: Configuration summary for "Dual CE-VID preserving/no filtering, stacking on CPE and CO"

CO NE	Intermediate NE (optional)	CPE NE
ETH-x [Tagged] for TRFC VID. ETH-x [Tagged] for MGMT VID (to manage CO NE). ETH-x [Stacked] for MGMT VID (to access CPE NE for management, traffic should pass through HSL as service traffic).	ETH-x [Tagged] for TRFC VID.	ETH-x [Stacked] for TRFC VID.
HSL-1 [Stacked] for TRFC VID (no MGMT VID through HSL, it is encapsulated by TRFC VID to achieve CPE NE).	HSL-1 [Tagged] for TRFC VID, HSL-1 [Tagged] for MGMT VID.	HSL-1 [Tagged] for TRFC VID HSL-1 [Tagged] for MGMT VID.
COLAN [Tagged or Untagged] for MGMT VID (to manage CO NE) (optional)(require STP).	COLAN [Untagged] for MGMT VID (optional).	COLAN [Untagged] for MGMT VID (optional).

SP-VID per both CPE & CPE Port (IP CPE MGMT)

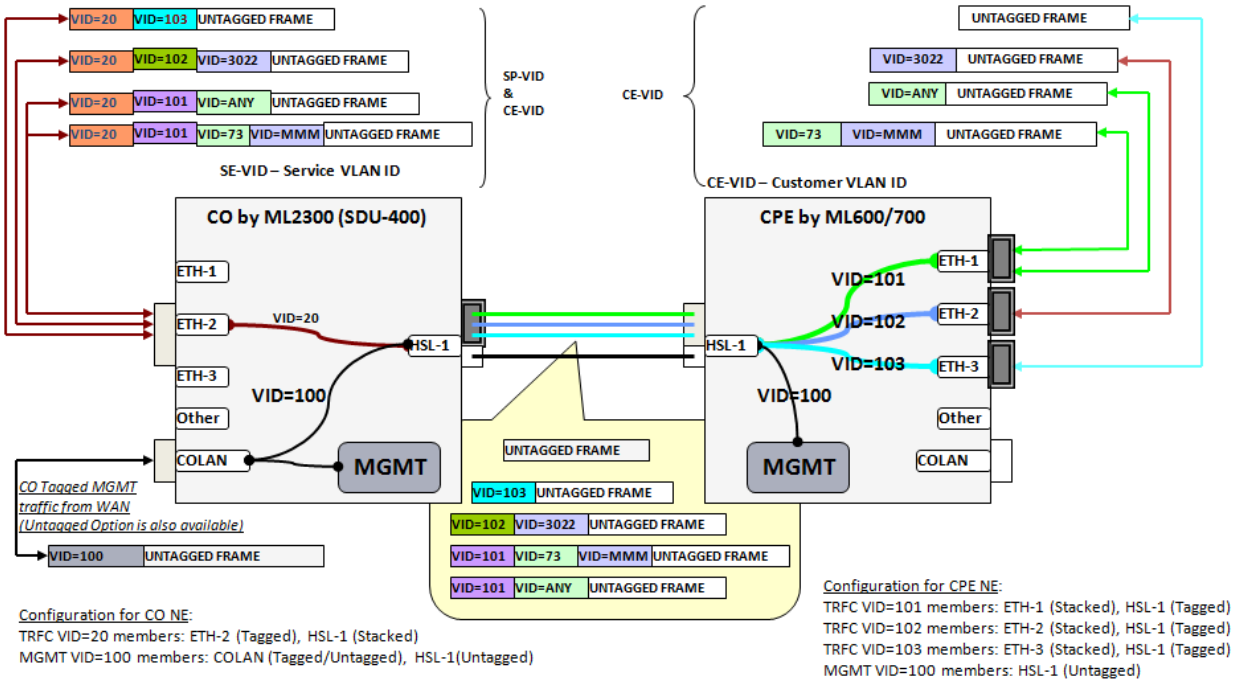


Figure 25: SP-VID per CPE and CPE port

SP-VID per CPE, CPE Port VLAN Filtering

This configuration applicable in any deployment, allows filtering of CE-VID on CPE and on CO encapsulates all permitted customer frames by additional SE-VID tag (one per each CPE). This configuration also allows intra-switching between CPEs, using switching between HSL ports (belonging to the same SE-VID) on CO NE. Management traffic in this configuration can be either VLAN-tagged or VLAN-untagged, as desired. In-band management traffic beyond the CPE is also available. This configuration allows Management VID re-mapping (applicable in case when MGMT VID to contradict with CE-VID on CPE).

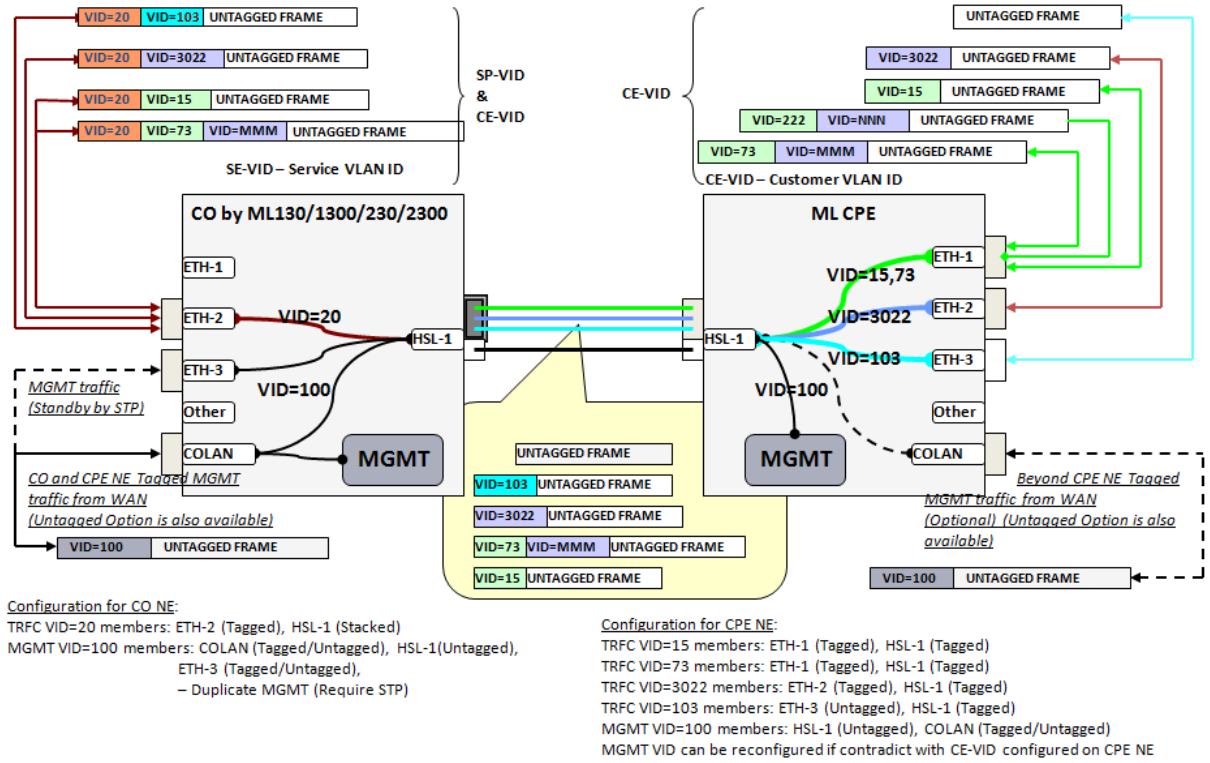


Figure 26: CE-VID preserving with filtering, VLAN stacking on CO NE per whole CPE NE

Table 114: Configuration summary for "CE-VID preserving with filtering, with stacking on CO, per CPE"

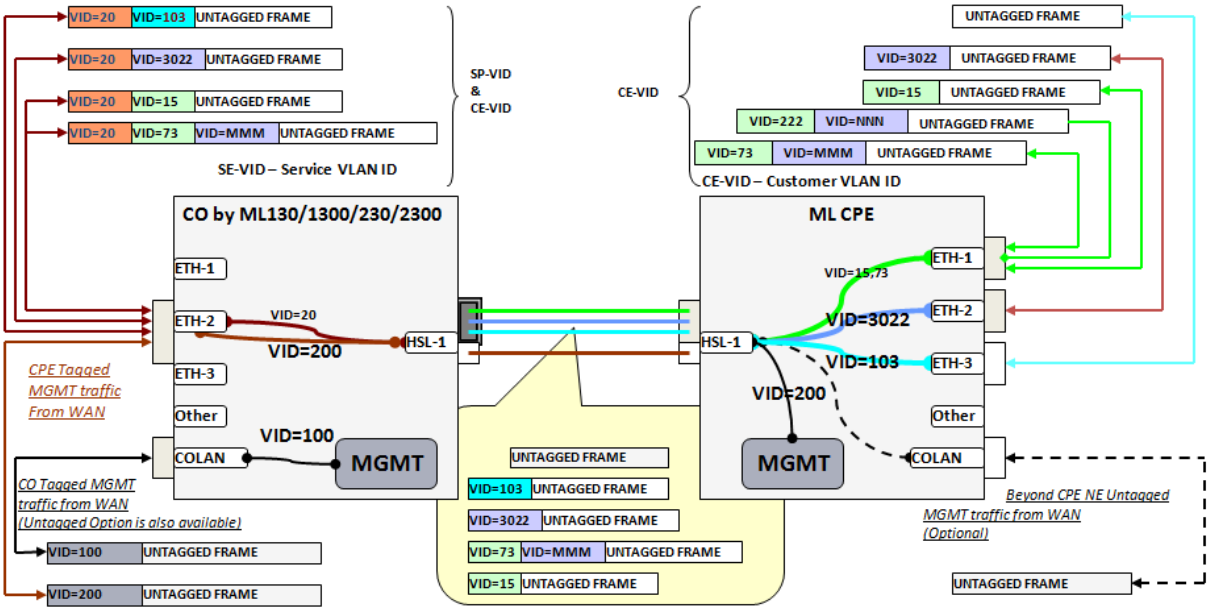
CO NE	Intermediate NE (optional)	CPE NE
ETH-x [Tagged] for TRFC VID and [Tagged] for MGMT VID (optional), (require STP).	ETH [Untagged] for TRFC VID.	ETH-x [Tagged or Untagged] for TRFC VID.
HSL-1 [Stacked] for TRFC VID and [Untagged] for MGMT VID.	HSL-1 [Tagged] for TRFC VID, HSL-1 [Untagged] for MGMT VID.	HSL-1 [Tagged] for TRFC VID, HSL-1 [Untagged] for MGMT VID.
COLAN [Tagged or Untagged] for MGMT VID.	COLAN [Untagged] for MGMT VID (optional).	COLAN [Untagged] for MGMT VID (optional).

SP-VID per CPE, CPE Port VLAN Filtering (Separate IP MGMT for CO/CPE)

Management Traffic toward CO and CPE may belong to different MGMT VLANs. To achieve this functionality, the following configuration should be applied:

- A port on the CO NE should be configured with two TRFC VLANs:
  - TRFC VLAN with STACKED membership will serve Tagged Traffic (VID=20 in the illustration below). All Customer traffic, passed through CPE is tagged – natively from Customer Side, or being modified on UNTAGGED port – where default Port VID is added
  - TRFC VLAN with UNTAGGED membership will serve Untagged Traffic (VID=200 in the illustration below). Only CPE Management traffic should be untagged.
- MGMT VLAN ID on the CO NE (VID=100 in the illustration below) should NOT include HSL port; i.e. CO Management traffic should not pass to the CPE on Customer side
- MGMT VLAN ID on CPE NE (VID=200 in the illustration below) should be set on CPE NE only. The same VID on the CO NE is configured as a TRFC VLAN (see above).

The next drawing illustrates configuration and traffic flow in case of CO/CPE Different Management VLANs



Configuration for CO NE:
TRFC VID=20 members: ETH-2 (Tagged), HSL-1 (Stacked)
TRFC VID=200 members ETH-2 (tagged), HSL-1 (Untagged)
MGMT VID=100 members: COLAN (Tagged/Untagged), HSL-1(Untagged),

Configuration for CPE NE:
TRFC VID=15 members: ETH-1 (Tagged), HSL-1 (Tagged)
TRFC VID=73 members: ETH-1 (Tagged), HSL-1 (Tagged)
TRFC VID=3022 members: ETH-2 (Tagged), HSL-1 (Tagged)
TRFC VID=103 members: ETH-3 (Untagged), HSL-1 (Tagged)
MGMT VID=200 members: HSL-1 (Untagged) COLAN (Untagged) (optional)

Appendix H - Environmental Alarm Condition Types

The following are the various environmental alarm types:

- AIRCOMPR Air compressor failure;
- AIRCOND Air condition failure;
- AIRDRYR Air dryer failure;
- BATDSCHRG Battery discharging;
- BATTERY Battery failure;
- CLFAN Cooling fan failure;
- CPMAJOR Centralized Power Major Environmental Alarm or Major Equipment Failure;
- CPMINOR Centralized Power Minor Environmental Alarm or Minor Equipment Failure;
- ENGINE Engine failure;
- ENGOPRG Engine operating;
- EXPLGS Explosive gas;
- FIRDETR Fire detector failure;
- FIRE Fire;
- FLOOD Flood;
- FUSE Fuse failure;
- GEN Generator failure;
- HIAIR High airflow;
- HIHUM High humidity;
- HITEMP High temperature;
- HIWTR High water;
- INTRUDER Intrusion;
- LWBATVG Low battery voltage;
- LWFUEL Low fuel;
- LWHUM Low humidity;
- LWPRES Low cable pressure;
- LWTEMP Low temperature;
- LWWTR Low water;
- MISC Miscellaneous;
- OPENDR Open door;
- POWER Commercial power failure;

- PUMP Pump failure;
- PWR1 Volt power supply 1 failure;
- PWR2 Volt power supply 2 failure;
- RECT Rectifier failure;
- RECTHI Rectifier high voltage;
- RECTLO Rectifier low voltage;
- SMOKE Smoke;
- TOXICGAS Toxic gas;
- VENTN Ventilation system failure.

Appendix I - Recommended Actelis MiTOP Configuration Parameters

The following tables provide Actelis recommended MiTOP settings.

NOTE: Refer to RAD's MiTOP UM for details on configurable parameters and configurable values.

MiTOP System Parameters

Table 115: MiTOP System Configuration

Parameter	Default Value	Menu Path	Set	Notes
System				
Management				
IP Address	0.0.0.0	Configuration > System > Management > Host IP	Must	Set the Management IP address of the device (Management IP, not for Service IP). In case of redundant system: Two MiTOP units share the same interface via Y power splitter – both units should have the same MGMT IP. Two MiTOP units connected to parallel cables – a different MGMT IP should be provided for each unit.
IP Mask	255.255.255.0		Must	Set the IP Mask (for Management, not Service).
Default Gateway	0.0.0.0		Must	Set the Default Gateway IP address (for Management, not Service). In order to be in the same MGMT plane where ML NE are managed, use default values proposed by MetaASSIST View.
Host Tagging	Untagged		Optional	This parameter is automatically set to **TAGGED** by the MAV when MGMT interface is configured on SFP. Untagged option is reserved for TRAFFIC VID.
Host VLAN ID	-		Optional	Enter Host VLAN ID. The parameter is automatically set with MGMT VID as on ML by the MAV, when MGMT interface is configured on SFP. *Note: ETH-x must be configured as MGMT VLAN member on ML.*
Host VLAN Priority	-		Optional	Enter Host VLAN Priority. Parameter is automatically set as COS=7 by the MAV when MGMT interface is configured on SFP.

Parameter	Default Value	Menu Path	Set	Notes
Device Name	MiTOP-T3	Configuration > System >Management > Device Info	Optional	Enter device name.
Device Location	-		Optional	Enter device location (text).
Contact Person	-		Optional	Enter the name of a contact person (text).
User account: User Level, User Name, Password	Su, 1234	Configuration > System > Management > User Access	Optional	Define Management Access Permissions for users.
LAN (Web)	Enable	Configuration > System > Management > Management Access	Optional	Management to the device is lost if changed to **Disable**. To restore the management, either use the **Restrat** button (reset to factory, all settings are lost) or connect the device to external SFP-CA, configuration module and change back to LAN.
Outband Mode	Normal	Configuration > System > Management > Outband	X	Keep default settings.
Fault Propagation				
LOS	Disable	Configuration > System > Fault Propagation	Optional	Set LOS propagation (TDM to Eth.) behavior. *Note: Configuring LOS propagation to Enable will prevent management connectivity to the MiTOP in case of TDM interface LOS.* For redundant system, if port equipped with SFP is listed as APS trigger, LOS propagation must be enabled.
AIS	Disable		Optional	Set LOS propagation (TDM to Eth.) behavior. *Note: Configuring AIS propagation to Enable will prevent management connectivity to the MiTOP in case of TDM interface AIS.* For redundant system see LOS propagation above.
Fault Propagation WTR	0		Optional	Enables setting the Wait to Restore time (if propagation enabled).
TX Disable				

Parameter	Default Value	Menu Path	Set	Notes
TX Disable Behaviour	Not Available (i.e. do nothing)	Configuration > System > Tx Disable Mode	Optional	Define the operation mode in case of TX disable. For redundant system (with passive coaxial 'Y' cable splitter) set to **Tri-state**.
LOS Behaviour				
LOS caused by AIS	Disable	Configuration > System > LOS Behavior	Optional	Set to **Enable** to provide LOS indication to the system in case of TDM LOS.
LOS caused by LOS	Disable		Optional	Set to **Enable** to provide LOS indication to the system in case of TDM RLOL (Receive Loss of Lock).
LOS caused by RLOL	Disable		Optional	Set to **Enable** to provide LOS indication to the system in case of TDM received AIS.

MiTOP Physical Layer Parameters

Table 116: MiTOP Physical Layer Configuration

Parameter	Default Value	Menu Path	Set	Notes
Physical Layer				
Interface Type	T3	Configuration > Physical Ports	Optional	Select the TDM Interface type (**E3** or **T3**).
TX Clock Source	Internal Clock	Configuration > Physical Ports > T3 (E3)	Must	For regular installations, set the Clock to **LBT** for the unit at the CO side and **Adaptive clock** on the unit at CPE.
Line Code	B3ZS		Optional	Set the required Line code: HDB3 for E3 and usually B3ZS for T3.
Line Type	T3 Unframed		X	Keep Line type Unframed.
Line Length	Up to 225 ft		Optional	Set the expected coax length, relevant only for T3 interface.
FEAC Code Receive	Enable		Optional	Keep enabled for better maintenance using FEAC (Far-End Alarm and Control).
Clock Recovery				
Source Quality	Stratum 3	Configuration > System > Clock Recovery	Optional	Set the Source clock quality, relevant only for units set to Adaptive Clock recovery.
Clock Mode	Auto		X	Keep in **Auto** (Manual mode is for debugging).

MiTOP Applications Parameters

Table 117: MiTOP Applications Configuration

Parameter	Default Value	Menu Path	Set	Notes
Applications				
Peer Unit				
Peer Number	1	Configuration > Applications > Multiservice over PSN > Peer	X	Should be kept **1**.
Peer Name	Peer Name 1		Optional	Set the Peer site name (description).
Peer IP Address	0.0.0.0		Must	Set Peer IP Address. In case of redundant system: Two MiTOP units share the same interface via Y-cable – both units should have the same MGMT IP. Two MiTOP units connected to parallel cables – different MGMT IP should be provided for each unit.
Next Hop address	0.0.0.0		Must	Set Next Hop IP Address.
Peer MAC Address	000000000000		Optional	Peer MAC IP Address, usually discovered automatically by ARP running on SFP.
PW Connection				
PW Number	1	Configuration > Applications > Multiservice over PSN > PW	X	Only valid value is **1**.
PW Name	PW Name 1		Optional	Defining a Pseudowire Connection.
Discarded by	15		Optional	Set the reasons for counting discarded frames.
PW Type	SAToP		X	Only valid value is **SAToP**.
Source IP	0.0.0.0	Configuration > Applications > Multiservice over PSN > PW > General Parameters	Must	Set the source IP for PW traffic (different from MGMT host IP).
PSN Type	UDP/IPv4		Must	Set the PSN Type (**UDP/IPv4**, **MPLS**, **MEF**).
Owner	Manually		X	Only valid value is **Manually**.
OAM	Enable		Optional	Defines OAM functionality.
Unreachable Detection	Disable		Optional	Defines Mitop operation in case of unreachable destination.
Multiplexing	Source		Optional	Define UDP source and destination ports.

Parameter	Default Value	Menu Path	Set	Notes
Out PW Label	16		Optional	Defines outgoing PW label. Needs to be changed if more than a single MiTOP SFP exists in the system.
In PW Label	16		Optional	Defines incoming PW label.
Enable Reorder Packets	Enable	Configuration > Applications > Multiservice over PSN > PW > PSN Parameters	Optional	Enable packet reordering.
TOS	0		Optional	Define ToS value.
VLAN Tagging	Disable		Optional	Enable/Disable VLAN tagging. Both options are valid, ETH-x port on ML should be set appropriately.
VLAN Priority	0		Optional	Defines VLAN priority value (if VLAN tagging is enabled).
VLAN ID	1		Optional	Define VLAN ID (if VLAN tagging is enabled).
Ingress Label	16		Optional	Define ingress MPLS tunnel label (valid only for MPLS network).
Egress Label	16		Optional	Define egress MPLS tunnel label (valid only for MPLS network).
EXP bit	0		Optional	Define EXP bits value (valid only for MPLS network).
TTL	0		Optional	Defines Time-To-Leave value (valid only for MPLS network).
Payload Size	256 bytes	Configuration > Applications > Multiservice over PSN > PW > Service Parameters	Optional	Define TDM payload size, low payload size would increase HSL required BW.
Jitter Buffer	500 usec		Must	Define jitter buffer, set to 2000usec or higher.
E3, T3 port number	1		X	Only valid value is **1**.