ETX-203A
Carrier Ethernet Demarcation Device
Version 3.0
Installation and Operation Manual

Notice

This manual contains information that is proprietary to RAD Data Communications Ltd. (“RAD”). No part of this publication may be reproduced in any form whatsoever without prior written approval by RAD Data Communications.

Right, title and interest, all information, copyrights, patents, know-how, trade secrets and other intellectual property or other proprietary rights relating to this manual and to the ETX-203A and any software components contained therein are proprietary products of RAD protected under international copyright law and shall be and remain solely with RAD.

The ETX-203A product name is owned by RAD. No right, license, or interest to such trademark is granted hereunder, and you agree that no such right, license, or interest shall be asserted by you with respect to such trademark. The RAD name, logo, logotype, and the terms EtherAccess, TDMoIP and TDMoIP Driven, and the product names Optimux and IPmux, are registered trademarks of RAD Data Communications Ltd. All other trademarks are the property of their respective holders.

You shall not copy, reverse compile or reverse assemble all or any portion of the Manual or the ETX-203A. You are prohibited from, and shall not, directly or indirectly, develop, market, distribute, license, or sell any product that supports substantially similar functionality as the ETX-203A, based on or derived in any way from the ETX-203A. Your undertaking in this paragraph shall survive the termination of this Agreement.

This Agreement is effective upon your opening of the ETX-203A package and shall continue until terminated. RAD may terminate this Agreement upon the breach by you of any term hereof. Upon such termination by RAD, you agree to return to RAD the ETX-203A and all copies and portions thereof.

For further information contact RAD at the address below or contact your local distributor.

<table>
<thead>
<tr>
<th>International Headquarters</th>
<th>North America Headquarters</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAD Data Communications Ltd.</td>
<td>RAD Data Communications Inc.</td>
</tr>
<tr>
<td>24 Raoul Wallenberg Street</td>
<td>900 Corporate Drive</td>
</tr>
<tr>
<td>Tel Aviv 69719, Israel</td>
<td>Mahwah, NJ 07430, USA</td>
</tr>
<tr>
<td>Tel: 972-3-6458181</td>
<td>Tel: (201) 5291100, Toll free: 1-800-4447234</td>
</tr>
<tr>
<td>Fax: 972-3-6498250, 6474436</td>
<td>Fax: (201) 5295777</td>
</tr>
<tr>
<td>E-mail: <a href="mailto:market@rad.com">market@rad.com</a></td>
<td>E-mail: <a href="mailto:market@rad.com">market@rad.com</a></td>
</tr>
</tbody>
</table>

© 2010–2011 RAD Data Communications Ltd.  Publication No. 530-200-07/11
Limited Warranty

RAD warrants to DISTRIBUTOR that the hardware in the ETX-203A to be delivered hereunder shall be free of defects in material and workmanship under normal use and service for a period of twelve (12) months following the date of shipment to DISTRIBUTOR.

If, during the warranty period, any component part of the equipment becomes defective by reason of material or workmanship, and DISTRIBUTOR immediately notifies RAD of such defect, RAD shall have the option to choose the appropriate corrective action: a) supply a replacement part, or b) request return of equipment to its plant for repair, or c) perform necessary repair at the equipment’s location. In the event that RAD requests the return of equipment, each party shall pay one-way shipping costs.

RAD shall be released from all obligations under its warranty in the event that the equipment has been subjected to misuse, neglect, accident or improper installation, or if repairs or modifications were made by persons other than RAD’s own authorized service personnel, unless such repairs by others were made with the written consent of RAD.

The above warranty is in lieu of all other warranties, expressed or implied. There are no warranties which extend beyond the face hereof, including, but not limited to, warranties of merchantability and fitness for a particular purpose, and in no event shall RAD be liable for consequential damages.

RAD shall not be liable to any person for any special or indirect damages, including, but not limited to, lost profits from any cause whatsoever arising from or in any way connected with the manufacture, sale, handling, repair, maintenance or use of the ETX-203A, and in no event shall RAD’s liability exceed the purchase price of the ETX-203A.

DISTRIBUTOR shall be responsible to its customers for any and all warranties which it makes relating to ETX-203A and for ensuring that replacements and other adjustments required in connection with the said warranties are satisfactory.

Software components in the ETX-203A are provided "as is" and without warranty of any kind. RAD disclaims all warranties including the implied warranties of merchantability and fitness for a particular purpose. RAD shall not be liable for any loss of use, interruption of business or indirect, special, incidental or consequential damages of any kind. In spite of the above RAD shall do its best to provide error-free software products and shall offer free Software updates during the warranty period under this Agreement.

RAD’s cumulative liability to you or any other party for any loss or damages resulting from any claims, demands, or actions arising out of or relating to this Agreement and the ETX-203A shall not exceed the sum paid to RAD for the purchase of the ETX-203A. In no event shall RAD be liable for any indirect, incidental, consequential, special, or exemplary damages or lost profits, even if RAD has been advised of the possibility of such damages.

This Agreement shall be construed and governed in accordance with the laws of the State of Israel.

Product Disposal

To facilitate the reuse, recycling and other forms of recovery of waste equipment in protecting the environment, the owner of this RAD product is required to refrain from disposing of this product as unsorted municipal waste at the end of its life cycle. Upon termination of the unit’s use, customers should provide for its collection for reuse, recycling or other form of environmentally conscientious disposal.
General Safety Instructions

The following instructions serve as a general guide for the safe installation and operation of telecommunications products. Additional instructions, if applicable, are included inside the manual.

Safety Symbols

This symbol may appear on the equipment or in the text. It indicates potential safety hazards regarding product operation or maintenance to operator or service personnel.

Danger of electric shock! Avoid any contact with the marked surface while the product is energized or connected to outdoor telecommunication lines.

Protective ground: the marked lug or terminal should be connected to the building protective ground bus.

Some products may be equipped with a laser diode. In such cases, a label with the laser class and other warnings as applicable will be attached near the optical transmitter. The laser warning symbol may be also attached.

Please observe the following precautions:

• Before turning on the equipment, make sure that the fiber optic cable is intact and is connected to the transmitter.
• Do not attempt to adjust the laser drive current.
• Do not use broken or unterminated fiber-optic cables/connectors or look straight at the laser beam.
• The use of optical devices with the equipment will increase eye hazard.
• Use of controls, adjustments or performing procedures other than those specified herein, may result in hazardous radiation exposure.

ATTENTION: The laser beam may be invisible!

In some cases, the users may insert their own SFP laser transceivers into the product. Users are alerted that RAD cannot be held responsible for any damage that may result if non-compliant transceivers are used. In particular, users are warned to use only agency approved products that comply with the local laser safety regulations for Class 1 laser products.

Always observe standard safety precautions during installation, operation and maintenance of this product. Only qualified and authorized service personnel should carry out adjustment, maintenance or repairs to this product. No installation, adjustment, maintenance or repairs should be performed by either the operator or the user.
Handling Energized Products

General Safety Practices

Do not touch or tamper with the power supply when the power cord is connected. Line voltages may be present inside certain products even when the power switch (if installed) is in the OFF position or a fuse is blown. For DC-powered products, although the voltages levels are usually not hazardous, energy hazards may still exist.

Before working on equipment connected to power lines or telecommunication lines, remove jewelry or any other metallic object that may come into contact with energized parts.

Unless otherwise specified, all products are intended to be grounded during normal use. Grounding is provided by connecting the mains plug to a wall socket with a protective ground terminal. If a ground lug is provided on the product, it should be connected to the protective ground at all times, by a wire with a diameter of 18 AWG or wider. Rack-mounted equipment should be mounted only in grounded racks and cabinets.

Always make the ground connection first and disconnect it last. Do not connect telecommunication cables to ungrounded equipment. Make sure that all other cables are disconnected before disconnecting the ground.

Some products may have panels secured by thumbscrews with a slotted head. These panels may cover hazardous circuits or parts, such as power supplies. These thumbscrews should therefore always be tightened securely with a screwdriver after both initial installation and subsequent access to the panels.

Connecting AC Mains

Make sure that the electrical installation complies with local codes.

Always connect the AC plug to a wall socket with a protective ground.

The maximum permissible current capability of the branch distribution circuit that supplies power to the product is 16A (20A for USA and Canada). The circuit breaker in the building installation should have high breaking capacity and must operate at short-circuit current exceeding 35A (40A for USA and Canada).

Always connect the power cord first to the equipment and then to the wall socket. If a power switch is provided in the equipment, set it to the OFF position. If the power cord cannot be readily disconnected in case of emergency, make sure that a readily accessible circuit breaker or emergency switch is installed in the building installation.

In cases when the power distribution system is IT type, the switch must disconnect both poles simultaneously.

Connecting DC Power

Unless otherwise specified in the manual, the DC input to the equipment is floating in reference to the ground. Any single pole can be externally grounded.

Due to the high current capability of DC power systems, care should be taken when connecting the DC supply to avoid short-circuits and fire hazards.

Make sure that the DC power supply is electrically isolated from any AC source and that the installation complies with the local codes.
The maximum permissible current capability of the branch distribution circuit that supplies power to the product is 16A (20A for USA and Canada). The circuit breaker in the building installation should have high breaking capacity and must operate at short-circuit current exceeding 35A (40A for USA and Canada).

Before connecting the DC supply wires, ensure that power is removed from the DC circuit. Locate the circuit breaker of the panel board that services the equipment and switch it to the OFF position. When connecting the DC supply wires, first connect the ground wire to the corresponding terminal, then the positive pole and last the negative pole. Switch the circuit breaker back to the ON position.

A readily accessible disconnect device that is suitably rated and approved should be incorporated in the building installation.

If the DC power supply is floating, the switch must disconnect both poles simultaneously.

### Connecting Data and Telecommunications Cables

Data and telecommunication interfaces are classified according to their safety status.

The following table lists the status of several standard interfaces. If the status of a given port differs from the standard one, a notice will be given in the manual.

<table>
<thead>
<tr>
<th>Ports</th>
<th>Safety Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>V.11, V.28, V.35, V.36, RS-530, X.21, 10 BaseT, 100 BaseT, Unbalanced E1, E2, E3, STM, DS-2, DS-3, S-Interface ISDN, Analog voice E&amp; M</td>
<td>SELV Safety Extra Low Voltage: Ports which do not present a safety hazard. Usually up to 30 VAC or 60 VDC.</td>
</tr>
<tr>
<td>xDSL (without feeding voltage), Balanced E1, T1, Sub E1/T1</td>
<td>TNV-1 Telecommunication Network Voltage-1: Ports whose normal operating voltage is within the limits of SELV, on which overvoltages from telecommunications networks are possible.</td>
</tr>
<tr>
<td>FXS (Foreign Exchange Subscriber)</td>
<td>TNV-2 Telecommunication Network Voltage-2: Ports whose normal operating voltage exceeds the limits of SELV (usually up to 120 VDC or telephone ringing voltages), on which overvoltages from telecommunication networks are not possible. These ports are not permitted to be directly connected to external telephone and data lines.</td>
</tr>
<tr>
<td>FXO (Foreign Exchange Office), xDSL (with feeding voltage), U-Interface ISDN</td>
<td>TNV-3 Telecommunication Network Voltage-3: Ports whose normal operating voltage exceeds the limits of SELV (usually up to 120 VDC or telephone ringing voltages), on which overvoltages from telecommunication networks are possible.</td>
</tr>
</tbody>
</table>

**Always connect a given port to a port of the same safety status. If in doubt, seek the assistance of a qualified safety engineer.**

Always make sure that the equipment is grounded before connecting telecommunication cables. Do not disconnect the ground connection before disconnecting all telecommunications cables.

Some SELV and non-SELV circuits use the same connectors. Use caution when connecting cables. Extra caution should be exercised during thunderstorms.
When using shielded or coaxial cables, verify that there is a good ground connection at both ends. The grounding and bonding of the ground connections should comply with the local codes.

The telecommunication wiring in the building may be damaged or present a fire hazard in case of contact between exposed external wires and the AC power lines. In order to reduce the risk, there are restrictions on the diameter of wires in the telecom cables, between the equipment and the mating connectors.

**Caution**

To reduce the risk of fire, use only No. 26 AWG or larger telecommunication line cords.

---

**Attention**

Pour réduire les risques s’incendie, utiliser seulement des conducteurs de télécommunications 26 AWG ou de section supérieure.

---

Some ports are suitable for connection to intra-building or non-exposed wiring or cabling only. In such cases, a notice will be given in the installation instructions.

Do not attempt to tamper with any carrier-provided equipment or connection hardware.

---

**Electromagnetic Compatibility (EMC)**

The equipment is designed and approved to comply with the electromagnetic regulations of major regulatory bodies. The following instructions may enhance the performance of the equipment and will provide better protection against excessive emission and better immunity against disturbances.

A good ground connection is essential. When installing the equipment in a rack, make sure to remove all traces of paint from the mounting points. Use suitable lock-washers and torque. If an external grounding lug is provided, connect it to the ground bus using braided wire as short as possible.

The equipment is designed to comply with EMC requirements when connecting it with unshielded twisted pair (UTP) cables. However, the use of shielded wires is always recommended, especially for high-rate data. In some cases, when unshielded wires are used, ferrite cores should be installed on certain cables. In such cases, special instructions are provided in the manual.

Disconnect all wires which are not in permanent use, such as cables used for one-time configuration.

The compliance of the equipment with the regulations for conducted emission on the data lines is dependent on the cable quality. The emission is tested for UTP with 80 dB longitudinal conversion loss (LCL).

Unless otherwise specified or described in the manual, TNV-1 and TNV-3 ports provide secondary protection against surges on the data lines. Primary protectors should be provided in the building installation.

The equipment is designed to provide adequate protection against electro-static discharge (ESD). However, it is good working practice to use caution when connecting cables terminated with plastic connectors (without a grounded metal hood, such as flat cables) to sensitive data lines. Before connecting such cables, discharge yourself by touching ground or wear an ESD preventive wrist strap.
FCC-15 User Information

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

Canadian Emission Requirements

This Class A digital apparatus meets all the requirements of the Canadian Interference-Causing Equipment Regulation.

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

Warning per EN 55022 (CISPR-22)

<table>
<thead>
<tr>
<th>Warning</th>
<th>This is a class A product. In a domestic environment, this product may cause radio interference, in which case the user will be required to take adequate measures.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avertissement</td>
<td>Cet appareil est un appareil de Classe A. Dans un environnement résidentiel, cet appareil peut provoquer des brouillages radioélectriques. Dans ces cas, il peut être demandé à l'utilisateur de prendre les mesures appropriées.</td>
</tr>
<tr>
<td>Achtung</td>
<td>Das vorliegende Gerät fällt unter die Funkstörgrenzwertklasse A. In Wohngebieten können beim Betrieb dieses Gerätes Rundfunkstörungen auftreten, für deren Behebung der Benutzer verantwortlich ist.</td>
</tr>
</tbody>
</table>
Mise au rebut du produit

Afin de faciliter la réutilisation, le recyclage ainsi que d’autres formes de récupération d’équipement mis au rebut dans le cadre de la protection de l’environnement, il est demandé au propriétaire de ce produit RAD de ne pas mettre ce dernier au rebut en tant que déchet municipal non trié, une fois que le produit est arrivé en fin de cycle de vie. Le client devrait proposer des solutions de réutilisation, de recyclage ou toute autre forme de mise au rebut de cette unité dans un esprit de protection de l’environnement, lorsqu’il aura fini de l’utiliser.

Instructions générales de sécurité

Les instructions suivantes servent de guide général d’installation et d’opération sécurisées des produits de télécommunications. Des instructions supplémentaires sont éventuellement indiquées dans le manuel.

Symboles de sécurité

Ce symbole peut apparaître sur l’équipement ou dans le texte. Il indique des risques potentiels de sécurité pour l’opérateur ou le personnel de service, quant à l’opération du produit ou à sa maintenance.

Avertissement

Danger de choc électrique ! Evitez tout contact avec la surface marquée tant que le produit est sous tension ou connecté à des lignes externes de télécommunications.

Mise à la terre de protection : la cosse ou la borne marquée devrait être connectée à la prise de terre de protection du bâtiment.
Certains produits peuvent être équipés d’une diode laser. Dans de tels cas, une étiquette indiquant la classe laser ainsi que d’autres avertissements, le cas échéant, sera jointe près du transmetteur optique. Le symbole d’avertissement laser peut aussi être joint.

Veuillez observer les précautions suivantes :

• Avant la mise en marche de l’équipement, assurez-vous que le câble de fibre optique est intact et qu’il est connecté au transmetteur.
• Ne tentez pas d’ajuster le courant de la commande laser.
• N’utilisez pas des câbles ou connecteurs de fibre optique cassés ou sans terminaison et n’observez pas directement un rayon laser.
• L’usage de périphériques optiques avec l’équipement augmentera le risque pour les yeux.
• L’usage de contrôles, ajustages ou procédures autres que celles spécifiées ici pourrait résulter en une dangereuse exposition aux radiations.

ATTENTION : Le rayon laser peut être invisible !

Les utilisateurs pourront, dans certains cas, insérer leurs propres émetteurs-récepteurs Laser SFP dans le produit. Les utilisateurs sont avertis que RAD ne pourra pas être tenue responsable de tout dommage pouvant résulter de l’utilisation d’émetteurs-récepteurs non conformes. Plus particulièrement, les utilisateurs sont avertis de n’utiliser que des produits approuvés par l’agence et conformes à la réglementation locale de sécurité laser pour les produits laser de classe 1.

Respectez toujours les précautions standards de sécurité durant l’installation, l’opération et la maintenance de ce produit. Seul le personnel de service qualifié et autorisé devrait effectuer l’ajustage, la maintenance ou les réparations de ce produit. Aucune opération d’installation, d’ajustage, de maintenance ou de réparation ne devrait être effectuée par l’opérateur ou l’utilisateur.

**Manipuler des produits sous tension**

**Règles générales de sécurité**

Ne pas toucher ou alterer l’alimentation en courant lorsque le câble d’alimentation est branché. Des tensions de lignes peuvent être présentes dans certains produits, même lorsque le commutateur (s’il est installé) est en position OFF ou si le fusible est rompu. Pour les produits alimentés par CC, les niveaux de tension ne sont généralement pas dangereux mais des risques de courant peuvent toujours exister.

Avant de travailler sur un équipement connecté aux lignes de tension ou de télécommunications, retirez vos bijoux ou tout autre objet métallique pouvant venir en contact avec les pièces sous tension.

Sauf s’il en est autrement indiqué, tous les produits sont destinés à être mis à la terre durant l’usage normal. La mise à la terre est fournie par la connexion de la fiche principale à une prise murale équipée d’une borne protectrice de mise à la terre. Si une cosse de mise à la terre est fournie avec le produit, elle devrait être connectée à tout moment à une mise à la terre de protection par un conducteur de diamètre 18 AWG ou plus. L’équipement monté en châssis ne devrait être monté que sur des châssis et dans des armoires mises à la terre.

Branchez toujours la mise à la terre en premier et débranchez-la en dernier. Ne branchez pas des câbles de télécommunications à un équipement qui n’est pas mis à la terre. Assurez-vous que tous les autres câbles sont débrançhés avant de déconnecter la mise à la terre.
**Connexion au courant du secteur**

Assurez-vous que l'installation électrique est conforme à la réglementation locale.

Branchez toujours la fiche de secteur à une prise murale équipée d'une borne protectrice de mise à la terre.

La capacité maximale permissible en courant du circuit de distribution de la connexion alimentant le produit est de 16A (20A aux Etats-Unis et Canada). Le coupe-circuit dans l'installation du bâtiment devrait avoir une capacité élevée de rupture et devrait fonctionner sur courant de court-circuit dépassant 35A (40A aux Etats-Unis et Canada).

Branchez toujours le câble d'alimentation en premier à l'équipement puis à la prise murale. Si un commutateur est fourni avec l'équipement, fixez-le en position OFF. Si le câble d'alimentation ne peut pas être facilement débranché en cas d'urgence, assurez-vous qu'un coupe-circuit ou un disjoncteur d'urgence facilement accessible est installé dans l'installation du bâtiment.

Le disjoncteur devrait déconnecter simultanément les deux pôles si le système de distribution de courant est de type IT.

**Connexion d'alimentation CC**

Sauf s'il en est autrement spécifié dans le manuel, l'entrée CC de l'équipement est flottante par rapport à la mise à la terre. Tout pôle doit être mis à la terre en externe.

A cause de la capacité de courant des systèmes à alimentation CC, des précautions devraient être prises lors de la connexion de l'alimentation CC pour éviter des courts-circuits et des risques d'incendie.

Assurez-vous que l'alimentation CC est isolée de toute source de courant CA (secteur) et que l'installation est conforme à la réglementation locale.

La capacité maximale permissible en courant du circuit de distribution de la connexion alimentant le produit est de 16A (20A aux Etats-Unis et Canada). Le coupe-circuit dans l'installation du bâtiment devrait avoir une capacité élevée de rupture et devrait fonctionner sur courant de court-circuit dépassant 35A (40A aux Etats-Unis et Canada).

Avant la connexion des câbles d'alimentation en courant CC, assurez-vous que le circuit CC n'est pas sous tension. Localisez le coupe-circuit dans le tableau desservant l’équipement et fixez-le en position OFF. Lors de la connexion de câbles d'alimentation CC, connectez d'abord le conducteur de mise à la terre à la borne correspondante, puis le pôle positif et en dernier, le pôle négatif. Remettez le coupe-circuit en position ON.

Un disjoncteur facilement accessible, adapté et approuvé devrait être intégré à l'installation du bâtiment.

Le disjoncteur devrait déconnecter simultanément les deux pôles si l'alimentation en courant CC est flottante.
<p>| <strong>Glossary</strong> |
|-----------------|--------------------------------------------------------------------------------------------------|
| <strong>Address</strong>     | A coded representation of the origin or destination of data.                                    |
| <strong>Agent</strong>       | In SNMP, this refers to the managed system.                                                      |
| <strong>Analog</strong>      | A continuous wave or signal (such as human voice).                                               |
| <strong>ANSI</strong>        | American National Standards Institute.                                                           |
| <strong>Attenuation</strong> | Signal power loss through equipment, lines or other transmission devices. Measured in decibels. |
| <strong>AWG</strong>         | The American Wire Gauge System, which specifies wire width.                                      |
| <strong>Backhaul</strong>    | Transporting traffic between distributed sites (typically access points) and more centralized points of presence. |
| <strong>Balanced</strong>    | A transmission line in which voltages on the two conductors are equal in magnitude, but opposite in polarity, with respect to ground. |
| <strong>Bandwidth</strong>   | The range of frequencies passing through a given circuit. The greater the bandwidth, the more information can be sent through the circuit in a given amount of time. |
| <strong>Baud</strong>        | Unit of signaling speed equivalent to the number of discrete conditions or events per second. If each signal event represents only one bit condition, baud rate equals bps (bits per second). |
| <strong>Best Effort</strong> | A QoS class in which no specific traffic parameters and no absolute guarantees are provided.    |
| <strong>Bipolar</strong>     | Signaling method in E1/T1 representing a binary “1” by alternating positive and negative pulses, and a binary “0” by absence of pulses. |
| <strong>Bit</strong>         | The smallest unit of information in a binary system. Represents either a one or zero (“1” or “0”). |
| <strong>Bit Interleaving/Multiplexing</strong> | A process used in time division multiplexing where individual bits from different lower speed channel sources are combined (one bit from one channel at a time) into one continuous higher speed bit stream. |
| <strong>bps (Bits Per Second)</strong> | A measure of data transmission rate in serial transmission.                                      |
| <strong>Bridge</strong>      | A device interconnecting local area networks at the OSI data link layer, filtering and forwarding frames according to media access control (MAC) addresses. |</p>
<table>
<thead>
<tr>
<th><strong>Broadband</strong></th>
<th>Wideband technology capable of supporting voice, video and data, possibly using multiple channels.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Buffer</strong></td>
<td>A storage device. Commonly used to compensate for differences in data rates or event timing when transmitting from one device to another. Also used to remove jitter.</td>
</tr>
<tr>
<td><strong>Bus</strong></td>
<td>A transmission path or channel. A bus is typically an electrical connection with one or more conductors, where all attached devices receive all transmissions at the same time.</td>
</tr>
<tr>
<td><strong>Byte</strong></td>
<td>A group of bits (normally 8 bits in length).</td>
</tr>
<tr>
<td><strong>Carrier</strong></td>
<td>A continuous signal at a fixed frequency that is capable of being modulated with a second (information carrying) signal.</td>
</tr>
<tr>
<td><strong>Cell</strong></td>
<td>The 53-byte basic information unit within an ATM network. The user traffic is segmented into cells at the source and reassembled at the destination. An ATM cell consists of a 5-byte ATM header and a 48-byte ATM payload, which contains the user data.</td>
</tr>
<tr>
<td><strong>Channel</strong></td>
<td>A path for electrical transmission between two or more points. Also called a link, line, circuit or facility.</td>
</tr>
<tr>
<td><strong>CLI</strong></td>
<td>Command Line Interface (CLI) is a mechanism for interacting with a RAD product by typing commands in response to a prompt.</td>
</tr>
<tr>
<td><strong>Clock</strong></td>
<td>A term for the source(s) of timing signals used in synchronous transmission.</td>
</tr>
<tr>
<td><strong>Congestion</strong></td>
<td>A state in which the network is overloaded and starts to discard user data (frames, cells or packets).</td>
</tr>
<tr>
<td><strong>Data</strong></td>
<td>Information represented in digital form, including voice, text, facsimile and video.</td>
</tr>
<tr>
<td><strong>Data Link Layer</strong></td>
<td>Layer 2 of the OSI model. The entity, which establishes, maintains, and releases data-link connections between elements in a network. Layer 2 is concerned with the transmission of units of information, or frames, and associated error checking.</td>
</tr>
<tr>
<td><strong>Diagnostics</strong></td>
<td>The detection and isolation of a malfunction or mistake in a communications device, network or system.</td>
</tr>
<tr>
<td><strong>Digital</strong></td>
<td>The binary (“1” or “0”) output of a computer or terminal. In data communications, an alternating, non-continuous (pulsating) signal.</td>
</tr>
<tr>
<td><strong>E1 Line</strong></td>
<td>A 2.048 Mbps line, common in Europe, that supports thirty-two 64 kbps channels, each of which can transmit and receive data or digitized voice. The line uses framing and signaling to achieve synchronous and reliable transmission. The most common configurations for E1 lines are E1 PRI, and unchannelized E1.</td>
</tr>
<tr>
<td><strong>E3</strong></td>
<td>The European standard for high speed digital transmission, operating at 34 Mbps.</td>
</tr>
<tr>
<td><strong>Ethernet</strong></td>
<td>A local area network (LAN) technology which has extended into the wide area networks. Ethernet operates at many speeds,</td>
</tr>
</tbody>
</table>
including data rates of 10 Mbps (Ethernet), 100 Mbps (Fast Ethernet), 1,000 Mbps (Gigabit Ethernet), 10 Gbps, 40 Gbps, and 100 Gbps.

<table>
<thead>
<tr>
<th><strong>Ethernet OAM</strong></th>
<th>Ethernet operation, administration and maintenance (OAM) are a set of standardized protocols for measuring and controlling network performance. There are two layers of Ethernet OAM: Service OAM (provides end-to-end connectivity fault management per customer service instance, even in multi-operator networks) and Link or Segment OAM (detailed monitoring and troubleshooting of an individual physical or emulated link).</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Flow Control</strong></td>
<td>A congestion control mechanism that results in an ATM system implementing flow control.</td>
</tr>
<tr>
<td><strong>Frame</strong></td>
<td>A logical grouping of information sent as a link-layer unit over a transmission medium. The terms packet, datagram, segment, and message are also used to describe logical information groupings.</td>
</tr>
<tr>
<td><strong>Framing</strong></td>
<td>At the physical and data link layers of the OSI model, bits are fit into units called frames. Frames contain source and destination information, flags to designate the start and end of the frame, plus information about the integrity of the frame. All other information, such as network protocols and the actual payload of data, is encapsulated in a packet, which is encapsulated in the frame.</td>
</tr>
<tr>
<td><strong>Full Duplex</strong></td>
<td>A circuit or device permitting transmission in two directions (sending and receiving) at the same time.</td>
</tr>
<tr>
<td><strong>FXO (Foreign Exchange Office)</strong></td>
<td>A voice interface, emulating a PBX extension, as it appears to the CO (Central Office) for connecting a PBX extension to a multiplexer.</td>
</tr>
<tr>
<td><strong>FXS (Foreign Exchange Subscriber)</strong></td>
<td>A voice interface, emulating the extension interface of a PBX (or subscriber interface of a CO) for connecting a regular telephone set to a multiplexer.</td>
</tr>
<tr>
<td><strong>G.703</strong></td>
<td>An ITU standard for the physical and electrical characteristics of various digital interfaces, including those at 64 kbps and 2.048 Mbps.</td>
</tr>
<tr>
<td><strong>Gateway</strong></td>
<td>Gateways are points of entrance and exit from a communications network. Viewed as a physical entity, a gateway is that node that translates between two otherwise incompatible networks or network segments. Gateways perform code and protocol conversion to facilitate traffic between data highways of differing architecture.</td>
</tr>
<tr>
<td><strong>GFP (Generic Framing Procedure)</strong></td>
<td>Defined by ITU-T G.7041, generic framing procedure allows efficient mapping of variable length, higher-layer client signals, such as Ethernet, over a transport network like SDH/SONET. Recently, GFP has been extended to lower speed PDH networks.</td>
</tr>
<tr>
<td><strong>Impedance</strong></td>
<td>The combined effect of resistance, inductance and capacitance on a transmitted signal. Impedance varies at different frequencies.</td>
</tr>
<tr>
<td><strong>Interface</strong></td>
<td>A shared boundary, defined by common physical interconnection characteristics, signal characteristics, and meanings of exchanged signals.</td>
</tr>
<tr>
<td><strong>IP Address</strong></td>
<td>Also known as an Internet address. A unique string of numbers that identifies a computer or device on a TCP/IP network. The format of an IP address is a 32-bit numeric address written as four numbers from 0 to 255, separated by periods (for example, 1.0.255.123).</td>
</tr>
<tr>
<td><strong>J1</strong></td>
<td>Digital interconnection protocol similar to T1 and E1 used in Japan.</td>
</tr>
<tr>
<td><strong>Jitter</strong></td>
<td>The deviation of a transmission signal in time or phase. It can introduce errors and loss of synchronization in high speed synchronous communications.</td>
</tr>
<tr>
<td><strong>Laser</strong></td>
<td>A device that transmits an extremely narrow and coherent beam of electromagnetic energy in the visible light spectrum. Used as a light source for fiber optic transmission (generally more expensive, shorter lived, single mode only, for greater distances than LED).</td>
</tr>
<tr>
<td><strong>Latency</strong></td>
<td>The time between initiating a request for data and the beginning of the actual data transfer. Network latency is the delay introduced when a packet is momentarily stored, analyzed and then forwarded.</td>
</tr>
<tr>
<td><strong>Loading</strong></td>
<td>The addition of inductance to a line in order to minimize amplitude distortion. Used commonly on public telephone lines to improve voice quality, it can make the lines impassable to high speed data, and baseband modems.</td>
</tr>
<tr>
<td><strong>Loopback</strong></td>
<td>A type of diagnostic test in which the transmitted signal is returned to the sending device after passing through all or part of a communications link or network.</td>
</tr>
<tr>
<td><strong>MA (Maintenance Association)</strong></td>
<td>See MEG (Maintenance Entity Group).</td>
</tr>
<tr>
<td><strong>Manager</strong></td>
<td>An application that receives Simple Network Management Protocol (SNMP) information from an agent. An agent and manager share a database of information, called the Management Information Base (MIB). An agent can use a message called a traps-PDU to send unsolicited information to the manager. A manager that uses the RADview MIB can query the RAD device, set parameters, sound alarms when certain conditions appear, and perform other administrative tasks.</td>
</tr>
<tr>
<td><strong>Mark</strong></td>
<td>In telecommunications, this means the presence of a signal. A mark is equivalent to a binary 1. A mark is the opposite of a space (0).</td>
</tr>
<tr>
<td><strong>Master Clock</strong></td>
<td>The source of timing signals (or the signals themselves) that all network stations use for synchronization.</td>
</tr>
<tr>
<td><strong>MD (Maintenance Domain)</strong></td>
<td>Maintenance Domains (MDs) are management entities in OAM.</td>
</tr>
<tr>
<td><strong>Domain</strong></td>
<td><strong>Definition</strong></td>
</tr>
<tr>
<td>-----------</td>
<td>---------------</td>
</tr>
<tr>
<td><strong>Metering</strong></td>
<td>This feature is intended for support of payphones, and therefore includes dedicated circuits for the detection of polarity and of 16 kHz or 12 kHz metering pulses.</td>
</tr>
<tr>
<td><strong>ME (Maintenance Entity)</strong></td>
<td>An ME is a maintenance entity as defined by ITU-T Y.1731 that requires management.</td>
</tr>
<tr>
<td><strong>MEG (Maintenance Entity Group)</strong></td>
<td>MEs are grouped into ME groups. For a point-to-point Ethernet connection/S-VLAN, a MEG contains a single ME. For a multipoint Ethernet connection, a MEG contains ( \frac{n(n-1)}{2} ) MEs, where ( n ) is the number of Ethernet connection end points. Each MEG is assigned a unique ID that is used in OAM messages. (MEGs are also referred to as Maintenance Associations or MAs in IEEE language.)</td>
</tr>
<tr>
<td><strong>MEP (Maintenance Entity Group End Point)</strong></td>
<td>MEPs are located at the ends of managed entities. MEPs generate and process OAM frames to monitor and maintain the ME.</td>
</tr>
<tr>
<td><strong>MIP (Maintenance Entity Group Intermediate Point)</strong></td>
<td>A MIP is located at an intermediate point along the end-to-end Ethernet path. It can respond to OAM messages, but cannot originate them.</td>
</tr>
<tr>
<td><strong>Multidrop</strong></td>
<td>A communications configuration in which multiple devices share a common transmission facility (or multipoint line), although generally only one may transmit at a time. Usually used with some kind of polling mechanism to address each connected terminal with a unique address code.</td>
</tr>
<tr>
<td><strong>Multiplexer</strong></td>
<td>At one end of a communications link, a device that combines several lower speed transmission channels into a single high speed channel. A multiplexer at the other end reverses the process. Sometimes called a mux. See Bit Interleaving/Multiplexing.</td>
</tr>
<tr>
<td><strong>Network</strong></td>
<td>(1) An interconnected group of nodes. (2) A series of points, nodes, or stations connected by communications channels; the collection of equipment through which connections are made between data stations.</td>
</tr>
<tr>
<td><strong>Node</strong></td>
<td>A point of interconnection to a network.</td>
</tr>
<tr>
<td><strong>NodeB</strong></td>
<td>The name of the BTS for 3G cellular traffic</td>
</tr>
<tr>
<td><strong>Packet</strong></td>
<td>An ordered group of data and control signals transmitted through a network, as a subset of a larger message.</td>
</tr>
<tr>
<td><strong>Parameters</strong></td>
<td>Parameters are often called arguments, and the two words are used interchangeably. However, some computer languages such as C define argument to mean actual parameter (i.e., the value), and parameter to mean formal parameter. In RAD CLI, parameter means formal parameter, not value.</td>
</tr>
<tr>
<td><strong>Payload</strong></td>
<td>The 48-byte segment of the ATM cell containing user data. Any adaptation of user data via the AAL will take place within the payload.</td>
</tr>
<tr>
<td><strong>Physical Layer</strong></td>
<td>Layer 1 of the OSI model. The layer concerned with electrical, mechanical, and handshaking procedures over the interface connecting a device to the transmission medium.</td>
</tr>
<tr>
<td><strong>Policing</strong></td>
<td>A method for verifying that the incoming VC complies with the user's service contract.</td>
</tr>
<tr>
<td><strong>Polling</strong></td>
<td>See Multidrop.</td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td>The physical interface to a computer or multiplexer, for connection of terminals and modems.</td>
</tr>
<tr>
<td><strong>Prioritization</strong></td>
<td>Also called CoS (class of service), classifies traffic into categories such as high, medium, and low. The lower the priority, the more &quot;drop eligible&quot; is a packet. When the network gets busy, prioritization ensures critical or high-rated traffic is passed first, and packets from the lowest categories may be dropped.</td>
</tr>
<tr>
<td><strong>prompt</strong></td>
<td>One or more characters in a command line interface to indicate that the computer is ready to accept typed input.</td>
</tr>
<tr>
<td><strong>Protocol</strong></td>
<td>A formal set of conventions governing the formatting and relative timing of message exchange between two communicating systems.</td>
</tr>
<tr>
<td><strong>RADIUS (Remote Authentication Dial-In User Service)</strong></td>
<td>An authentication, authorization and accounting protocol for applications such as network access or IP mobility. Many network services require the presentation of security credentials (such as a username and password or security certificate) in order to connect to the network. Before access to the network is granted, this information is passed to a network access server (NAS) device over the link-layer protocol, then to a RADIUS server over the RADIUS protocol. The RADIUS server checks that the information is correct using authentication schemes like PAP, CHAP or EAP.</td>
</tr>
<tr>
<td><strong>Router</strong></td>
<td>An interconnection device that connects individual LANs. Unlike bridges, which logically connect at OSI Layer 2, routers provide logical paths at OSI Layer 3. Like bridges, remote sites can be connected using routers over dedicated or switched lines to create WANs.</td>
</tr>
<tr>
<td><strong>Routing</strong></td>
<td>The process of selecting the most efficient circuit path for a message.</td>
</tr>
<tr>
<td><strong>Scalable</strong></td>
<td>Able to be changed in size or configuration to suit changing conditions. For example, a scalable network can be expanded from a few nodes to thousands of nodes.</td>
</tr>
<tr>
<td><strong>Serial Transmission</strong></td>
<td>A common mode of transmission, where the character bits are sent sequentially one at a time instead of in parallel.</td>
</tr>
<tr>
<td><strong>Single Mode</strong></td>
<td>Describing an optical wave-guide or fiber that is designed to propagate light of only a single wavelength (typically 5-10 microns</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>SONET (Synchronous Optical Network)</strong></td>
<td>A North American standard for using optical media as the physical transport for high speed long-haul networks. SONET basic speeds start at 51.84 Mbps and go up to 2.5 Gbps.</td>
</tr>
<tr>
<td><strong>Space</strong></td>
<td>In telecommunications, the absence of a signal. Equivalent to a binary 0.</td>
</tr>
<tr>
<td><strong>SSH (Secure Shell)</strong></td>
<td>A network protocol that allows data to be exchanged over a secure channel between two computers. Encryption provides confidentiality and integrity of data.</td>
</tr>
<tr>
<td><strong>Sync</strong></td>
<td>See <em>Synchronous Transmission</em>.</td>
</tr>
<tr>
<td><strong>Synchronous Transmission</strong></td>
<td>Transmission in which data bits are sent at a fixed rate, with the transmitter and receiver synchronized.</td>
</tr>
<tr>
<td><strong>T1</strong></td>
<td>A digital transmission link with a capacity of 1.544 Mbps used in North America. Typically channelized into 24 DS0s, each capable of carrying a single voice conversation or data stream. Uses two pairs of twisted pair wires.</td>
</tr>
<tr>
<td><strong>T3</strong></td>
<td>A digital transmission link with a capacity of 45 Mbps, or 28 T1 lines.</td>
</tr>
<tr>
<td><strong>Telnet</strong></td>
<td>The virtual terminal protocol in the Internet suite of protocols. It lets users on one host access another host and work as terminal users of that remote host. Instead of dialing into the computer, the user connects to it over the Internet using Telnet. When issuing a Telnet session, it connects to the Telnet host and logs in. The connection enables the user to work with the remote machine as though a terminal was connected to it.</td>
</tr>
<tr>
<td><strong>Throughput</strong></td>
<td>The amount of information transferred through the network between two users in a given period, usually measured in the number of packets per second (pps).</td>
</tr>
<tr>
<td><strong>Timeslot</strong></td>
<td>A portion of a serial multiplex of timeslot information dedicated to a single channel. In E1 and T1, one timeslot typically represents one 64 kbps channel.</td>
</tr>
<tr>
<td><strong>Traffic Shaping</strong></td>
<td>A method for smoothing the bursty traffic rate that might arrive on an access virtual circuit so as to present a more uniform traffic rate on the network.</td>
</tr>
</tbody>
</table>
Quick Start Guide

This section describes the minimum configuration needed to prepare ETX-203A for operation.

1. Installing the Unit

Perform the following steps to install the unit:
1. Determine the required configuration of ETX-203A, according to your application.
2. Connect the user/network ports as required for the application.
3. Connect the ASCII terminal to the RS-232 control port.
4. Connect power to the unit.

Connecting the Interfaces

➢ To connect the interfaces:
   1. Insert the SFP modules (if applicable) into the relevant SFP-based Ethernet ports.
   2. Connect the optical cables.
   3. Connect the network port(s) to the service provider network equipment.
   4. Connect the user port(s) to the customer network equipment.

Note

• The number of available Ethernet ports depends on the options you purchased.
• Lock the wire latch of each SFP module by lifting it up until it clicks into place.
  For additional information, refer to Chapter 2.

Connecting to a Terminal

➢ To connect the unit to a terminal:
   1. Connect the male RJ-45 connector of the cable supplied by RAD to the unit's 8-pin connector, designated CONTROL.
   2. Connect the other side of the cable to the ASCII terminal equipment.
Connecting the Power

The unit can be connected to AC or DC power, depending on what you ordered.

► To connect to AC power:
1. Connect the power cable to the AC power connector on the unit’s front panel.
2. Connect the power cable to mains outlet.

   The unit turns on automatically upon connection to the mains, and the PWR indicator lights up.

► To connect to DC power:
• For instructions on wiring the DC adapters, refer to the DC Power Supply Terminal Block Connection supplement at the end of this manual.

2. Configuring the Unit for Management

Configure ETX-203A for management, using a local ASCII-based terminal.

Starting a Terminal Session for the First Time

► To start the terminal session:
1. Connect an ASCII terminal to the CONTROL port.
2. Configure the ASCII terminal to the settings listed below and then set the terminal emulator to VT100 emulation for optimal view of system menus.
   ▪ Data Rate: 9,600 bps
   ▪ Data bits: 8
   ▪ Parity: None
   ▪ Stop bits: 1
   ▪ Flow control: None.
3. If you are using HyperTerminal, set the terminal mode to 132-column mode for optimal view of system menus (Properties > Settings > Terminal Setup > 132 column mode).
4. Power-up ETX-203A.
5. ETX-203A boots up. When the startup process is completed, you are prompted to press <ENTER> to receive the login prompt.
6. Press <ENTER> until you receive the login prompt.
7. To log in, enter your user name (su for full configuration and monitoring access) and your password.
8. The device prompt appears:

   ETX-203A#
You can now type the necessary CLI commands.

**Configuring the Host Parameters**

By default, DHCP is enabled. When ETX-203A boots up, it acquires an IP address from a DHCP server if one is available. If you are not working with DHCP, you need to disable DHCP and set the IP address manually.

This section provides an example of disabling DHCP and assigning the following host parameters:

- ETX-203A unit – IP address 192.178.1.175 with mask 255.255.255.0
- Default gateway – IP address 192.178.1.1.

To disable DHCP and set the IP address parameters:

- Enter the following commands:

```plaintext
configure management host 1
no dhcp
ip-address 192.178.1.175/24
default-gateway 192.178.1.1
exit all
```

**Adding Network Managers**

To add a manager to the manager list, use the following procedure. The example uses 192.178.1.4 as the manager IP address.

To add a network manager:

1. Enter the following command:

```plaintext
configure management manager 192.178.1.4/32
```

   The management station is added to the manager list, and the `config>mngmnt>manager(192.178.1.4/32)#` prompt is displayed.

2. If you want to prevent traps from being sent to the manager, enter the following command to mask traps:

```plaintext
trap-mask
```

3. Type `exit all` to return to the device prompt.

**Configuring Management Flows**

You need to define management flows to and from the host in order to be able to manage the unit.

This section provides an example of configuring management flows for out-of-band management via the Ethernet management port, tagged with management VLAN 105.

You need to set up the following flows:

- The flow to the host forwards frames from the management VLAN...
• The flow from the host forwards all frames, adding the management VLAN and priority.

➤ To configure the flow to the host:

1. Type the following commands to set up a classifier profile to forward frames from VLAN 105:

```plaintext
configure flows
classifier-profile v105 match-any
match vlan 105
exit all
```

2. Type the following commands to set up a flow using the previously defined classifier profile, with ingress at the Ethernet management port and egress at the host:

```plaintext
configure flows flow fh_in
no policer
classifier v105
ingress-port ethernet 101
egress-port host queue 1
no shutdown
exit all
```

➤ To configure the flow from the host:

1. Type the following commands to set up a classifier profile to forward all frames:

```plaintext
configure flows
classifier-profile mng_all match-any
match all
exit all
```

2. Type the following commands to set up a flow using the previously defined classifier profile, with ingress at the host and egress at the Ethernet management port, and pushing VLAN 105 with p-bit 6:

```plaintext
configure flows flow fh_out
classifier mng_all
ingress-port host
egress-port ethernet 101
vlan-tag push vlan 105 p-bit fixed 6
no shutdown
exit all
```

3. Saving Management Configuration

Saving Configuration

Type `save` in any level to save your configuration in `startup-config`. 
Copying User Configuration to Default Configuration

In addition to saving your configuration in `startup-config`, you may also wish to save your configuration as a user default configuration.

➢ To save user default configuration:
  • Enter the following commands:

```plaintext
exit all
file copy startup-config user-default-config
```

4. Verifying Connectivity

At the network manager station or the ASCII terminal, ping the IP address assigned to ETX-203A and verify that replies are received. If there is no reply to the ping, check your configuration and make the necessary corrections.
Contents

Chapter 1. Introduction
1.1 Overview ........................................................................................................... 1-1
   Product Options .................................................................................................. 1-1
   Applications ....................................................................................................... 1-2
   Features ........................................................................................................... 1-2
      Service Types ................................................................................................. 1-2
      Service Level Agreement (SLA) Monitoring .................................................. 1-3
      Flow Classification ......................................................................................... 1-3
      Tagging and Marking ...................................................................................... 1-4
      Quality of Service (QoS) ............................................................................... 1-4
      Traffic Prioritization ....................................................................................... 1-4
      Queue Mapping and Marking ......................................................................... 1-5
      Hierarchical Scheduling and Shaping Per Flow ............................................. 1-5
      Ethernet OAM ............................................................................................... 1-6
      RFC-2544 Testing and Analysis ...................................................................... 1-6
      Jumbo Frames and Egress MTU ..................................................................... 1-6
      Link Redundancy ............................................................................................ 1-6
      Ethernet Linear Protection ............................................................................ 1-6
      L2CP Handling ............................................................................................... 1-7
      Fault Propagation .......................................................................................... 1-7
      Smart SFPs .................................................................................................... 1-7
      Management .................................................................................................. 1-7
      DHCP Client ................................................................................................. 1-8
      SFTP .............................................................................................................. 1-8
      Statistics Collection ....................................................................................... 1-8
      Network Time Protocol .................................................................................. 1-9
      Diagnostic Tools ............................................................................................ 1-9

1.2 New in This Version ......................................................................................... 1-10
1.3 Physical Description ....................................................................................... 1-11
1.4 Functional Description .................................................................................... 1-11
1.5 Technical Specifications .................................................................................. 1-13

Chapter 2. Installation and Setup
2.1 Site Requirements and Prerequisites ................................................................. 2-1
2.2 Package Contents ............................................................................................ 2-1
2.3 Mounting the Unit ........................................................................................... 2-2
2.4 Installing SFP Modules ................................................................................... 2-2
2.5 Connecting to Ethernet Equipment ................................................................. 2-3
2.6 Connecting to a Terminal ............................................................................... 2-4
2.7 Connecting to Management Station ............................................................... 2-5
2.8 Connecting to Power ....................................................................................... 2-6
   Connecting to AC Power ................................................................................. 2-6
   Connecting to DC Power ................................................................................ 2-6

Chapter 3. Operation
3.1 Turning On the Unit ........................................................................................ 3-1
3.2 Indicators ........................................................................................................ 3-2
3.3 Startup ............................................................................................................ 3-2
5.1 Services ............................................................................................................. 5-2
  Ethernet Management Traffic .............................................................................. 5-2
  Ethernet to Host .................................................................................................. 5-2
  Host to Ethernet ................................................................................................. 5-3
  Ethernet User Traffic .......................................................................................... 5-5
  Network to User .................................................................................................. 5-5
  User to Network .................................................................................................. 5-6
  TDM User Traffic ............................................................................................... 5-8
  TDM Network to Ethernet User .......................................................................... 5-8
  TDM User to Network ........................................................................................... 5-11
5.2 Configuring the Host IP Settings ...................................................................... 5-14
  Working with DHCP ............................................................................................. 5-14
  Disabling DHCP .................................................................................................. 5-15
  Enabling DHCP .................................................................................................... 5-15
  Setting Host IP Parameters .................................................................................. 5-15
5.3 Configuring Device Information ........................................................................ 5-16
  Example ................................................................................................................ 5-17
5.4 SNMP Management ............................................................................................ 5-17
  Standards ............................................................................................................. 5-18
  Benefits ............................................................................................................... 5-18
  Functional Description ......................................................................................... 5-19
  Factory Defaults ................................................................................................... 5-19
  Enabling or Disabling SNMPv3 .......................................................................... 5-19
  Setting SNMP Communities ................................................................................. 5-19
  SNMPv3 Default Configuration .......................................................................... 5-20
  Configuring SNMPv3 Parameters ....................................................................... 5-21
  Example ................................................................................................................ 5-25
5.5 Network Managers ............................................................................................. 5-29
  Factory Defaults ................................................................................................... 5-29
  Configuring Management Subnets ....................................................................... 5-29
  Examples .............................................................................................................. 5-29
  Configuring Network Manager Stations ................................................................ 5-30
  Example ................................................................................................................ 5-31
5.6 Controlling Management Access ........................................................................ 5-31
  Factory Defaults ................................................................................................... 5-31
  Configuring Management Access ......................................................................... 5-31
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.7 Access Policy</td>
<td>5-32</td>
</tr>
<tr>
<td>Factory Defaults</td>
<td>5-32</td>
</tr>
<tr>
<td>Configuring Access Policy</td>
<td>5-32</td>
</tr>
<tr>
<td>5.8 Authentication via RADIUS Server</td>
<td>5-33</td>
</tr>
<tr>
<td>Standards</td>
<td>5-33</td>
</tr>
<tr>
<td>Benefits</td>
<td>5-33</td>
</tr>
<tr>
<td>Functional Description</td>
<td>5-33</td>
</tr>
<tr>
<td>Factory Defaults</td>
<td>5-34</td>
</tr>
<tr>
<td>Configuring RADIUS Parameters</td>
<td>5-34</td>
</tr>
<tr>
<td>Displaying RADIUS Statistics</td>
<td>5-35</td>
</tr>
<tr>
<td>5.9 Authentication via TACACS+ Server</td>
<td>5-35</td>
</tr>
<tr>
<td>Standards</td>
<td>5-35</td>
</tr>
<tr>
<td>Benefits</td>
<td>5-35</td>
</tr>
<tr>
<td>Functional Description</td>
<td>5-35</td>
</tr>
<tr>
<td>Factory Defaults</td>
<td>5-36</td>
</tr>
<tr>
<td>Configuring TACACS+ Parameters</td>
<td>5-36</td>
</tr>
<tr>
<td>5.10 Terminal Control Port</td>
<td>5-37</td>
</tr>
<tr>
<td>Factory Defaults</td>
<td>5-37</td>
</tr>
<tr>
<td>Configuring Control Port Parameters</td>
<td>5-37</td>
</tr>
<tr>
<td>5.11 User Access</td>
<td>5-37</td>
</tr>
<tr>
<td>Factory Defaults</td>
<td>5-38</td>
</tr>
<tr>
<td>Example – Defining Users</td>
<td>5-38</td>
</tr>
<tr>
<td>Example – Displaying Users</td>
<td>5-40</td>
</tr>
<tr>
<td>5.12 Layer 2 Control Processing</td>
<td>5-40</td>
</tr>
<tr>
<td>Standards</td>
<td>5-40</td>
</tr>
<tr>
<td>Benefits</td>
<td>5-40</td>
</tr>
<tr>
<td>Factory Defaults</td>
<td>5-40</td>
</tr>
<tr>
<td>Adding Layer 2 Control Processing Profiles</td>
<td>5-40</td>
</tr>
<tr>
<td>Deleting Layer 2 Control Processing Profiles</td>
<td>5-41</td>
</tr>
<tr>
<td>Configuring Layer 2 Control Processing Profile Parameters</td>
<td>5-41</td>
</tr>
<tr>
<td>Example</td>
<td>5-42</td>
</tr>
<tr>
<td>5.13 Ethernet Ports</td>
<td>5-43</td>
</tr>
<tr>
<td>Configuring Ethernet Port Parameters</td>
<td>5-44</td>
</tr>
<tr>
<td>Setting Second Network Interface as Network or User Port</td>
<td>5-45</td>
</tr>
<tr>
<td>Example</td>
<td>5-46</td>
</tr>
<tr>
<td>Displaying Ethernet Port Status</td>
<td>5-46</td>
</tr>
<tr>
<td>Examples</td>
<td>5-46</td>
</tr>
<tr>
<td>Testing Ethernet Ports</td>
<td>5-47</td>
</tr>
<tr>
<td>Example</td>
<td>5-48</td>
</tr>
<tr>
<td>Displaying Ethernet Port Statistics</td>
<td>5-48</td>
</tr>
<tr>
<td>Setting Sampling Interval for Port Statistics</td>
<td>5-48</td>
</tr>
<tr>
<td>Displaying Port Statistics</td>
<td>5-48</td>
</tr>
<tr>
<td>Example</td>
<td>5-49</td>
</tr>
<tr>
<td>Displaying Layer-2 Control Processing Statistics</td>
<td>5-50</td>
</tr>
<tr>
<td>Example</td>
<td>5-51</td>
</tr>
<tr>
<td>Clearing Statistics</td>
<td>5-51</td>
</tr>
<tr>
<td>5.14 Smart SFPs</td>
<td>5-51</td>
</tr>
<tr>
<td>Benefits</td>
<td>5-52</td>
</tr>
<tr>
<td>Factory Defaults</td>
<td>5-52</td>
</tr>
<tr>
<td>Configuring Smart SFPs</td>
<td>5-52</td>
</tr>
<tr>
<td>Example</td>
<td>5-52</td>
</tr>
<tr>
<td>5.15 E1 Ports</td>
<td>5-54</td>
</tr>
<tr>
<td>Standards and MIBs</td>
<td>5-54</td>
</tr>
<tr>
<td>Benefits</td>
<td>5-54</td>
</tr>
<tr>
<td>Section</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>5.16 T1 Ports</td>
<td>Standards and MIBs</td>
</tr>
<tr>
<td>5.17 E3 Ports</td>
<td>Standards and MIBs</td>
</tr>
<tr>
<td>5.18 T3 Ports</td>
<td>Standards and MIBs</td>
</tr>
<tr>
<td>5.19 SDH/SONET Ports</td>
<td>Standards and MIBs</td>
</tr>
<tr>
<td>5.20 GFP Ports</td>
<td>Standards and MIBs</td>
</tr>
<tr>
<td>5.21 Logical MAC Ports</td>
<td>Standards and MIBs</td>
</tr>
<tr>
<td>5.22 Network Interface Redundancy</td>
<td>Standards and MIBs</td>
</tr>
<tr>
<td>5.23 Ethernet Linear Protection</td>
<td>Standards</td>
</tr>
</tbody>
</table>
## 5.24 Service Virtual Interface
- Configuring Service Virtual Interfaces .............................................. 5-86

## 5.25 Quality of Service (QoS)
- Standards ........................................................................................... 5-86
- Benefits ................................................................................................ 5-86
- Factory Defaults .................................................................................. 5-86
- Functional Description ........................................................................ 5-87
- Queue Mapping Profiles ...................................................................... 5-87
  - Factory Defaults ............................................................................ 5-87
  - Adding Queue Mapping Profiles ................................................. 5-88
  - Configuring Queue Mappings ....................................................... 5-89
  - Examples .......................................................................................... 5-89
- CoS Mapping Profiles ........................................................................ 5-91
  - Factory Defaults ............................................................................ 5-91
  - Configuring CoS Mapping Profiles ............................................. 5-91
  - Example ............................................................................................ 5-92
- Marking Profiles .................................................................................. 5-92
  - Factory Defaults ............................................................................ 5-92
  - Configuring Marking Profiles ....................................................... 5-93
  - Example ............................................................................................ 5-94
- Bandwidth Profiles ............................................................................... 5-95
  - Factory Defaults ............................................................................ 5-96
  - Configuring Shaper Profiles ........................................................ 5-96
  - Configuring Policer Profiles ........................................................ 5-97
  - Configuring Policer Aggregates ..................................................... 5-99
- Queue Block Profiles ........................................................................... 5-100
  - Factory Defaults ............................................................................ 5-100
  - Adding Queue Block Profiles ..................................................... 5-101
  - Configuring Queue Block Profile Parameters .................................. 5-101
  - Example ............................................................................................ 5-101
- Queue Group Profiles .......................................................................... 5-102
  - Adding Queue Group Profiles ..................................................... 5-102
  - Configuring Queue Group Parameters ....................................... 5-102
  - Example ............................................................................................ 5-103
- WRED Profiles .................................................................................... 5-104
  - Factory Defaults ............................................................................ 5-104
  - Configuring WRED Profiles ......................................................... 5-105
  - Example ............................................................................................ 5-105

## 5.26 Flows
- Standards ............................................................................................. 5-105
- Benefits ................................................................................................ 5-106
- Functional Description ......................................................................... 5-106
- Factory Defaults .................................................................................. 5-106
- Defining Classifier Profiles ............................................................... 5-113
  - Examples .......................................................................................... 5-114
- Configuring Flows ............................................................................... 5-114
Table of Contents

5.31 Administration

ETX-203A Ver. 3.0
Chapter 6. Monitoring and Diagnostics

6.1 Detecting Problems ................................................................. 6-1
   LEDs ................................................................................. 6-1
   Alarms and Traps .............................................................. 6-1
   Statistic Counters ............................................................ 6-1

6.2 Handling Events ..................................................................... 6-2
   Working with the Event Log ............................................... 6-2
   Working with Traps ........................................................... 6-5
   Setting the Trap Delay ........................................................ 6-6
   Masking Traps .................................................................. 6-6
   Working with Trap Synchronization .................................... 6-7

6.3 Troubleshooting .................................................................... 6-10
   Troubleshooting Chart ....................................................... 6-10

6.4 Performing Diagnostic Tests .................................................... 6-11
   RFC-2544 Testing ............................................................... 6-11
   Standards .......................................................................... 6-11
   Benefits ............................................................................. 6-11
   Functional Description ...................................................... 6-12
   Factory Defaults ............................................................... 6-12
   Performing Tests .............................................................. 6-13
   Running a Ping Test ........................................................... 6-14
   Tracing the Route .............................................................. 6-14

6.5 Frequently Asked Questions .................................................... 6-16
6.6 Technical Support ........................................................................................................6-16

Chapter 7. Software Upgrade

7.1 Impact ............................................................................................................................7-1
7.2 Software Upgrade Options ..........................................................................................7-2
7.3 Prerequisites ..................................................................................................................7-2
7.4 Upgrading the Device Software via CLI .....................................................................7-2
    Verifying the Host Parameters ......................................................................................7-3
    Pinging the PC ..............................................................................................................7-3
    Activating the SFTP Server ..........................................................................................7-3
    Activating the TFTP Server ..........................................................................................7-4
    Downloading the Software ...........................................................................................7-4
7.5 Upgrading the Device Software via the Boot Menu .....................................................7-4
    Accessing the Boot Menu ............................................................................................7-5
    Using the XMODEM Protocol .......................................................................................7-6
    Using TFTP ..................................................................................................................7-7
7.6 Verifying Upgrade Results ...........................................................................................7-8

Appendix A. Connection Data

Appendix B. Operation, Administration, and Maintenance (OAM)
Chapter 1

Introduction

1.1 Overview

ETX-203A is a carrier Ethernet demarcation device owned and operated by the service provider and installed at the customer premises, delivering SLA-based Ethernet business services to the customer premises over native Ethernet access. It serves as a clear demarcation point between the user and operator networks. The device delivers Ethernet E-line services (EPL and EVPL) and is MEF 9 and MEF 14 certified.

Incoming customer traffic is classified and mapped according to port-based (all-in-one) bundling or by user port and CE VLAN-ID, VLAN priority, DSCP, IP precedence, MAC, IP address, and Ethertype. This offers operators the flexibility to differentiate services using different kinds of classification methods, police the traffic, and enforce SLA per service.

ETX-203A supports powerful bandwidth profiles such as CIR/CBS and EIR/EBS for differentiated Ethernet services and includes comprehensive Ethernet OAM (Operation, Administration, and Maintenance) functionality together with SLA monitoring.

The SFP-based interfaces accommodate a wide range of Fast Ethernet and Gigabit Ethernet SFP transceivers, allowing service providers to seamlessly connect customers located at different distances from the device.

The network ports support 1:1 or LAG link aggregation. At the physical layer, ETX-203A supports autonegotiation and fault propagation.

The unit can be managed via a local terminal port, via a dedicated out-of-band Ethernet port, or via a user or network port.

Product Options

Several versions of the unit are available, offering different combinations of Ethernet ports and enclosures. The basic port type is Fast Ethernet, which can be optionally increased to Gigabit Ethernet.

- **Network ports** – Up to two SFP-based fiber optic or electrical, depending on whether port 2 is configured as network or user port.

- **User ports** – Up to two SFP-based fiber optic or electrical, or three if port 2 is configured as user port.

- **Enclosure** – Plastic, 8.4”. For the allowed storage and operating temperature range, refer to *Technical Specifications*. 
Applications

ETX-203A delivers Ethernet services as defined by the MEF standards.

![Figure 1-1. EPL Service](image1)

![Figure 1-2. EVPL Service](image2)

Features

Service Types

ETX-203A provides port- and flow-based services.

Port-Based Service

In a typical port-based (all-to-one bundling) application ETX-203A receives different services via different user ports (Figure 1-3). This method achieves clearer service separation, it does not require any marking for CoS, and provides straightforward SLA measurement.

![Figure 1-3. Port-Based Service](image3)

Flow-Based Service

In a typical flow-based application different services are assigned to different Ethernet flows received by the same user port (Figure 1-4). This provides a
cheaper, more scalable solution, with a possibility of mixing different service types.

![Flow-Based Service](image)

**Figure 1-4. Flow-Based Service**

**Service Level Agreement (SLA) Monitoring**

ETX-203A is an effective tool for measuring the Service Level Agreement parameters, such as Frame Delay, Frame Delay Variance (jitter), Frame Loss and Availability.

**Flow Classification**

The ingress user traffic is mapped to the Ethernet flows using the following list of per-port classification criteria. In the classifications, VLAN refers to the service provider (outer) VLAN, previously referred to as SP-VLAN, while inner VLAN refers to the Customer Entity VLAN, previously referred to as CE-VLAN.

- Port-based (All to one bundling)
- VLAN
- VLAN + VLAN priority
- VLAN + IP precedence
- VLAN + DSCP
- VLAN + source/destination MAC
- VLAN + source/destination IP address
- VLAN + inner VLAN
- VLAN + VLAN priority + inner VLAN
- VLAN + non-IP
- VLAN + Ethertype
- VLAN priority
- IP precedence
- DSCP
- Source/destination MAC
- Source/destination IP address
- Non-IP
- Ether Type
- Untagged.
ETX-203A supports up to 192 Ethernet flows. Flows are unidirectional.

**Tagging and Marking**

ETX-203A supports several options for marking and tagging.

You can perform the following marking actions:

- Overwrite inner or outer VLAN with a new value
- Overwrite inner or outer VLAN p-bit with a new value.

You can perform the following tagging actions:

- Add (push) outer VLAN, with p-bit value that can be copied from the original value or set to a new value. When you add a new VLAN, the original outer VLAN becomes the inner VLAN.
- Remove (pop) outer VLAN and p-bit. When you remove a VLAN, the inner VLAN becomes the outer VLAN.
- Add (push) inner VLAN, with p-bit value that can be copied from the original value or set to a new value.
- Remove (pop) inner VLAN and p-bit.

Only certain combinations of actions on the outer and inner VLAN are allowed. Refer to Chapter 5 for details on the permitted combinations of actions.

**Quality of Service (QoS)**

Different service types require different levels of QoS to be provided end-to-end. QoS can be defined per subscriber as well as per flow. QoS has three aspects: rate limitation, traffic shaping, and traffic prioritization.

A single policer can be applied per flow, or a policer aggregate can be applied to a group of flows. The policers operate according to the dual token bucket mechanism (CIR+CBS, EIR+EBS). A special mechanism compensates for Layer 1 headers. Traffic can be limited to the line rate or the data rate.

In addition, ETX-203A features unique p-bit re-marking capabilities that assign color-specific p-bit values to Ethernet frames at network ingress to ensure metering continuity across the Metro Ethernet network. User traffic that was marked “yellow” according to the CIR/EIR parameters by the device QoS engine is assigned a new p-bit value to signal its status and priority, so that it is dropped first by 802.1Q and 802.1ad network elements in the event of congestion. This is especially useful in color-blind as well as color-aware networks with no “discard eligible“ (“yellow”) marking.

As well as assigning color-specific p-bit values, the Drop Eligible Indicator (DEI) bit in the Ethernet frames can be used to indicate that frames marked “yellow” are eligible for dropping, while frames marked “green” are not eligible for dropping.

**Traffic Prioritization**

Once traffic is classified to a flow, it can be mapped to Strict (Strict Priority) queues or WFQ (Weighted Fair Queues):
- **Strict.** The data flow set to the highest priority is transmitted first. If this data flow stops, all tasks at lower priorities move up by one priority level. For example, the data flow set to the second-highest priority is then transmitted at the highest priority.

- **WFQ.** Allows different scheduling priorities to statistically multiplex data flows with different shares on the service. Each data flow has a separate FIFO queue. A link transmitting at a data rate $R$, all non-empty data flows $N$ are served simultaneously according to the assigned share $w$, each at an average rate of $R/(w_1 + w_2 + w_3 + \ldots + w_N)$. If one data flow stops, the remaining data flows each receive a larger share $w$.

The WRED mechanism ensures that queues are not congested and high-priority traffic is maintained. Each queue is assigned a WRED profile for which you can configure the thresholds and probability to suit your needs.

**Queue Structure**

Level 0 contains up to 31 queue blocks. Each block has eight queues and its own scheduling (Strict and WFQ). For each queue block in level 0, there is a queue in level 1 that represents the scheduling between the queue blocks in level 0. Flows can be bound to each queue block in level 0.

**Queue Mapping and Marking**

The queue mapping functionality associates the user priorities with queue numbers (CoS).

The marking functionality maps the user priority to the SP priority, according to p-bit/DSCP/IP precedence. The marking can also be done according to color (green and/or yellow) in addition to user priority.

The queue mapping and marking functionality is bound to each flow. For every port, a queue mapping can be done for one type of user priority classification.
Hierarchical Scheduling and Shaping Per Flow

Every flow has its own queues and scheduler. ETX-203A supports up to 31 queue blocks per queue group. There are up to 31 available queues for the network ports and eight available queues for the user ports. Flows that are in the direction user port to network port can be bound to one of up to 31 queues, and flows that are in the direction network port to user port can be bound to one of eight queues.

Ethernet OAM

Featuring ultra-fast, hardware-based processing capabilities, ETX-203A performs OAM and PM measurements in under 1 microsecond with maximum precision. ETX-203A provides OAM to monitor and troubleshoot an Ethernet network and quickly detect failures:

- CFM OAM (End-to-end OAM) based on IEEE 802.1ag-D8 and Y.1731 for continuity check, non-intrusive loopback, and performance management.
- EFM OAM (Link OAM) according to IEEE 802.3-2005 (formerly IEEE 802.3ah) for remote management and fault indication, including remote loopback, dying gasp, and MIB parameter retrieval.

RFC-2544 Testing and Analysis

ETX-203A provides BERT testing based on RFC-2544:

- Throughput test – Until binary search convergence
- Packet loss rate – 10% steps
- Latency – Roundtrip frame latency.

Jumbo Frames and Egress MTU

ETX-203A supports large frames of up to 12 Kbytes. The egress MTU can be defined per port.

Link Redundancy

The unit features network link redundancy in a LAG architecture that supports the LACP protocol according to 802.3-2005. Dual homing technology in a 1:1 architecture allows ETX-203A to be connected to two different upstream devices. Link redundancy is available if two ports are configured as network ports.

Ethernet Linear Protection

The device offers protection switching in the following modes for network ports per ITU-T G.8031:

- 1:1
- Unidirectional
- Using APS messages.
The protection functions for the following topologies:

- EVC protection with one fiber — Both EVCs running on same fiber
- EVC protection with two fibers — Each path on different fiber (dual link)
- EVC protection with dual fiber working with MC-LACP to dual PE.

**L2CP Handling**

ETX-203A can be configured to pass through Layer-2 control frames (including other vendors’ L2CP frames) across the network, to peer-supported protocols (IEEE 802.3-2005), or to discard L2CP frames.

**Fault Propagation**

The unit provides the following types of fault propagation:

- Network-to-user fault propagation mechanism on the port and OAM CFM levels – When fault propagation is enabled, the user port shuts itself down or an OAM CFM indication of failure is sent when a link failure is detected at the network port or when an OAM CFM indication of failure is received.

- User-to-network fault propagation mechanism on the port and OAM CFM levels – When fault propagation is enabled, the network port shuts itself down or an OAM CFM indication of failure is sent when a link failure is detected at the user port or an OAM CFM indication of failure is received.

![Figure 1-6. Fault Propagation](image)

**Smart SFPs**

Smart SFPs can be used to provide a full duplex 100/1000 Ethernet remote bridge over E1/T1/E3/T3, or STM-1/OC-3. The following MiRICi devices are supported, with integrated configuration and management:

- MiRICi-E1
- MiRICi-T1
- MiRICi-E3
- MiRICi-T3
- MiRICi-155.

**Management**

ETX-203A can be managed as follows:

- Local management via ASCII terminal connected to the V.24/RS-232 DCE control port.
- Local management via dedicated out of band (OOB) management port.
- Remote management via a network or user port using Telnet SSH or an SNMP-based management system. ETX-203A supports the SNMP version 3 entity, providing secure access to the device by authenticating and encrypting packets transmitted over the network.

Management can be performed by creating a flow to/from the host port, thus enabling QoS on the management traffic. Management can be configured to use untagged or tagged frames.

**Command Line Interface**

You can create data bases and scripts of commonly used commands and easily apply them to multiple units in your infrastructure using RAD's new command line interface.

**Security**

To ensure client-server communication privacy and correct user authentication, ETX-203A supports the security protocols listed below:

- SNMPv3
- RADIUS (client authentication)
- TACACS+ (client authentication)
- SSH for Secure Shell communication session.

**Syslog**

The syslog protocol is a client/server-type protocol, featuring a standard for forwarding log messages in an IP network and supports up to four syslog servers at present. A syslog sender sends a small text message of less than 1024 bytes to the syslog receiver. Syslog messages are sent via UDP in cleartext.

**DHCP Client**

When enabled, the DHCP client of ETX-203A requests an IP address, IP mask, and default gateway from the DHCP server.

**SFTP**

SFTP (Secure File Transfer Protocol) is supported, to provide secure encrypted file transfer using SSH.

**Statistics Collection**

ETX-203A collects performance statistics for the physical layers of the network/user ports, Ethernet flows, OAM CFM, and Radius.

In addition, ETX-203A provides Rmon Statistics based on RFC 2819. In this scenario, ETX-203A can send reports when one of the defined counters rises above or drops below specified thresholds within the sampling period of time. These reports can be sent as SNMP traps to defined network management stations and/or written to the event log.
Network Time Protocol

The Network Time Protocol (NTP) provides the means of synchronizing all managed elements across the network to a reliable clock source provided by multiple servers. ETX-203A supports the client side of NTP v.3 (RFC 1305).

Diagnostic Tools

ETX-203A offers several types of diagnostic procedures:

- Ping test – Check IP connectivity by pinging remote IP hosts.
- Trace route – Quickly trace a route from ETX-203A to any other network device
- Loopback tests:
  - Layer-1 loopback performed at the PHY of the physical ports. When the loopback is active the data forwarded to a port is looped from the Tx path to the Rx path, disrupting the traffic. This loopback cannot pass through Ethernet bridges.
  - Layer-2/Layer-3 loopback on flows with optional MAC and/or IP address swapping. When the loopback is active, ETX-203A can exchange the source and destination MAC/IP addresses of the incoming packets. This loopback passes through Ethernet bridges and routers, and does not disrupt traffic flows that are not being tested.
1.2 New in This Version

The following features have been added for Version 3.0:

- Hardware-based OAM, with MIP functionality
- RFC-2544 testing and analysis
- Ethernet linear protection on the network ports (G.8031) via EVC Termination Point (ETP)
- Smart SFP (MiRIC/MiRICi) support
- CoS mapping profiles
- TACACS+ authentication.
1.3 Physical Description

*Figure 1-7* shows a 3D view of the front and back of ETX-203A.

The LEDs are located on the front panel, and the network and user Ethernet ports are located on the rear panel. The ETX-203A interface connections are described in greater detail in *Chapter 2*.

![3D View of ETX-203A](image)

*Figure 1-7. 3D View of ETX-203A*

1.4 Functional Description

*Figure 1-8* shows the data flow in the device. *Table 1-1* provides an overview of the traffic handling stages.
**Figure 1-8. Data Flow**

**Table 1-1. Traffic Handling Stages**

<table>
<thead>
<tr>
<th>Processing Stage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classification</td>
<td>Classifying traffic such as email traffic, content streaming, large document transmission, etc.</td>
</tr>
<tr>
<td>Policer per Flow or Group of Flows</td>
<td>Policing the traffic within the flow or group of flows</td>
</tr>
<tr>
<td>CoS/Services</td>
<td>Dividing the services using a 3-bit field, specifying a priority value between 0 (signifying best-effort) and 7 (signifying priority real-time data)</td>
</tr>
<tr>
<td>Queues</td>
<td>'Storing' data that is transmitted according to the CoS level specified</td>
</tr>
<tr>
<td>Rate Limitation/Shaping</td>
<td>Ensuring that traffic is shaped to the desired rate</td>
</tr>
<tr>
<td>Scheduling</td>
<td>Scheduling and ‘regulating’ traffic</td>
</tr>
<tr>
<td>Editing and Marking</td>
<td>Adding or removing VLAN IDs, as well as marking the priority on the outer VLAN header</td>
</tr>
</tbody>
</table>
### 1.5 Technical Specifications

**Network Interface**  
*Number of Ports*  
Up to 2 (RJ-45 or fiber optic SFPs). The second port can be configured as a network or user port.  

<table>
<thead>
<tr>
<th>Type</th>
<th>Fast or Gigabit Ethernet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fiber Optic Specifications and Ranges</td>
<td>See SFP Transceivers data sheet</td>
</tr>
<tr>
<td>Electrical Operation Mode</td>
<td>10/100 Mbps or 10/100/1000 Mbps, full duplex, autonegotiation, MDI/MDIX</td>
</tr>
</tbody>
</table>

**User Interface**  
*Number of Ports*  
Up to 2 (RJ-45 or fiber optic SFPs). If the second network port is configured as a user port, there are three user ports.  

<table>
<thead>
<tr>
<th>Type</th>
<th>Fast or Gigabit Ethernet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fiber Optic Specifications and Ranges</td>
<td>See SFP Transceivers data sheet</td>
</tr>
</tbody>
</table>
| Electrical Operation Mode | 10/100 Mbps or 10/100/1000 Mbps  
Full duplex, autonegotiation, MDI/MDIX |

**Standards Compliance**  
*IEEE*  
802.3, 802.3u, 802.1q, 802.1p, 802.3-2005 (relevant parts), 802.1ag-D8, RFC-2544  

*MEF*  
MEF 6 (E-Line – EPL and EVPL), MEF 9, MEF 10, MEF 14  

*ITU-T*  
Y.1731, G.8031  

**Ethernet Flows**  
*Number of Flows*  
192  

**Management**  
*Local*  
Via dedicated terminal port; V.24/RS-232 DCE; 9.6, 19.2, 38.4, 57.6, 115.2 kbps; RJ-45 connector  

*Inband*  
Via one of the Ethernet ports  

*Out-of-band*  
Via dedicated management port  

**Indicators**  
*PWR (green)*  
Power status  

*TST/ALM (red)*  
Alarm and loopback status
NET 1, NET 2, USER 3-4 (green) Link/activity status of the network/user port

**Power**

*AC/DC* AC/DC inlet connector with auto detection
Wide-range AC: 100–240 VAC, 50/60 Hz
DC: 8V (40–370 VDC)

*Power Consumption* 8W typical
12W max

**Physical**

*Height* 43.7 mm (1.7 in)

*Width* 215 mm (8.4 in)

*Depth* 150 mm (5.9 in)

*Weight* 2.4 kg (5.2 lb)

**Environment**

*Temperature* 0°C to 50°C (32°F to 122°F)

*Humidity* Up to 90%, non-condensing
Chapter 2
Installation and Setup

This chapter describes installation and setup procedures for the ETX-203A unit.

After installing the unit, refer to Chapter 3 for operating instructions and Chapter 4 for management instructions.

If a problem is encountered, refer to Chapter 6 for test and diagnostic instructions.

Internal settings, adjustment, maintenance, and repairs may be performed only by a skilled technician who is aware of the hazards involved.

Always observe standard safety precautions during installation, operation, and maintenance of this product.

2.1 Site Requirements and Prerequisites

AC-powered units should be installed within 1.5 m (5 ft) of an easily-accessible grounded AC outlet capable of furnishing the voltage in accordance with the nominal supply voltage.

DC-powered units require a -48 VDC power source, which must be adequately isolated from the main supply.

Allow at least 90 cm (36 in) of frontal clearance for operating and maintenance accessibility. Allow at least 10 cm (4 in) clearance at the rear of the unit for signal lines and interface cables.

The ambient operating temperature of ETX-203A is 0 to 50°C (32 to 122°F) at a relative humidity of up to 90%, non-condensing.

2.2 Package Contents

The ETX-203A package includes the following items:
- One ETX-203A unit
- Matching SFP module(s) (if ordered)
- CBL-RJ45/D9/F/6FT control port cable
- AC power cord or DC connection kit.
• Optional accessories included if ordered:
  • RM-33-2 rack-mount kit for mounting one or two ETX-203A units in a 19" rack.

2.3 Mounting the Unit

ETX-203A is designed for installation as a desktop unit. It can also be mounted in a 19" rack or on a wall.

• For rack mounting instructions, refer to the associated installation kit manual
• For wall mounting instructions, refer to the drilling template at the end of this manual
• If ETX-203A is to be used as a desktop unit, place and secure the unit on a stable, non-movable surface.

Refer to the clearance and temperature requirements in Site Requirements and Prerequisites.

2.4 Installing SFP Modules

ETX-203A uses SFP modules with LC fiber optic connectors.

⚠️ Warning

Third-party SFP optical transceivers must be agency-approved, complying with the local laser safety regulations for Class I laser equipment.

➢ To install the SFP modules:
  • Lock the wire latch of each SFP module by lifting it up until it clicks into place, as illustrated in Figure 2-1.

>Note

Some SFP models have a plastic door instead of a wire latch.
1. Carefully remove the dust covers from the SFP slot.

2. Insert the rear end of the SFP into the socket, and push slowly backwards to mate the connectors until the SFP clicks into place. If you feel resistance before the connectors are fully mated, retract the SFP using the wire latch as a pulling handle, and then repeat the procedure.

   **Caution**

   Insert the SFP gently. Using force can damage the connecting pins.

3. Remove the protective rubber caps from the SFP modules.

   **To remove the SFP module:**

   1. Disconnect the fiber optic cables from the SFP module.
   2. Unlock the wire latch by lowering it downwards (as opposed to locking).
   3. Hold the wire latch and pull the SFP module out of the Ethernet port.

   **Caution**

   Do not remove the SFP while the fiber optic cables are still connected. This may result in physical damage (such as a chipped SFP module clip or socket), or cause malfunction (e.g., the network port redundancy switching may be interrupted).

### 2.5 Connecting to Ethernet Equipment

ETX-203A can be connected to the Ethernet equipment via the following connectors, according to the relevant hardware configuration:

- Fiber optic LC designated ETH
- 8-pin RJ-45 electrical port designated ETH.

Refer to *Appendix A* for the RJ-45 connector pinout. The instructions below are illustrated using a sample configuration.

**To connect to the Ethernet equipment with fiber optic interface:**

- Connect ETX-203A to the Ethernet equipment using a standard fiber optic cable terminated with an LC connector.
To connect to the Ethernet equipment with a copper interface:

- Connect ETX-203A to the Ethernet network equipment using a standard straight UTP cable terminated with an RJ-45 connector.

**Note**

In order to comply with electromagnetic compatibility requirements, it is recommended to use shielded cables when connecting to the RJ-45 port of the ETX-203A electrical network or user interface.

---

### 2.6 Connecting to a Terminal

ETX-203A is connected to a terminal/laptop via an 8-pin RJ-45 connector designated CONTROL. Refer to Appendix A for the connector pinout.

- To connect to an ASCII terminal:
  1. Connect the RJ-45 connector of CBL-RJ45/D9/F/6FT cable to the CONTROL connector.
  2. Connect the other end of the CBL-RJ45/D9/F/6FT cable to an ASCII terminal.
**Caution**

Terminal cables must have a frame ground connection. Use ungrounded cables when connecting a supervisory terminal to a DC-powered unit with floating ground. Using improper terminal cable may result in damage to the supervisory terminal port.

---

### 2.7 Connecting to Management Station

ETX-203A is connected to remote network management stations via the dedicated Ethernet management port, an 8-pin RJ-45 connector designated MNG-ETH. Refer to Appendix A for the connector pinout.

- **To connect to an NMS:**
  - Connect ETX-203A to an Ethernet switch.

---

**Note**

*In order to provide protection against surges, use shielded cables when connecting to the MNG-ETH port.*

---

---

*Figure 2-5: Ethernet Management Connector*
2.8 Connecting to Power

Regular units are available with a universal AC/DC power supply. For the exact specs, refer to Technical Specifications in Chapter 1.

Before connecting or disconnecting any cable, the protective ground terminals of this unit must be connected to the protective ground conductor of the mains (AC or DC) power cord. If you are using an extension cord (power cable) make sure it is grounded as well.

Any interruption of the protective (grounding) conductor (inside or outside the instrument) or disconnecting of the protective ground terminal can make this unit dangerous. Intentional interruption is prohibited.

Note: Refer also to the sections describing connections of AC and DC power at the beginning of the manual.

Connecting to AC Power

AC power should be supplied via a 1.5 m (5 ft) standard power cable terminated by a standard 3-prong socket. A cable is provided with the unit.

To connect AC power:
1. Connect the power cable to the power connector on the ETX-203A rear panel.
2. Connect the power cable to the mains outlet.

The unit turns on automatically once connected to the mains.

Connecting to DC Power

Terminal block connectors with adapters are available for DC power supplies.

To connect DC power:
- Refer to the Terminal Block Connector DC Power Supply Connection supplement for instructions on wiring the DC adapters. This supplement can be found at the end of this manual.
Chapter 3

Operation

This chapter:

- Explains power-on and power-off procedures
- Provides a detailed description of the front panel controls and indicators and their functions

For a detailed explanation of parameters, see Chapter 5.

3.1 Turning On the Unit

To turn on ETX-203A:

- Connect the power cord to the mains.
  
The PWR indicator lights up and remains lit as long as ETX-203A receives power.

ETX-203A requires no operator attention once installed, with the exception of occasional monitoring of front panel indicators. Intervention is only required when ETX-203A must be configured to its operational requirements, or diagnostic tests are performed.
3.2 Indicators

The unit’s LEDs are located on the front panel (see Figure 3-1). Table 3-1 lists the functions of the ETX-203A LED indicators.

![Figure 3-1. Device LEDs](image)

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>PWR</td>
<td>Green LED</td>
<td>ON – Power is ON</td>
</tr>
<tr>
<td>NET 1</td>
<td>Green LEDs</td>
<td>ON – Corresponding Ethernet link is OK</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Blinking – Data is being transmitted or received on the corresponding Ethernet link</td>
</tr>
<tr>
<td>NET/ USER 2</td>
<td>Green LEDs</td>
<td>ON – Corresponding Ethernet link is OK</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Blinking – Data is being transmitted or received on the corresponding Ethernet link</td>
</tr>
<tr>
<td>USER 3,4</td>
<td>Green LEDs</td>
<td>ON – Corresponding Ethernet link is OK</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Blinking – Data is being transmitted or received on the corresponding Ethernet link</td>
</tr>
</tbody>
</table>

*Note* The number of network ports and user ports and the corresponding number of LEDs depend on the hardware configuration.

3.3 Startup

Configuration Files

The following files contain configuration settings:

- **factory-default** – Contains the manufacturer default settings
- **running-config** – Contains the current configuration that the device is running
- **startup-config** – Contains saved non-default user configuration. This file is not automatically created. You can use the `save` or `copy` command to create it.
- **user-default-config** – Contains default user configuration. This file is not automatically created. You can use the `copy` command to create it.

Refer to Chapter 5 for details on file operations.

**Note**

The `save` command is used to save the user configuration. Some commands that reset the device also erase the saved user configuration by copying another file to it before the reset. Refer to Figure 3-2 for details.

![Figure 3-2. Commands That Reset Device/Copy Configuration Files](image)

**Loading Sequence**

At startup, the device boots from the `startup-config` file, or the `user-default` file, or the `factory-default` file, in the sequence shown in Figure 3-3. If none of these files exist, the device boots using hard-coded defaults.

If the loading of `startup-config` or the `user-default` file fails, the file is deleted, the loading failure event is written in the event log, and the device reboots. After the reboot the device again attempts to load configuration files in the sequence shown in Figure 3-3.

To display the parameter values after startup, use the `info [detail]` command.
3.4 Using a Custom Configuration File

In large deployments, often a central network administrator sends configuration scripts to the remote locations and all that remains for the local technician to do is to replace the IP address in the script or other similar minor changes (using any text editor), and then download the file to the device.

To download the configuration file, use the copy command, as explained in Chapter 5. It is recommended to copy the file to both `startup-config` and the `user-default` file.

After downloading the configuration file, the unit must be reset in order to execute the file. After the unit completes its startup, the custom configuration is complete.
3.5 Turning Off the Unit

To power off the unit:

- Remove the power cord from the power source.
Chapter 4
Management

This chapter describes alternative methods of product management for ETX-203A. Detailed configuration procedures are given in Chapter 5.

4.1 Management Access Methods

Table 4-1 summarizes management alternatives for ETX-203A.

<table>
<thead>
<tr>
<th>Port</th>
<th>Manager Location</th>
<th>Transport Method</th>
<th>Management Protocol</th>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONTROL</td>
<td>Local</td>
<td>Out-of-band</td>
<td>RS-232</td>
<td>Terminal emulation programs such as HyperTerminal, Procomm, SecureCRT, Putty (see Working with Terminal below)</td>
</tr>
<tr>
<td>MNG-ETH</td>
<td>Local, remote</td>
<td>Out-of-band</td>
<td>Telnet, SSH</td>
<td>Procomm, SecureCRT, Putty (see Working with Telnet and SSH below)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>SNMP</td>
<td>Third-party NMS (see Working with Third-Party Network Management Systems below)</td>
</tr>
<tr>
<td>NET</td>
<td>Local, remote</td>
<td>Inband</td>
<td>Telnet, SSH</td>
<td>Procomm, SecureCRT, Putty (see Working with Telnet and SSH below)</td>
</tr>
<tr>
<td>USER</td>
<td></td>
<td></td>
<td>SNMP</td>
<td>Third-party NMS (see Working with Third-Party Network Management Systems below)</td>
</tr>
</tbody>
</table>

Note

By default, the terminal, Telnet (SSH), and SNMP management access methods are enabled. Refer to the section on Controlling Management Access in Chapter 5 for details on enabling/disabling a particular method.

4.2 Working with Terminal

ETX-203A has a V.24/RS-232 asynchronous DCE port, designated CONTROL and terminated in an RJ-45 connector. The control port continuously monitors the incoming data stream and immediately responds to any input string received through this port.
To start a terminal control session:

1. Make sure all ETX-203A cables and connectors are properly connected.

2. Connect ETX-203A to a PC equipped with an ASCII terminal emulation application (for example, HyperTerminal). Refer to Chapter 2 for details on connecting to the control port.

3. Start the PC terminal emulation (in Windows XP: Select Start > All Programs > Accessories > Communications > HyperTerminal to create a new terminal connection).

   The HyperTerminal application opens, and the Connection Description dialog box is displayed.

   ![HyperTerminal with Connection Description Dialog Box](image)

   **Figure 4-1. HyperTerminal with Connection Description Dialog Box**

4. Enter a name for the connection.

5. Select an icon to represent the terminal connection, or leave the default icon selected.

6. Click <OK>.

   The Connect To dialog box is displayed.
7. Select a PC COM port to be used to communicate with ETX-203A, and click <OK>.

The COM Properties dialog box is displayed.

8. Configure the communication port parameters as follows:
   - Bits per second: 9,600
   - Data bits: 8
- Parity: None
- Stop bits: 1
- Flow control: None.

9. Click <OK> to close the COM Properties dialog box.

HyperTerminal is now ready for communication with the unit.

**Note**  *It is not necessary to set the emulation type.*

10. Power-up ETX-203A.

ETX-203A boots up. When the startup process is completed, you are prompted to press <ENTER> to receive the login prompt.

![HyperTerminal Window after Startup](image)

**Figure 4-4. HyperTerminal Window after Startup**

11. Press <ENTER> until you receive the login prompt. Refer to *Logging In* for details on logging in.
Logging In

To prevent unauthorized modification of the operating parameters, ETX-203A supports two access levels:

- **Superuser** can perform all the activities supported by the ETX-203A management facility, including defining new users.
- **User** access rights *(full control or read only)* are defined by the superuser. Users are not allowed to create new users.

**Note**

*It is recommended to change default passwords to prevent unauthorized access to the unit.*

To enter as superuser:

1. At the User prompt *(user)*, enter `su` and press `<Enter>.
   
   The Password prompt *(password)* appears.
2. Enter **1234** as password and press `<Enter>.
   
   The base prompt **ETX-203A#** appears.

**Superuser** allows you to configure all parameters of ETX-203A and to change the **su** and **user** passwords.
To enter as User:

1. Enter user as user name and press <Enter>.
2. Enter 1234 as password and press <Enter>.

The base prompt ETX-203A# appears.

Using the CLI

The CLI consists of commands organized in a tree structure, starting at the base prompt. The base prompt is the device name, which can be configured in the system level (refer to Configuring Device Information in Chapter 5). By default the device name is.

Commands that are not global are available only at their specific tree location. To find out what commands are available at the current location, type ?. For a list of the commands and their levels, refer to Command Tree.

To navigate down the tree, type the name of the next level. The prompt then reflects the new location, followed by #. To navigate up, use the global command exit. To navigate all the way up to the root, type exit all.

At the prompt, one or more level names separated by a space can be typed, followed (or not) by a command. If only level names are typed, navigation is performed and the prompt changes to reflect the current location in the tree. If the level names are followed by a command, the command is executed, but no navigation is performed and the prompt remains unchanged.

Note

To use show commands without navigating, type show followed by the level name(s) followed by the rest of the show command.

In the following example, the levels and command were typed together and therefore no navigation was performed, so the prompt has not changed.

```
ETX-203A#
ETX-203A# configure port ethernet 1 loopback local
ETX-203A# show configure port ethernet 1 loopback
Loopback : Local Forever

ETX-203A#
```

Figure 4-6. Commands Without Level Navigation

In the following example, the levels were typed separately and the navigation is reflected by the changing prompt.

```
ETX-203A#
ETX-203A# configure
ETX-203A>config# port
ETX-203A>config# port# ethernet 1
ETX-203A>config# port>eth(1)# loopback local
ETX-203A>config# port>eth(1)# show loopback
Loopback : Local Forever

ETX-203A>config# port>eth(1)#
```

Figure 4-7. Commands With Level Navigation
**Note**

Level names are abbreviated in the prompt.

You can type only as many letters of the level or command as required by the system to identify the level or command, for example you can enter `config manag` to navigate to the **management** level.

In addition to being the default prompt, the `#` symbol also indicates a static entity (such as a port) or already configured entity. The `$` symbol indicates a new dynamic entity (such as a flow) that takes several commands to configure. The dynamic entity is created as inactive. After the configuration is completed, it is activated by using the `no shutdown` command, as shown in the following example.

```
ETX-203A#
ETX-203A# configure flows flow flow1
ETX-203A>config>flows>flow(flow1)$ ingress-port ethernet 3
ETX-203A>config>flows>flow(flow1)$ egress-port ethernet 1 queue 1 block 0/1
ETX-203A>config>flows>flow(flow1)$ classifier Classifier1
ETX-203A>config>flows>flow(flow1)$ no shutdown
ETX-203A>config>flows>flow(flow1)$exit
ETX-203A>config>flows#
```

Figure 4-8. Creating and Activating Flow

The `shutdown` command is also used to deactivate/disable a hardware element (such as a port), while `no shutdown` enables/activates it.

CLI commands have the following basic format:
```
command [parameter]{ value1 | value2 | ... | valuen } [ optional parameter <value> ]
```

where:

{} Indicates that one of the values must be selected
[] Indicates an optional parameter
<> Indicates a value to be typed by user according to parameter requirements

The following keys are available at any time:

- `?` Lists all commands available at the current level
- `<Tab>` Command autocomplete
- `↑` Displays the previous command
- `↓` Displays the next command
- `<Backspace>` Deletes character
- `<Ctrl-C>` Interrupts current command
- `<Ctrl-Z>` Logs out

The commands shown in Table 4-6 are available at any level.

CLI commands can be gathered into text files called scripts. They can be created using a text editor, by recording the user commands or by saving the current
The scripts can be imported from and exported to RAD devices via file transfer protocols.

**Command Tree**

At the CLI root, the following categories are available:

- configure
- file
- admin
- root
- global-commands.

Each category is detailed in the tables below.

*Table 4.2. Commands in the configure category*

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure</td>
<td>Enter configure level</td>
</tr>
<tr>
<td></td>
<td>chassis</td>
</tr>
<tr>
<td></td>
<td>show environment</td>
</tr>
<tr>
<td></td>
<td>temperature-threshold</td>
</tr>
<tr>
<td>test</td>
<td>Enter test level</td>
</tr>
<tr>
<td></td>
<td>rfc2544</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>test</td>
</tr>
<tr>
<td></td>
<td>activate</td>
</tr>
<tr>
<td></td>
<td>bind</td>
</tr>
<tr>
<td></td>
<td>max-rate</td>
</tr>
<tr>
<td></td>
<td>test-profile</td>
</tr>
<tr>
<td></td>
<td>type</td>
</tr>
</tbody>
</table>
## Command Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show report</td>
<td>Display test report</td>
</tr>
<tr>
<td>show status</td>
<td>Show test status</td>
</tr>
<tr>
<td>show summary</td>
<td>Show test summary</td>
</tr>
<tr>
<td>system</td>
<td>Configure system parameters</td>
</tr>
<tr>
<td>name</td>
<td>Configure name of device</td>
</tr>
<tr>
<td>contact</td>
<td>Configure contact person</td>
</tr>
<tr>
<td>location</td>
<td>Configure location of device</td>
</tr>
<tr>
<td>tftp</td>
<td>Configure TFTP parameters</td>
</tr>
<tr>
<td>clear-event-log</td>
<td>Clear event log</td>
</tr>
<tr>
<td>clear-cpu-utilization</td>
<td>Clear CPU utilization counters</td>
</tr>
<tr>
<td>show device-information</td>
<td>Display device information</td>
</tr>
<tr>
<td>show inventory-table</td>
<td>Display inventory information</td>
</tr>
<tr>
<td>show event-log</td>
<td>Display event log</td>
</tr>
<tr>
<td>show time</td>
<td>Display date and time</td>
</tr>
<tr>
<td>show cpu-utilization</td>
<td>Shows the CPU utilization</td>
</tr>
<tr>
<td>show buffers</td>
<td>Display memory buffer usage</td>
</tr>
<tr>
<td>inventory</td>
<td>Configure inventory entity</td>
</tr>
<tr>
<td>alias</td>
<td>Configure inventory entity alias</td>
</tr>
<tr>
<td>asset-id</td>
<td>Configure inventory entity asset ID</td>
</tr>
<tr>
<td>serial-number</td>
<td>Configure inventory entity serial number</td>
</tr>
<tr>
<td>show status</td>
<td>Display inventory entity status</td>
</tr>
<tr>
<td>date-and-time</td>
<td>Configure date &amp; time parameters</td>
</tr>
<tr>
<td>date-format</td>
<td>Configure system date format</td>
</tr>
<tr>
<td>date</td>
<td>Configure system date</td>
</tr>
<tr>
<td>time</td>
<td>Configure system time</td>
</tr>
<tr>
<td>zone</td>
<td>Configure time zone and offset</td>
</tr>
<tr>
<td>sntp</td>
<td>Configure Simple Network Time Protocol parameters</td>
</tr>
<tr>
<td>broadcast</td>
<td>Enable/disable broadcast client mode for SNTP</td>
</tr>
<tr>
<td>poll-interval</td>
<td>Configure SNTP polling interval</td>
</tr>
<tr>
<td>server</td>
<td>Configure SNTP server</td>
</tr>
<tr>
<td>address</td>
<td>Configure SNTP server IP address</td>
</tr>
<tr>
<td>prefer</td>
<td>Set/Reset the SNTP server Preference</td>
</tr>
<tr>
<td>query-server</td>
<td>Query the timestamp from the SNTP Server</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>shutdown</td>
<td>Enable/Disable SNTP Server</td>
</tr>
<tr>
<td>udp</td>
<td>UDP Port of SNTP Server</td>
</tr>
<tr>
<td>show status</td>
<td>Displays SNTP Servers Status</td>
</tr>
<tr>
<td>send-request</td>
<td>Send SNTP request to server</td>
</tr>
<tr>
<td>syslog</td>
<td>Configure syslog entities</td>
</tr>
<tr>
<td>address</td>
<td>Configure target address of syslog server</td>
</tr>
<tr>
<td>shutdown</td>
<td>Enable/disable logging of syslog entity</td>
</tr>
<tr>
<td>facility</td>
<td>Configure facility of device</td>
</tr>
<tr>
<td>severity-level</td>
<td>Configure severity level of device</td>
</tr>
<tr>
<td>port</td>
<td>Configure UDP port number</td>
</tr>
<tr>
<td>show statistics</td>
<td>Display syslog statistics</td>
</tr>
<tr>
<td>clock-quality</td>
<td>[Not supported in Ver. 3.0]</td>
</tr>
<tr>
<td>source-port-identity</td>
<td>Identifier number of the master clock</td>
</tr>
<tr>
<td>sync-rate</td>
<td>Specify the synchronization rate desired by the slave</td>
</tr>
<tr>
<td>max-frequency-deviation</td>
<td>[Not supported in Ver. 3.0]</td>
</tr>
<tr>
<td>management</td>
<td>Configure management parameters</td>
</tr>
<tr>
<td>user</td>
<td>Create/delete user</td>
</tr>
<tr>
<td>show users</td>
<td>Display users</td>
</tr>
<tr>
<td>host</td>
<td>Configure host parameters</td>
</tr>
<tr>
<td>dhcp</td>
<td>Enable or disable DHCP</td>
</tr>
<tr>
<td>ip-address</td>
<td>Configure host IP address</td>
</tr>
<tr>
<td>default-gateway</td>
<td>Configure IP address of default gateway</td>
</tr>
<tr>
<td>arp-timeout</td>
<td>Configure ARP timeout</td>
</tr>
<tr>
<td>show status</td>
<td>Display host status</td>
</tr>
<tr>
<td>snmp</td>
<td>Configure SNMP parameters</td>
</tr>
<tr>
<td>community</td>
<td>Configure SNMP read, write, and trap community</td>
</tr>
<tr>
<td>trap-mask</td>
<td>Mask specific alarm traps to all network managers</td>
</tr>
<tr>
<td>trap-delay</td>
<td>Configure delay for sending trap</td>
</tr>
<tr>
<td>snmp-engine-id-string</td>
<td>Text, administratively assigned. Maximum remaining length 27</td>
</tr>
<tr>
<td>snmpv3</td>
<td>Enable or disable SNMPv3</td>
</tr>
<tr>
<td>show snmpv3 information</td>
<td>Display SNMPv3 information</td>
</tr>
<tr>
<td>user</td>
<td>Configure SNMPv3 user</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>shutdown</td>
<td>Activate or deactivate SNMPv3 user</td>
</tr>
<tr>
<td>authentication</td>
<td>Configure authentication for SNMPv3 user</td>
</tr>
<tr>
<td>privacy</td>
<td>Configure privacy for SNMPv3 user</td>
</tr>
<tr>
<td>access-group</td>
<td>Configure SNMPv3 access group</td>
</tr>
<tr>
<td>shutdown</td>
<td>Activate or deactivate SNMPv3 access group</td>
</tr>
<tr>
<td>context-match</td>
<td>Configure context match</td>
</tr>
<tr>
<td>read-view</td>
<td>Configure read view</td>
</tr>
<tr>
<td>write-view</td>
<td>Configure write view</td>
</tr>
<tr>
<td>notify-view</td>
<td>Configure notify view</td>
</tr>
<tr>
<td>security-to-group</td>
<td>Configure security for access group</td>
</tr>
<tr>
<td>shutdown</td>
<td>Activate or deactivate security for access group</td>
</tr>
<tr>
<td>group-name</td>
<td>Specify access group</td>
</tr>
<tr>
<td>view</td>
<td>Configure SNMPv3 view</td>
</tr>
<tr>
<td>shutdown</td>
<td>Activate or deactivate</td>
</tr>
<tr>
<td>mask</td>
<td>Configure SNMPv3 view mask</td>
</tr>
<tr>
<td>type</td>
<td>Configure SNMPv3 view type</td>
</tr>
<tr>
<td>community</td>
<td>Configure SNMPv3 community</td>
</tr>
<tr>
<td>shutdown</td>
<td>Activate or deactivate</td>
</tr>
<tr>
<td>name</td>
<td>Configure SNMPv3 community name</td>
</tr>
<tr>
<td>sec-name</td>
<td>Configure SNMPv3 community security name</td>
</tr>
<tr>
<td>tag</td>
<td>Configure SNMPv3 community tag</td>
</tr>
<tr>
<td>target-params</td>
<td>Configure SNMPv3 target parameters</td>
</tr>
<tr>
<td>shutdown</td>
<td>Activate or deactivate SNMPv3 target parameters</td>
</tr>
<tr>
<td>message-processing-model</td>
<td>Configure SNMPv3 target parameters message processing model</td>
</tr>
<tr>
<td>version</td>
<td>Configure SNMPv3 target parameters version</td>
</tr>
<tr>
<td>security</td>
<td>Configure SNMPv3 target parameters security</td>
</tr>
<tr>
<td>target</td>
<td>Configure SNMPv3 target</td>
</tr>
<tr>
<td>shutdown</td>
<td>Activate or deactivate SNMPv3 target</td>
</tr>
<tr>
<td>target-params</td>
<td>Configure SNMPv3 target parameters</td>
</tr>
<tr>
<td>tag-list</td>
<td>Configure SNMPv3 target tag list</td>
</tr>
<tr>
<td>address</td>
<td>Configure SNMPv3 target address</td>
</tr>
<tr>
<td>trap-sync-group</td>
<td>Configure trap synchronization group with SNMPv3 managers</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>notify</td>
<td>Configure SNMPv3 notification</td>
</tr>
<tr>
<td>shutdown</td>
<td>Activate or deactivate SNMPv3 notification</td>
</tr>
<tr>
<td>tag</td>
<td>Configure SNMPv3 notification tag</td>
</tr>
<tr>
<td>bind</td>
<td>Configure SNMPv3 notification bind</td>
</tr>
<tr>
<td>notify-filter</td>
<td>Configure SNMPv3 notification filter</td>
</tr>
<tr>
<td>shutdown</td>
<td>Activate or deactivate SNMPv3 notification filter</td>
</tr>
<tr>
<td>type</td>
<td>Configure SNMPv3 notification filter type</td>
</tr>
<tr>
<td>mask</td>
<td>Configure SNMPv3 notification filter mask</td>
</tr>
<tr>
<td>notify-filter-profile</td>
<td>Configure SNMPv3 notification filter profile</td>
</tr>
<tr>
<td>shutdown</td>
<td>Activate or deactivate SNMPv3 notification filter profile</td>
</tr>
<tr>
<td>profile-name</td>
<td>Configure SNMPv3 notification filter profile name</td>
</tr>
<tr>
<td>trap-sync-group</td>
<td>Configure trap synchronization group with SNMPv3 managers</td>
</tr>
<tr>
<td>target-params</td>
<td>Configure target parameters for trap synchronization group with SNMPv3 managers</td>
</tr>
<tr>
<td>tag-list</td>
<td>Configure tag list for trap synchronization group with SNMPv3 managers</td>
</tr>
<tr>
<td>show trap-sync</td>
<td>Display the trap synchronization information if SNMPv3 is enabled</td>
</tr>
<tr>
<td>access</td>
<td>Configure management access</td>
</tr>
<tr>
<td>telnet</td>
<td>Configure telnet access</td>
</tr>
<tr>
<td>ssh</td>
<td>Configure SSH access</td>
</tr>
<tr>
<td>snmp</td>
<td>Configure SNMP access</td>
</tr>
<tr>
<td>auth-policy</td>
<td>Configure policy of authentication</td>
</tr>
<tr>
<td>radius</td>
<td>RADIUS parameters</td>
</tr>
<tr>
<td>server</td>
<td>Create/delete RADIUS server</td>
</tr>
<tr>
<td>address</td>
<td>Configure address of RADIUS server</td>
</tr>
<tr>
<td>shutdown</td>
<td>Enable/disable RADIUS server</td>
</tr>
<tr>
<td>key</td>
<td>Configure client and RADIUS server shared secret</td>
</tr>
<tr>
<td>retry</td>
<td>Configure number of request attempts from RADIUS server</td>
</tr>
<tr>
<td>timeout</td>
<td>Configure timeout for a response from RADIUS server</td>
</tr>
<tr>
<td>auth-port</td>
<td>Configure logical port to be used by the authentication protocol</td>
</tr>
</tbody>
</table>
### Command Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show status</td>
<td>Display RADIUS status</td>
</tr>
<tr>
<td>show statistics</td>
<td>Display RADIUS statistics</td>
</tr>
<tr>
<td>tacacsplus</td>
<td>TACACS+ parameters</td>
</tr>
<tr>
<td>server</td>
<td>Configure TACACS+ server</td>
</tr>
<tr>
<td>shutdown</td>
<td>Enable/disable TACACS+ server</td>
</tr>
<tr>
<td>retry</td>
<td>Configure number of request attempts from RADIUS server</td>
</tr>
<tr>
<td>timeout</td>
<td>Configure timeout for a response from RADIUS server</td>
</tr>
<tr>
<td>show statistics</td>
<td>Display TACACS+ server statistics</td>
</tr>
<tr>
<td>show status</td>
<td>Display TACACS+ server status</td>
</tr>
<tr>
<td>show status-summary</td>
<td>Display TACACS+ status summary</td>
</tr>
<tr>
<td>manager</td>
<td>Configure network manager</td>
</tr>
<tr>
<td>udp-port</td>
<td>Define UDP port used to send traps</td>
</tr>
<tr>
<td>trap-mask</td>
<td>Mask or unmask traps to network manager</td>
</tr>
<tr>
<td>trap-sync-group</td>
<td>Configure trap synchronization group with SNMPv1 managers</td>
</tr>
<tr>
<td>trap-mask</td>
<td>Configure trap masking for trap synchronization group with SNMPv1 managers</td>
</tr>
<tr>
<td>show trap-sync</td>
<td>Display the trap synchronization information if SNMPv3 is not enabled</td>
</tr>
<tr>
<td>qos</td>
<td>Enter quality of service level</td>
</tr>
<tr>
<td>cos-map-profile</td>
<td>Configure profile for mapping user priority to internal cos</td>
</tr>
<tr>
<td>map</td>
<td>Define the mapping from user priority to internal cos</td>
</tr>
<tr>
<td>policer-profile</td>
<td>Configure a policer profile</td>
</tr>
<tr>
<td>bandwidth</td>
<td>Define the bandwidth for the policer profile</td>
</tr>
<tr>
<td>traffic-type</td>
<td>Define the policed traffic type</td>
</tr>
<tr>
<td>compensation</td>
<td>Define how many bytes to compensate for layer 1 overhead</td>
</tr>
<tr>
<td>policer-aggregate</td>
<td>Configure policer aggregate that specifies a policer profile to apply to a group of flows</td>
</tr>
<tr>
<td>policer</td>
<td>Define policer profile for the policer aggregate</td>
</tr>
<tr>
<td>show statistics</td>
<td>Display policer aggregate statistics</td>
</tr>
<tr>
<td>show flows</td>
<td>Display the flows corresponding to policer aggregate</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>clear-statistics</td>
<td>Clear policer aggregate statistics</td>
</tr>
<tr>
<td>rate-sampling-window</td>
<td>Configure interval for rate sampling statistics</td>
</tr>
<tr>
<td>shaper-profile</td>
<td>Configure shaper profile</td>
</tr>
<tr>
<td>bandwidth</td>
<td>Define the bandwidth for the shaper profile</td>
</tr>
<tr>
<td>compensation</td>
<td>Define how many bytes to compensate for layer 1 overhead</td>
</tr>
<tr>
<td>marking-profile</td>
<td>Configure a marking profile to map the P-bit, IP precedence, or DHCP classifications to the egress priority tags</td>
</tr>
<tr>
<td>mark</td>
<td>Map the user priority to a priority marking value</td>
</tr>
<tr>
<td>queue-block-profile</td>
<td>Configure queue block profile</td>
</tr>
<tr>
<td>queue</td>
<td>Define queue</td>
</tr>
<tr>
<td>depth</td>
<td>Define the queue length</td>
</tr>
<tr>
<td>scheduling</td>
<td>Define the queue scheduling method</td>
</tr>
<tr>
<td>queue-group-profile</td>
<td>Configure queue group profile</td>
</tr>
<tr>
<td>queue-block</td>
<td>Configure queue block</td>
</tr>
<tr>
<td>name</td>
<td>Define the name of the queue block</td>
</tr>
<tr>
<td>profile</td>
<td>Define the queue block profile for the queue block</td>
</tr>
<tr>
<td>bind</td>
<td>Bind to next level block in specific queue</td>
</tr>
<tr>
<td>shaper</td>
<td>Define the shaper profile for the queue block</td>
</tr>
<tr>
<td>queue-map-profile</td>
<td>Define a queue map profile to map the P-bit, IP precedence, or DSCP classifications to internal priority queues (classes of service)</td>
</tr>
<tr>
<td>map</td>
<td>Define the mapping between the user priority and the queue id</td>
</tr>
<tr>
<td>wred-profile</td>
<td>Configure WRED profile</td>
</tr>
<tr>
<td>color</td>
<td>Configure the minimum and maximum queue usage threshold, and percentage of packets to drop when queue reaches maximum usage threshold</td>
</tr>
<tr>
<td>fault</td>
<td>Enter fault level</td>
</tr>
<tr>
<td>fault-propagation</td>
<td>Configure fault propagation</td>
</tr>
<tr>
<td>action-on-group</td>
<td>Action(s) to perform in order to propagate a fault</td>
</tr>
<tr>
<td>trigger</td>
<td>Trigger for propagating fault</td>
</tr>
<tr>
<td>wait-to-restore</td>
<td>Define the time between recovery and resumption of transmission</td>
</tr>
<tr>
<td>cfm</td>
<td>Enter fault CFM level</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>service</td>
<td>Configure event reporting for service</td>
</tr>
<tr>
<td>frames-report</td>
<td>Define event reporting type for service</td>
</tr>
<tr>
<td>oam</td>
<td>Enter OAM level</td>
</tr>
<tr>
<td>efm</td>
<td>Enter OAM EFM level</td>
</tr>
<tr>
<td>descriptor</td>
<td>Configure OAM EFM descriptor</td>
</tr>
<tr>
<td>cfm</td>
<td>Enter OAM CFM level</td>
</tr>
<tr>
<td>multicast-addr</td>
<td>Define the multicast address for OAM messages</td>
</tr>
<tr>
<td>show summary</td>
<td>Display OAM CFM information</td>
</tr>
<tr>
<td>maintenance-domain</td>
<td>Configure a maintenance domain (MD)</td>
</tr>
<tr>
<td>name</td>
<td>Define the name of the MD</td>
</tr>
<tr>
<td>md-level</td>
<td>Define the level of the MD</td>
</tr>
<tr>
<td>mip-policy</td>
<td>Define MIP policy</td>
</tr>
<tr>
<td>proprietary-cc</td>
<td>Define whether the OAM protocol of the MD is standard or pre-standard</td>
</tr>
<tr>
<td>maintenance-association</td>
<td>Configure a maintenance association (MA)</td>
</tr>
<tr>
<td>classification</td>
<td>Associate the MA with a VLAN</td>
</tr>
<tr>
<td>mip-policy</td>
<td>Define MIP policy</td>
</tr>
<tr>
<td>name</td>
<td>Define the name of the MA</td>
</tr>
<tr>
<td>ccm-interval</td>
<td>Define the continuity check interval of the MA</td>
</tr>
<tr>
<td>mep</td>
<td>Configure a maintenance endpoint (MEP)</td>
</tr>
<tr>
<td>ais</td>
<td>Define sending of AIS</td>
</tr>
<tr>
<td>bind</td>
<td>Bind MEP to Ethernet port or EVC Termination Point (ETP) port</td>
</tr>
<tr>
<td>ccm-initiate</td>
<td>Enable or disable continuity check messages</td>
</tr>
<tr>
<td>ccm-priority</td>
<td>Define the priority of the CC message</td>
</tr>
<tr>
<td>classification</td>
<td>Associate the MEP with a classifier profile or VLAN</td>
</tr>
<tr>
<td>client-md-level</td>
<td>Define client MD level</td>
</tr>
<tr>
<td>continuity-verification</td>
<td>Define continuity verification as CC-based or lb-based (only if OAM protocol is pre-standard and ccm-initiate is enabled)</td>
</tr>
<tr>
<td>dest-addr-type</td>
<td>Define MAC address types sent in OAM continuity check messages and in performance measurement messages, as standard multicast address or user-defined unicast address</td>
</tr>
</tbody>
</table>
### Command Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dest-mac-addr</td>
<td>Define the unicast MAC address sent in OAM CCM messages if you defined</td>
</tr>
<tr>
<td></td>
<td>unicast MAC address type for CCM messages</td>
</tr>
<tr>
<td>direction</td>
<td>Define direction</td>
</tr>
<tr>
<td>forwarding-method</td>
<td>Define forwarding method</td>
</tr>
<tr>
<td>lbm</td>
<td>Configure OAM loopback</td>
</tr>
<tr>
<td>linktrace</td>
<td>Configure OAM link trace</td>
</tr>
<tr>
<td>queue</td>
<td>Define queue for the MEP</td>
</tr>
<tr>
<td>remote-mep</td>
<td>Define a remote MEP for the MEP</td>
</tr>
<tr>
<td>show remote-mep status</td>
<td>Display status of remote MEP</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>[show remote-mep &lt;remote-mep-id&gt; status]</td>
</tr>
<tr>
<td>shutdown</td>
<td>Activate or deactivate the MEP</td>
</tr>
<tr>
<td>show status</td>
<td>Display status of MEP</td>
</tr>
<tr>
<td>show lbm-results</td>
<td>Display result of OAM loopback</td>
</tr>
<tr>
<td>show linktrace-results</td>
<td>Display result of OAM link trace</td>
</tr>
<tr>
<td>service</td>
<td>Configure MEP service</td>
</tr>
<tr>
<td>classification</td>
<td>Associate service with p-bit</td>
</tr>
<tr>
<td>delay-threshold</td>
<td>Define delay threshold for the MEP service</td>
</tr>
<tr>
<td>delay-var-threshold</td>
<td>Define delay variation threshold for the MEP service</td>
</tr>
<tr>
<td>dmm-interval</td>
<td>Specify the interval for delay measurement messages</td>
</tr>
<tr>
<td>lmm-interval</td>
<td>Specify the interval for loss measurement messages</td>
</tr>
<tr>
<td>shutdown</td>
<td>Activate or deactivate the MEP service</td>
</tr>
<tr>
<td>clear-statistics</td>
<td>Clear the OAM CFM statistics for service</td>
</tr>
<tr>
<td>show statistics</td>
<td>Display the OAM CFM statistics for service</td>
</tr>
<tr>
<td>dest-ne</td>
<td>Configure destination NE</td>
</tr>
<tr>
<td>remote</td>
<td>Define remote MAC address or remote MEP ID</td>
</tr>
<tr>
<td>delay</td>
<td>Enable two-way delay measurement method</td>
</tr>
<tr>
<td>delay-measurement-bin</td>
<td>Define the delay measurement bin profile to use as delay bin policy</td>
</tr>
<tr>
<td>delay-var-measurement-bin</td>
<td>Define the delay variation measurement bin profile to use as delay variation</td>
</tr>
<tr>
<td>loss</td>
<td>Enable single-ended loss measurement method</td>
</tr>
<tr>
<td>clear-statistics</td>
<td>Clear the OAM CFM statistics for destination NE</td>
</tr>
<tr>
<td>show delay-measurement-bins</td>
<td>Display the delay measurement bins</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>show statistics</td>
<td>Display the OAM CFM statistics for destination NE</td>
</tr>
<tr>
<td>port</td>
<td>Enter configure port level</td>
</tr>
<tr>
<td>rate-sampling-window</td>
<td>Configure interval for rate sampling statistics</td>
</tr>
<tr>
<td>show summary</td>
<td>Display the status of all Ethernet ports</td>
</tr>
<tr>
<td>e1</td>
<td>Configure E1 port</td>
</tr>
<tr>
<td>line-code</td>
<td>Specifies the line code and zero suppression method used by the port</td>
</tr>
<tr>
<td>line-type</td>
<td>Specifies the E1 framing mode</td>
</tr>
<tr>
<td>loopback</td>
<td>Enables/disables loopback mode for the specified port</td>
</tr>
<tr>
<td>name</td>
<td>Assigns/removes a port name</td>
</tr>
<tr>
<td>rx-sensitivity</td>
<td>Specifies the attenuation level of the receive signal that is compensated for by the interface receive path</td>
</tr>
<tr>
<td>tx-clock-source</td>
<td>Specifies the source of the port’s transmit clock</td>
</tr>
<tr>
<td>shutdown</td>
<td>Administratively disables/enables the port</td>
</tr>
<tr>
<td>show alarms</td>
<td>Displays alarms</td>
</tr>
<tr>
<td>show bind</td>
<td>Displays a list of interfaces bound to port</td>
</tr>
<tr>
<td>show loopback</td>
<td>Displays loopback test results</td>
</tr>
<tr>
<td>show status</td>
<td>Displays the port status</td>
</tr>
<tr>
<td>show statistics</td>
<td>Displays the port statistics</td>
</tr>
<tr>
<td>clear-statistics</td>
<td>Clears the statistics</td>
</tr>
<tr>
<td>e3</td>
<td>Configure E3 port</td>
</tr>
<tr>
<td>loopback</td>
<td>Enables/disables loopback mode for the specified port</td>
</tr>
<tr>
<td>name</td>
<td>Assigns/removes a port name</td>
</tr>
<tr>
<td>tx-clock-source</td>
<td>Specifies the source of the port’s transmit clock</td>
</tr>
<tr>
<td>shutdown</td>
<td>Administratively disables/enables the port</td>
</tr>
<tr>
<td>show alarms</td>
<td>Displays alarms</td>
</tr>
<tr>
<td>show bind</td>
<td>Displays a list of interfaces bound to port</td>
</tr>
<tr>
<td>show loopback</td>
<td>Displays loopback test results</td>
</tr>
<tr>
<td>show status</td>
<td>Displays the port status</td>
</tr>
<tr>
<td>show statistics</td>
<td>Displays the port statistics</td>
</tr>
<tr>
<td>clear-statistics</td>
<td>Clears the statistics</td>
</tr>
<tr>
<td>ethernet</td>
<td>Configure Ethernet port</td>
</tr>
</tbody>
</table>
### Command Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Define port name</td>
</tr>
<tr>
<td>shutdown</td>
<td>This command administratively disables a port. The no form of this command administratively enables a port.</td>
</tr>
<tr>
<td>auto-negotiation</td>
<td>Configure auto negotiation ability</td>
</tr>
<tr>
<td>max-capability</td>
<td>Configure maximum capability advertising</td>
</tr>
<tr>
<td>speed-duplex</td>
<td>This command configures the speed and duplex of an Ethernet port when auto negotiation is disabled.</td>
</tr>
<tr>
<td>tag-ethernet-type</td>
<td>This command specifies the Ethertype expected in Ethernet packet</td>
</tr>
<tr>
<td>efm</td>
<td>Enable or disable link OAM EFM for Ethernet port</td>
</tr>
<tr>
<td>loopback</td>
<td>Define loopback</td>
</tr>
<tr>
<td>snmp-tunneling</td>
<td>Define SNMP tunneling for OAM EFM</td>
</tr>
<tr>
<td>egress-mtu</td>
<td>Define the maximum transmission unit (MTU)</td>
</tr>
<tr>
<td>queue-group</td>
<td>Define queue group profile for port</td>
</tr>
<tr>
<td>loopback</td>
<td>This command puts the specified port into a loopback mode. The no form of the command disables the specified type of lookback.</td>
</tr>
<tr>
<td>l2cp</td>
<td>Assign L2CP profile to Ethernet port</td>
</tr>
<tr>
<td>functional-mode</td>
<td>Determine if second network port works in user mode or network. If in network then redundancy is available</td>
</tr>
<tr>
<td>policer</td>
<td>Associate the port with a policer profile</td>
</tr>
<tr>
<td>clear-statistics</td>
<td>Clear Ethernet port statistics</td>
</tr>
<tr>
<td>clear-l2cp-statistics</td>
<td>Clear L2CP statistics</td>
</tr>
<tr>
<td>dhcp-request</td>
<td>Configure whether DHCP request should be sent whenever the port is activated</td>
</tr>
<tr>
<td>show status</td>
<td>Display Ethernet port status</td>
</tr>
<tr>
<td>show statistics</td>
<td>Display Ethernet port statistics</td>
</tr>
<tr>
<td>show oam-efm</td>
<td>Display OAM EFM status</td>
</tr>
<tr>
<td>show oam-efm-statistics</td>
<td>Display OAM EFM statistics</td>
</tr>
<tr>
<td>show loopback</td>
<td>Display loopback status</td>
</tr>
<tr>
<td>show l2cp-statistics</td>
<td>Display L2CP statistics</td>
</tr>
<tr>
<td>gfp</td>
<td>Configure GFP port</td>
</tr>
<tr>
<td>bind</td>
<td>Bind to lower-level port</td>
</tr>
<tr>
<td>fcs-payload</td>
<td>Enable or disable FCS payload</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td>name</td>
<td>Assign name to port</td>
</tr>
<tr>
<td>shutdown</td>
<td>Administratively enable or disable port</td>
</tr>
<tr>
<td>show status</td>
<td>Display port status</td>
</tr>
<tr>
<td>l2cp-profile</td>
<td>Define L2CP profile</td>
</tr>
<tr>
<td>shutdown</td>
<td>Define MAC address L2CP action</td>
</tr>
<tr>
<td>default</td>
<td>Default action for undefined control protocols</td>
</tr>
<tr>
<td>protocol</td>
<td>Choose specific protocol</td>
</tr>
<tr>
<td>lag</td>
<td>Configure LAG</td>
</tr>
<tr>
<td>shutdown</td>
<td>Activate or deactivate the LAG</td>
</tr>
<tr>
<td>admin-key</td>
<td>Define an admin key that indicates the port speed</td>
</tr>
<tr>
<td>bind</td>
<td>Bind a port to the LAG</td>
</tr>
<tr>
<td>lACP</td>
<td>Enable the LACP protocol on the LAG</td>
</tr>
<tr>
<td>distribution-method</td>
<td>Define the distribution method</td>
</tr>
<tr>
<td>sys-priority</td>
<td>Assign value used to build LAG ID, which determines aggregation precedence</td>
</tr>
<tr>
<td>show members-status</td>
<td>Display the status of the LAG members</td>
</tr>
<tr>
<td>show members-statistics</td>
<td>Display statistics for the LAG members</td>
</tr>
<tr>
<td>logical-mac</td>
<td>Configure logical MAC port</td>
</tr>
<tr>
<td>bind</td>
<td>Bind to lower-level port</td>
</tr>
<tr>
<td>clear-statistics</td>
<td>Clear port statistics</td>
</tr>
<tr>
<td>dhcp-request</td>
<td>Configure whether DHCP request should be sent whenever the port is activated</td>
</tr>
<tr>
<td>efm</td>
<td>Enables/disables OAM (EFM) on the Ethernet port</td>
</tr>
<tr>
<td>loopback</td>
<td>Enables/disables loopback operations</td>
</tr>
<tr>
<td>snmp-tunneling</td>
<td>Enable/disable tunneling SNMP messages to remote</td>
</tr>
<tr>
<td>egress-mtu</td>
<td>Define the maximum transmission unit (MTU)</td>
</tr>
<tr>
<td>l2cp</td>
<td>Assign L2CP profile to port</td>
</tr>
<tr>
<td>loopback</td>
<td>This command puts the specified port into a loopback mode. The no form of the command disables the specified type of lookback.</td>
</tr>
<tr>
<td>name</td>
<td>Define port name</td>
</tr>
<tr>
<td>queue-group</td>
<td>Assigns/removes a queue group profile</td>
</tr>
<tr>
<td>tag-ethernet-type</td>
<td>This command specifies the Ethertype expected in packets</td>
</tr>
<tr>
<td>shutdown</td>
<td>Administratively disables/enables the port</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>show bind</td>
<td>Displays a list of interfaces bound to the port</td>
</tr>
<tr>
<td>show statistics</td>
<td>Displays port statistics</td>
</tr>
<tr>
<td>show status</td>
<td>Displays port status</td>
</tr>
<tr>
<td>sdh-sonet</td>
<td>Configure SDH/SONET port</td>
</tr>
<tr>
<td>aug</td>
<td>Defines the administrative unit group (AUG)</td>
</tr>
<tr>
<td>j1-pathtrace</td>
<td>Configure J1 path trace</td>
</tr>
<tr>
<td>loopback</td>
<td>Enables/disables loopback mode for the AUG</td>
</tr>
<tr>
<td>payload-label</td>
<td>Specifies the payload string to attach to packets</td>
</tr>
<tr>
<td>plm-response</td>
<td>Enable or disable the sending of remote defect indication (RDI) if payload string mismatch (PLM-P) occurs</td>
</tr>
<tr>
<td>tim-response</td>
<td>Enable or disable the sending of remote defect indication (RDI) if trace identifier mismatch payload (TIM-P) occurs</td>
</tr>
<tr>
<td>frame-type</td>
<td>Specifies the cell frame type</td>
</tr>
<tr>
<td>loopback</td>
<td>Enables/disables loopback mode for the port</td>
</tr>
<tr>
<td>oc3</td>
<td>Defines an OC-3 (STM-1) connection</td>
</tr>
<tr>
<td>j1-pathtrace</td>
<td>Configure J1 path trace</td>
</tr>
<tr>
<td>loopback</td>
<td>Enables/disables loopback mode for the OC-3 (STM-1) connection</td>
</tr>
<tr>
<td>payload-label</td>
<td>Specifies the payload string to attach to packets</td>
</tr>
<tr>
<td>plm-response</td>
<td>Enable or disable the sending of remote defect indication (RDI) if payload string mismatch (PLM-P) occurs</td>
</tr>
<tr>
<td>tim-response</td>
<td>Enable or disable the sending of remote defect indication (RDI) if trace identifier mismatch payload (TIM-P) occurs</td>
</tr>
<tr>
<td>threshold</td>
<td>Bit error rate above which an alarm is triggered</td>
</tr>
<tr>
<td>tim-response</td>
<td>Enables/disables triggering AIS &amp; RDI on path trace error</td>
</tr>
<tr>
<td>tx-clock-source</td>
<td>Specifies the source of the port’s transmit clock</td>
</tr>
<tr>
<td>shutdown</td>
<td>Administratively disables/ enables the port</td>
</tr>
<tr>
<td>show bind</td>
<td>Display the interfaces that are bound to the port</td>
</tr>
<tr>
<td>show statistics</td>
<td>Display port statistics</td>
</tr>
<tr>
<td>show status</td>
<td>Display port status</td>
</tr>
<tr>
<td>smart-sfp</td>
<td>Provision smart SFP</td>
</tr>
<tr>
<td>type</td>
<td>Assign SFP type</td>
</tr>
</tbody>
</table>
### Command Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>reset</td>
<td>Reset SFP</td>
</tr>
<tr>
<td>show status</td>
<td>Display interface status</td>
</tr>
<tr>
<td>shutdown</td>
<td>Administratively disable-enable interface</td>
</tr>
<tr>
<td>t1</td>
<td>Configure T1 port</td>
</tr>
<tr>
<td>line-code</td>
<td>Specifies the variety of zero code suppression used for this port</td>
</tr>
<tr>
<td>line-length</td>
<td>Specifies the length of the T1 line in DSU mode</td>
</tr>
<tr>
<td>line-type</td>
<td>Specifies the T1 framing mode</td>
</tr>
<tr>
<td>loopback</td>
<td>Enables/disables loopback mode for the specified port</td>
</tr>
<tr>
<td>name</td>
<td>Assigns/removes a port name</td>
</tr>
<tr>
<td>rx-sensitivity</td>
<td>Specifies the attenuation level of the receive signal that is compensated for by the interface receive path</td>
</tr>
<tr>
<td>tx-clock-source</td>
<td>Specifies the source of the port’s transmit clock</td>
</tr>
<tr>
<td>shutdown</td>
<td>Administratively disables/enables the port</td>
</tr>
<tr>
<td>show alarms</td>
<td>Displays alarms</td>
</tr>
<tr>
<td>show bind</td>
<td>Displays a list of interfaces bound to port</td>
</tr>
<tr>
<td>show loopback</td>
<td>Displays loopback test results</td>
</tr>
<tr>
<td>show status</td>
<td>Displays the port status</td>
</tr>
<tr>
<td>show statistics</td>
<td>Displays the port statistics</td>
</tr>
<tr>
<td>clear-statistics</td>
<td>Clears the statistics</td>
</tr>
<tr>
<td>t3</td>
<td>Configure T3 port</td>
</tr>
<tr>
<td>line-length</td>
<td>Specifies the length of the T3 line</td>
</tr>
<tr>
<td>line-type</td>
<td>Specifies type of T3 line</td>
</tr>
<tr>
<td>loopback</td>
<td>Enables/disables loopback mode for the specified port</td>
</tr>
<tr>
<td>name</td>
<td>Assigns/removes a port name</td>
</tr>
<tr>
<td>tx-clock-source</td>
<td>Specifies the source of the port’s transmit clock</td>
</tr>
<tr>
<td>shutdown</td>
<td>Administratively disables/enables the port</td>
</tr>
<tr>
<td>show alarms</td>
<td>Displays alarms</td>
</tr>
<tr>
<td>show bind</td>
<td>Displays a list of interfaces bound to port</td>
</tr>
<tr>
<td>show loopback</td>
<td>Displays loopback test results</td>
</tr>
<tr>
<td>show status</td>
<td>Displays the port status</td>
</tr>
<tr>
<td>show statistics</td>
<td>Displays the port statistics</td>
</tr>
</tbody>
</table>
### Command Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear-statistics</td>
<td>Clears the statistics</td>
</tr>
<tr>
<td>arp-timeout</td>
<td>Enable/disable address aging function</td>
</tr>
<tr>
<td>peer</td>
<td>Create/delete peer</td>
</tr>
<tr>
<td>flows</td>
<td>Enter flows level</td>
</tr>
<tr>
<td>rate-sampling-window</td>
<td>Configure interval for rate sampling statistics</td>
</tr>
<tr>
<td>show summary</td>
<td>Display information for all flows</td>
</tr>
<tr>
<td>classifier-profile</td>
<td>Configure a classifier profile</td>
</tr>
<tr>
<td>match</td>
<td>Specifies the criteria for the classifier profile</td>
</tr>
<tr>
<td>flow</td>
<td>Configure flow</td>
</tr>
<tr>
<td>shutdown</td>
<td>Activate or deactivate the flow</td>
</tr>
<tr>
<td>classifier</td>
<td>Associate the flow with a classifier profile</td>
</tr>
<tr>
<td>drop</td>
<td>Discard traffic transmitted via the flow</td>
</tr>
<tr>
<td>policer</td>
<td>Associate the flow with a policer profile or aggregate</td>
</tr>
<tr>
<td>l2cp</td>
<td>Assign L2CP profile to flow</td>
</tr>
<tr>
<td>mark</td>
<td>Enter marking level for overwriting VLAN or inner VLAN</td>
</tr>
<tr>
<td>vlan</td>
<td>Overwrite VLAN with a new value</td>
</tr>
<tr>
<td>marking-profile</td>
<td>Overwrite p-bit for VLAN as specified by marking profile</td>
</tr>
<tr>
<td>p-bit</td>
<td>Overwrite p-bit for VLAN</td>
</tr>
<tr>
<td>inner-vlan</td>
<td>Overwrite inner VLAN</td>
</tr>
<tr>
<td>inner-marking-profile</td>
<td>Overwrite p-bit for inner VLAN as specified by marking profile</td>
</tr>
<tr>
<td>inner-p-bit</td>
<td>Overwrite p-bit for inner VLAN</td>
</tr>
<tr>
<td>vlan-tag</td>
<td>Perform push/pop of VLAN or inner VLAN, optionally with p-bits</td>
</tr>
<tr>
<td>ingress-port</td>
<td>Define the ingress port of the flow</td>
</tr>
<tr>
<td>egress-port</td>
<td>Define the egress port of the flow</td>
</tr>
<tr>
<td>test</td>
<td>This command puts the specified flow into a loopback mode. The no form of the command disables the specified type of loopback.</td>
</tr>
<tr>
<td>show statistics</td>
<td>Display statistics for the flow</td>
</tr>
<tr>
<td>clear-statistics</td>
<td>Clear statistics for the flow</td>
</tr>
<tr>
<td>show test</td>
<td>Display flow test status</td>
</tr>
<tr>
<td>etps</td>
<td>Enter EVC Termination Point (ETP) level</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>etp</td>
<td>Configure ETP</td>
</tr>
<tr>
<td>clear-statistics</td>
<td>This command clears all statistics of ETP</td>
</tr>
<tr>
<td>port</td>
<td>This command creates an ETP port</td>
</tr>
<tr>
<td>loopback</td>
<td>This command puts the ETP port in loopback mode</td>
</tr>
<tr>
<td>name</td>
<td>Assign name to ETP port</td>
</tr>
<tr>
<td>show status</td>
<td>Display ETP port status</td>
</tr>
<tr>
<td>show loopback</td>
<td>Display loopback status</td>
</tr>
<tr>
<td>shutdown</td>
<td>Activate or deactivate ETP port</td>
</tr>
<tr>
<td>protection</td>
<td>Enter ETP protection level</td>
</tr>
<tr>
<td>aps-protocol</td>
<td>Define APS protocol</td>
</tr>
<tr>
<td>bind</td>
<td>Bind transport port id</td>
</tr>
<tr>
<td>clear</td>
<td>Clears the active near end lockout of Protection, Forced Switch, Manual Switch, WTR state, or Exercise command</td>
</tr>
<tr>
<td>force-switch</td>
<td>Forces normal traffic signal to be selected from the protection transport entity, meaning jump to next port even if it is down</td>
</tr>
<tr>
<td>lockout</td>
<td>This command prevents a working signal from being selected from the protection transport entity, effectively disabling the protection group</td>
</tr>
<tr>
<td>manual-switch</td>
<td>In the absence of failure of working or protection transport entity, forces normal traffic signal to be selected from the protection transport entity, meaning jump to next port only if it is not down</td>
</tr>
<tr>
<td>master-etp</td>
<td>Configure master ETP</td>
</tr>
<tr>
<td>mode</td>
<td>Configure protection mode</td>
</tr>
<tr>
<td>revertive</td>
<td>Indicates if mode is revertive</td>
</tr>
<tr>
<td>sf-trigger</td>
<td>Define signal failure trigger</td>
</tr>
<tr>
<td>wait-to-restore</td>
<td>Define time between recovery and resumption of transmission</td>
</tr>
<tr>
<td>show status</td>
<td>Display protection status</td>
</tr>
<tr>
<td>shutdown</td>
<td>Activate or deactivate ETP protection</td>
</tr>
<tr>
<td>show status</td>
<td>Display ETP status</td>
</tr>
<tr>
<td>show statistics running</td>
<td>Display ETP statistics</td>
</tr>
<tr>
<td>show flows-summary</td>
<td>Display flows corresponding to ETP</td>
</tr>
<tr>
<td>protection</td>
<td>Configure link protection</td>
</tr>
<tr>
<td>ethernet-group</td>
<td>Define Ethernet group</td>
</tr>
</tbody>
</table>
Command Description
bind Add/remove protection and working ports
shutdown Activate or deactivate Ethernet group
oper-mode Define protection mode as 1-to-1 or manual
revertive Define whether port recovery mode is revertive (traffic switched back to the primary port after it recovers)
wait-to-restore Define time between recovery and resumption of transmission
tx-down-duration-upon-flip Define period of time that failed link stops transmitting to report the failure
force-active-port Define if port is forced to be active
show status Display protection status
terminal Configure control port parameters
baud-rate Define control port data rate
timeout Define security timeout
length Define number of rows to display

Table 4-3. Commands in the file category

Command Description
file Enter file level
copy Copy files
swap Swap files
delete Delete file
dir Displays files in base directory
show version Display active, main, and backup software file versions, dates, and times

Table 4-4. Commands in the admin category

Command Description
admin Administrative commands
factory-default Reset the device to factory defaults
reboot Restart the device
user-default Reset the device to user defaults
Table 4-5. Commands in the root category

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear-statistics</td>
<td>Clear statistics for Ethernet ports, flows, and OAM services</td>
</tr>
</tbody>
</table>

Table 4-6. Commands in the global-commands category

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>global-commands</td>
<td>Global commands can be typed at any level</td>
</tr>
<tr>
<td>exit</td>
<td>Return to previous level in the commands hierarchy</td>
</tr>
<tr>
<td>tree</td>
<td>Displays all lower command levels and commands accessible from the current context level, optionally with parameter information</td>
</tr>
<tr>
<td>help</td>
<td>Displays general help, or optionally just the hotkeys and/or global commands</td>
</tr>
<tr>
<td>history</td>
<td>Displays the command history for the current session (by default the history contains the last 10 commands)</td>
</tr>
<tr>
<td>echo</td>
<td>Echo the text that is typed in</td>
</tr>
<tr>
<td>exec</td>
<td>Execute a file, optionally echoing the commands</td>
</tr>
<tr>
<td>logout</td>
<td>Log out this system</td>
</tr>
<tr>
<td>info</td>
<td>Displays information on the current configuration</td>
</tr>
<tr>
<td>ping</td>
<td>Verify the reachability of a remote host</td>
</tr>
<tr>
<td>save</td>
<td>Save user configuration</td>
</tr>
<tr>
<td>trace-route</td>
<td>Determine the route to a destination address</td>
</tr>
</tbody>
</table>

4.3 Working with Telnet and SSH

Typically, the Telnet host is a PC or Unix station with the appropriate suite of TCP/IP protocols.

To enable the Telnet host to communicate with ETX-203A, it is necessary to configure the ETX-203A IP address settings (refer to Chapter 5 for details). This is usually done via a terminal emulation program (see Working with Terminal). After this preliminary configuration, you can use a Telnet host connected directly or via a local area network.
To connect to ETX-203A via Telnet:

1. At the Telnet host, enter the necessary command (e.g. at a PC enter: `
telnet <IP-address>`).

The Telnet login window appears for the device as shown below.

2. Log into the device as explained in *Logging In*. Refer to *Using the CLI* and *Command Tree* for details on using the CLI commands.

---

### 4.4 Working with Third-Party Network Management Systems

ETX-203A can be integrated into third-party network management systems at the following levels:

- Viewing device inventory and receiving traps (see *Chapter 6* for trap list)
- Managing device, including configuration, statistics collection, and diagnostics, using the following standard and private MIBs:
  - CFM MIB (IEEE8021-CFM-MIB)
  - IANAifType-MIB
  - IETF Syslog Device MIB
  - IEEE8023-LAG-MIB
  - MEF-R MIB
  - RAD private MIB
  - RFC 2819 (RMON-MIB)
  - RFC 2863 (IF-MIB)
  - RFC 3273 (Remote Network Monitoring MIB)
  - RFC 3411 (SNMP-FRAMEWORK-MIB)
  - RFC 3413 (SNMP-TARGET-MIB)
  - RFC 3414 (SNMP-USER-BASED-SM-MIB)
  - RFC 3415 (SNMP-VIEW-BASED-ACM-MIB)
• RFC 3418 (SNMPv2-MIB)
• RFC 3433 (ENTITY-SENSOR-MIB)
• RFC 3636 (MAU-MIB)
• RFC 4133 (ENTITY-MIB)
• RFC 4668 (RADIUS-AUTH-CLIENT-MIB)
• RFC 4836.MIB (MAU-MIB)
• RFC 4878.MIB (DOT3-OAM-MIB).

4.5 Services and Features

Usually, initial configuration of the management parameters is performed via
ASCII terminal. Once the ETX-203A host IP parameters have been set and the
management flows to/from the host have been defined, it is possible to access it
via Telnet or RADview for operation configuration. Configure the following in
order to prepare ETX-203A for management (refer to Chapter 5 for details):

• Host IP Settings
• Network Managers
• SNMP Management
• Management Flows
• Device Information
• Management Access
• Access Policy
• Authentication via RADIUS Server
• Authentication via TACACS+ Server
• Terminal Control Port
• User Access.
Chapter 5

Configuration

This chapter lists the commands used to configure ETX-203A and explains their parameters.

This chapter includes the following sections:

- Services
- Layer 2 Control Processing
- Ethernet Ports
- E1 Ports
- T1 Ports
- E3 Ports
- T3 Ports
- SDH/SONET Ports
- GFP Ports
- Logical MAC Ports
- Smart SFPs
- Network Interface Redundancy
- Ethernet Linear Protection
- Quality of Service (QoS)
- Flows
- Ethernet OAM
- Fault Propagation
- Date and Time
- Syslog
- Clearing Device Statistics
- Working with the Inventory
- Displaying Environment
- Displaying Software Versions
- Displaying CPU and Memory Utilization
- File Operations
- Saving Configuration
- Reset.
For a list of commands and their context, refer to Chapter 3.

Note
When you enter a level that causes the creation of a dynamic entity, § is displayed at the end of the prompt until you exit the entity level. The next time you enter the entity level, # is displayed at the end of the prompt. For the purposes of illustration, # is usually shown at the end of the prompts in this chapter. Examples of dynamic entities include QoS profiles and OAM CFM entities.

5.1 Services

This section shows the data flow and configuration steps for services.

Ethernet Management Traffic

Ethernet to Host

The following figure illustrates the data flow for Ethernet management traffic from an Ethernet port to the host port. Table 5-1 shows the configuration steps corresponding to the figure callouts.

![Figure 5-1. Ethernet Management Traffic Data Flow – Ethernet to Host](image)

Table 5-1. Ethernet Management Traffic Configuration – Ethernet to Host

<table>
<thead>
<tr>
<th>Callout</th>
<th>Step</th>
<th>Commands</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Defining Classifier Profiles</td>
<td>classifier-profile match</td>
<td>The classifier profile defines the criteria for the incoming management flow</td>
</tr>
<tr>
<td>2</td>
<td>Marking Profiles</td>
<td>marking-profile mark</td>
<td>Necessary only if a profile is needed for non-default mapping of p-bit, IP precedence, DSCP, or CoS classifications to egress priority tags for the incoming management flow</td>
</tr>
<tr>
<td>3</td>
<td>Queue Mapping Profiles</td>
<td>queue-map-profile map</td>
<td>Necessary only if a profile is needed for non-default mapping of user priorities to queues for the incoming management flow</td>
</tr>
<tr>
<td>4</td>
<td>Configuring Policer Profiles</td>
<td>policer-profile bandwidth compensation</td>
<td>Necessary only if you need to define non-default bandwidth limits or overhead compensation for the incoming management flow</td>
</tr>
</tbody>
</table>
### Host to Ethernet

The following figure illustrates the data flow for Ethernet management traffic from the host port to an Ethernet port. *Table 5-2* shows the configuration steps corresponding to the figure callouts.

**Figure 5-2. Ethernet Management Traffic Data Flow – Host to Ethernet**

**Table 5-2. Ethernet Management Traffic Configuration – Host to Ethernet**

<table>
<thead>
<tr>
<th>Callout</th>
<th>Step</th>
<th>Commands</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>Defining Classifier Profiles</strong></td>
<td>classifier-profile match</td>
<td>The classifier profile defines the criteria for the outgoing management flow</td>
</tr>
<tr>
<td>2</td>
<td><strong>Marking Profiles</strong></td>
<td>marking-profile mark</td>
<td>Necessary only if a profile is needed for non-default mapping of p-bit, IP precedence, DSCP, or CoS classifications to egress priority tags for the outgoing management flow</td>
</tr>
<tr>
<td>3</td>
<td><strong>Queue Mapping Profiles</strong></td>
<td>queue-map-profile map</td>
<td>Necessary only if a profile is needed for non-default mapping of user priorities to queues for the outgoing management flow</td>
</tr>
<tr>
<td>Callout</td>
<td>Step</td>
<td>Commands</td>
<td>Comments</td>
</tr>
<tr>
<td>---------</td>
<td>-----------------</td>
<td>-----------------------------------</td>
<td>--------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>4</td>
<td>Configuring Policer Profiles</td>
<td>policer-profile</td>
<td>Necessary only if you need to define non-default bandwidth limits or overhead compensation for the outgoing management flow</td>
</tr>
<tr>
<td></td>
<td></td>
<td>bandwidth compensation</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Configuring Queue Block Profile Parameters</td>
<td>queue-block-profile</td>
<td>Necessary only if you need to define non-default queue configuration for the outgoing management flow, or the egress port</td>
</tr>
<tr>
<td></td>
<td></td>
<td>queue scheduling</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>depth</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>WRED Profiles</td>
<td>wred-profile</td>
<td>Necessary only if you need to define non-default WRED configuration for the queue blocks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>color</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Configuring Flows</td>
<td>classifier</td>
<td>You must define the flow for the management traffic from the host port to the Ethernet port</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ingress-port</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>egress-port</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>policer</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>mark</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>vlan-tag</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>shutdown</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Configuring Shaper Profiles</td>
<td>shaper-profile</td>
<td>Necessary only if you need to define non-default bandwidth limits or overhead compensation for the outgoing traffic of the user-to-network flow (via attaching shaper profile to queue group profile attached to egress port)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>bandwidth compensation</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Queue Group Profiles</td>
<td>queue-group-profile</td>
<td>Necessary only if you need to define non-default queue group configuration for the egress port</td>
</tr>
<tr>
<td></td>
<td></td>
<td>queue-block</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>name</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>profile</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>shaper</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Ethernet Ports</td>
<td>name</td>
<td>Necessary only if you need to define non-default configuration for the egress port</td>
</tr>
<tr>
<td></td>
<td></td>
<td>auto-negotiation</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>max-capability</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>speed-duplex</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>queue-group</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>egress-mtu</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>tag-ethernet-type</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>shutdown</td>
<td></td>
</tr>
</tbody>
</table>
**Ethernet User Traffic**

**Network to User**

In *Figure 5-3* the rectangles illustrate the data flow for Ethernet user traffic from a network port to a user port. The rounded rectangles indicate the features that need to be configured, numbered according to the order of configuration. *Table 5-3* shows the configuration steps corresponding to the numbers.

![Image of Ethernet User Traffic Data Flow - Network to User](image)

*Figure 5-3. Ethernet User Traffic Data Flow – Network to User*

**Table 5-3. Ethernet User Traffic Configuration – Network to User**

<table>
<thead>
<tr>
<th>Sequence</th>
<th>Step</th>
<th>Commands</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>Defining Classifier Profiles</strong></td>
<td>classifier-profile</td>
<td>The classifier profile defines the criteria for the network-to-user flow</td>
</tr>
<tr>
<td></td>
<td></td>
<td>match</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td><strong>Marking Profiles</strong></td>
<td>marking-profile</td>
<td>Necessary only if a profile is needed for non-default mapping of p-bit, IP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mark</td>
<td>precedence, DSCP, or CoS classifications to egress priority tags for the</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>network-to-user flow</td>
</tr>
<tr>
<td>3</td>
<td><strong>Queue Mapping Profiles</strong></td>
<td>queue-map-profile</td>
<td>Necessary only if a profile is needed for non-default mapping of user</td>
</tr>
<tr>
<td></td>
<td></td>
<td>map</td>
<td>priorities to queues for the network-to-user flow</td>
</tr>
<tr>
<td>4</td>
<td><strong>Configuring Policer Profiles</strong></td>
<td>policer-profile</td>
<td>Necessary only if you need to define non-default bandwidth limits or</td>
</tr>
<tr>
<td></td>
<td></td>
<td>bandwidth compensation</td>
<td>overhead compensation for the incoming traffic of the network-to-user flow</td>
</tr>
<tr>
<td>5</td>
<td><strong>Configuring Queue Block Profile Parameters</strong></td>
<td>queue-block-profile</td>
<td>Necessary only if you need to define non-default queue configuration for</td>
</tr>
<tr>
<td></td>
<td></td>
<td>queue</td>
<td>the network-to-user flow</td>
</tr>
<tr>
<td></td>
<td></td>
<td>scheduling</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>depth</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td><strong>WRED Profiles</strong></td>
<td>wred-profile</td>
<td>Necessary only if you need to define non-default WRED configuration for</td>
</tr>
<tr>
<td></td>
<td></td>
<td>color</td>
<td>the queue blocks</td>
</tr>
</tbody>
</table>

---

ETX-203A Ver. 3.0 Services 5-5
### Chapter 5  Configuration Installation and Operation Manual

#### 5-6 Services ETX-203A Ver. 3.0

<table>
<thead>
<tr>
<th>Sequence</th>
<th>Step</th>
<th>Commands</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Configuring Flows</td>
<td>classifier ingress-port egress-port policer mark vlan-tag shutdown</td>
<td>You must define the flow for the user traffic from the network port to the user port</td>
</tr>
<tr>
<td>8</td>
<td>Configuring Shaper Profiles</td>
<td>shaper-profile bandwidth compensation</td>
<td>Necessary only if you need to define non-default bandwidth limits or overhead compensation for the outgoing traffic of the network-to-user flow (via attaching shaper profile to queue group profile attached to egress port)</td>
</tr>
<tr>
<td>9</td>
<td>Queue Group Profiles</td>
<td>queue-group-profile queue-block name profile shaper</td>
<td>Necessary only if you need to define non-default queue group configuration for the egress port</td>
</tr>
<tr>
<td>10</td>
<td>Ethernet Ports</td>
<td>name auto-negotiation max-capability speed-duplex queue-group egress-mtu tag-ethernet-type shutdown</td>
<td>Necessary only if you need to define non-default configuration for the ingress or egress port</td>
</tr>
</tbody>
</table>

**User to Network**

In Figure 5-4 the rectangles illustrate the data flow for Ethernet user traffic from a network port to a user port. The rounded rectangles indicate the features that need to be configured, numbered according to the order of configuration. *Table 5-4* shows the configuration steps corresponding to the numbers.

*Figure 5-4. Ethernet User Traffic Data Flow – User to Network*
### Table 5-4. Ethernet User Traffic Configuration – User to Network

<table>
<thead>
<tr>
<th>Callout</th>
<th>Step</th>
<th>Commands</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Defining Classifier Profiles</td>
<td>classifier-profile</td>
<td>The classifier profile defines the criteria for the user-to-network flow</td>
</tr>
<tr>
<td></td>
<td></td>
<td>match</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Marking Profiles</td>
<td>marking-profile</td>
<td>Necessary only if a profile is needed for non-default mapping of p-bit,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mark</td>
<td>IP precedence, DSCP, or CoS classifications to egress priority tags</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>for the user-to-network flow</td>
</tr>
<tr>
<td>3</td>
<td>Queue Mapping Profiles</td>
<td>queue-map-profile</td>
<td>Necessary only if a profile is needed for non-default mapping of user</td>
</tr>
<tr>
<td></td>
<td></td>
<td>map</td>
<td>priorities to queues for the user-to-network flow</td>
</tr>
<tr>
<td>4</td>
<td>Configuring Policer Profiles</td>
<td>policer-profile</td>
<td>Necessary only if you need to define non-default bandwidth limits or</td>
</tr>
<tr>
<td></td>
<td></td>
<td>bandwidth</td>
<td>overhead compensation for the incoming traffic of the user-to-network</td>
</tr>
<tr>
<td></td>
<td></td>
<td>compensation</td>
<td>flow</td>
</tr>
<tr>
<td>5</td>
<td>Configuring Queue Block Profile Parameters</td>
<td>queue-block-profile</td>
<td>Necessary only if you need to define non-default queue configuration for</td>
</tr>
<tr>
<td></td>
<td></td>
<td>queue</td>
<td>the user-to-network flow, or the egress port</td>
</tr>
<tr>
<td></td>
<td></td>
<td>scheduling</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>depth</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>WRED Profiles</td>
<td>wred-profile</td>
<td>Necessary only if you need to define non-default WRED configuration for</td>
</tr>
<tr>
<td></td>
<td></td>
<td>color</td>
<td>the queue blocks</td>
</tr>
<tr>
<td>7</td>
<td>Configuring Flows</td>
<td>classifier</td>
<td>You must define the flow for the user traffic from the user port to the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ingress-port</td>
<td>network port</td>
</tr>
<tr>
<td></td>
<td></td>
<td>egress-port</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>policer</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>mark</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>vlan-tag</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>shutdown</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Configuring Shaper Profiles</td>
<td>shaper-profile</td>
<td>Necessary only if you need to define non-default bandwidth limits or</td>
</tr>
<tr>
<td></td>
<td></td>
<td>bandwidth</td>
<td>overhead compensation for the outgoing traffic of the user-to-network</td>
</tr>
<tr>
<td></td>
<td></td>
<td>compensation</td>
<td>flow (via attaching shaper profile to queue group profile attached to</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>egress port)</td>
</tr>
</tbody>
</table>
TDM User Traffic

**TDM Network to Ethernet User**

The following figure illustrates the data flow for Ethernet user traffic from a network port provisioned as a TDM port via a smart SFP, to an Ethernet user port. *Table 5-5* shows the configuration steps corresponding to the figure callouts.

![TDM User Traffic Data Flow - TDM Network to Ethernet User](image)

*Figure 5-5.  TDM User Traffic Data Flow – TDM Network to Ethernet User*

*Table 5-5.  TDM User Traffic Configuration – TDM Network to Ethernet User*

<table>
<thead>
<tr>
<th>Callout</th>
<th>Step</th>
<th>Commands</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>Queue Group Profiles</td>
<td>queue-group-profile queue-block name profile shaper</td>
<td>Necessary only if you need to define non-default queue group configuration for the egress port</td>
</tr>
<tr>
<td>10</td>
<td>Ethernet Ports</td>
<td>name auto-negotiation max-capability speed-duplex queue-group egress-mtu tag-ethernet-type shutdown</td>
<td>Necessary only if you need to define non-default configuration for the ingress or egress port</td>
</tr>
</tbody>
</table>

**Callout Step Commands Comments**

<table>
<thead>
<tr>
<th>Callout</th>
<th>Step</th>
<th>Commands</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Smart SFPs</td>
<td>smart-sfp type shutdown</td>
<td>You must provision the smart SFP for the network port</td>
</tr>
<tr>
<td>Callout</td>
<td>Step</td>
<td>Commands</td>
<td>Comments</td>
</tr>
<tr>
<td>---------</td>
<td>----------------</td>
<td>-------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>2</td>
<td><strong>E1 Ports</strong></td>
<td>e1 name line-code line-type rx-sensitivity tx-clock-source shutdown</td>
<td>Necessary only if non-default configuration is needed for the TDM port Note: The specific step is according to the TDM port type.</td>
</tr>
<tr>
<td></td>
<td><strong>T1 Ports</strong></td>
<td>t1 name line-code line-length line-type rx-sensitivity tx-clock-source shutdown</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>E3 Ports</strong></td>
<td>e3 name tx-clock-source shutdown</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>T3 Ports</strong></td>
<td>t3 name line-length line-type shutdown</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>SDH/SONET Ports</strong></td>
<td>sdh-sonet name frame-type threshold tim-response tx-clock-source shutdown</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td><strong>GFP Ports</strong></td>
<td>gfp bind fcs-payload name</td>
<td>You must configure a GFP port, and bind the TDM port to it</td>
</tr>
<tr>
<td>Callout</td>
<td>Step</td>
<td>Commands</td>
<td>Comments</td>
</tr>
<tr>
<td>---------</td>
<td>------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>4</td>
<td>Logical MAC Ports</td>
<td>logical-mac name, bind, egress-mtu, queue-group, tag-ethernet-type, shutdown</td>
<td>You must configure a logical MAC port, and bind the GFP port to it. The logical MAC port is used as the ingress port of the flow.</td>
</tr>
<tr>
<td>5</td>
<td>Defining Classifier Profiles</td>
<td>classifier-profile match</td>
<td>The classifier profile defines the criteria for the network-to-user flow.</td>
</tr>
<tr>
<td>6</td>
<td>Marking Profiles</td>
<td>marking-profile mark</td>
<td>Necessary only if a profile is needed for non-default mapping of p-bit, IP precedence, DSCP, or CoS classifications to egress priority tags for the network-to-user flow.</td>
</tr>
<tr>
<td>7</td>
<td>Queue Mapping Profiles</td>
<td>queue-map-profile map</td>
<td>Necessary only if a profile is needed for non-default mapping of user priorities to queues for the network-to-user flow.</td>
</tr>
<tr>
<td>8</td>
<td>Configuring Policer Profiles</td>
<td>policer-profile bandwidth compensation</td>
<td>Necessary only if you need to define non-default bandwidth limits or overhead compensation for the incoming traffic of the network-to-user flow.</td>
</tr>
<tr>
<td>9</td>
<td>Configuring Queue Block Profile Parameters</td>
<td>queue-block-profile queue, scheduling depth</td>
<td>Necessary only if you need to define non-default queue configuration for the network-to-user flow.</td>
</tr>
<tr>
<td>10</td>
<td>WRED Profiles</td>
<td>wred-profile color</td>
<td>Necessary only if you need to define non-default WRED configuration for the queue blocks.</td>
</tr>
<tr>
<td>11</td>
<td>Configuring Flows</td>
<td>classifier ingress-port egress-port policer mark vlan-tag shutdown</td>
<td>You must define the flow for the user traffic from the network port (logical MAC port) to the user port.</td>
</tr>
</tbody>
</table>
### TDM User to Network

The following figure illustrates the data flow for Ethernet user traffic from a user port provisioned as a TDM port via a smart SFP, to an Ethernet network port. Table 5-4 shows the configuration steps corresponding to the figure callouts.

![Figure 5-6. TDM User Traffic Data Flow – TDM User to Ethernet Network](image)

**Figure 5-6. TDM User Traffic Data Flow – TDM User to Ethernet Network**

<table>
<thead>
<tr>
<th>Callout</th>
<th>Step</th>
<th>Commands</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>Configuring Shaper Profiles</td>
<td>shaper-profile</td>
<td>Necessary only if you need to define non-default bandwidth limits or overhead compensation for the outgoing traffic of the network-to-user flow (via attaching shaper profile to queue group profile attached to egress port)</td>
</tr>
<tr>
<td>13</td>
<td>Queue Group Profiles</td>
<td>queue-group-profile</td>
<td>Necessary only if you need to define non-default queue group configuration for the egress port</td>
</tr>
<tr>
<td>14</td>
<td>Ethernet Ports</td>
<td>name</td>
<td>Necessary only if you need to define non-default configuration for the egress port</td>
</tr>
</tbody>
</table>

**Table 5-4. TDM User Traffic Configuration – TDM User to Ethernet Network**

<table>
<thead>
<tr>
<th>Callout</th>
<th>Step</th>
<th>Commands</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>Configuring Shaper Profiles</td>
<td>shaper-profile</td>
<td>Necessary only if you need to define non-default bandwidth limits or overhead compensation for the outgoing traffic of the network-to-user flow (via attaching shaper profile to queue group profile attached to egress port)</td>
</tr>
<tr>
<td>13</td>
<td>Queue Group Profiles</td>
<td>queue-group-profile</td>
<td>Necessary only if you need to define non-default queue group configuration for the egress port</td>
</tr>
<tr>
<td>14</td>
<td>Ethernet Ports</td>
<td>name</td>
<td>Necessary only if you need to define non-default configuration for the egress port</td>
</tr>
</tbody>
</table>

**Table 5-6. TDM User Traffic Configuration – TDM User to Ethernet Network**

<table>
<thead>
<tr>
<th>Callout</th>
<th>Step</th>
<th>Commands</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Smart SFPs</td>
<td>smart-sfp</td>
<td>You must provision the smart SFP for the user port</td>
</tr>
<tr>
<td></td>
<td></td>
<td>type</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>shutdown</td>
<td></td>
</tr>
<tr>
<td>Callout</td>
<td>Step</td>
<td>Commands</td>
<td>Comments</td>
</tr>
<tr>
<td>--------</td>
<td>---------------</td>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| 2      | **E1 Ports**  | `e1` `name` `line-code` `line-type` `rx-sensitivity` `tx-clock-source` `shutdown` | Necessary only if non-default configuration is needed for the TDM port.  
*Note:* The specific step is according to the TDM port type. |
|        | **T1 Ports**  | `t1` `name` `line-code` `line-length` `line-type` `rx-sensitivity` `tx-clock-source` `shutdown` |                                                                 |
|        | **E3 Ports**  | `e3` `name` `tx-clock-source` `shutdown` |                                                                 |
|        | **T3 Ports**  | `t3` `name` `line-length` `line-type` `shutdown` |                                                                 |
|        | **SDH/SONET Ports** | `sdh-sonet` `name` `frame-type` `threshold` `tim-response` `tx-clock-source` `shutdown` |                                                                 |
| 3      | **GFP Ports** | `gfp` `bind` `fcs-payload` `name` | You must configure a GFP port, and bind the TDM port to it. |
### Callout 4: Logical MAC Ports

<table>
<thead>
<tr>
<th>Step</th>
<th>Commands</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>logical-mac name</td>
<td>You must configure a logical MAC port, and bind the GFP port to it. The logical MAC port is used as the ingress port of the flow</td>
</tr>
<tr>
<td></td>
<td>bind egress-mtu queue-group tag-ethernet-type shutdown</td>
<td></td>
</tr>
</tbody>
</table>

### Callout 5: Defining Classifier Profiles

<table>
<thead>
<tr>
<th>Step</th>
<th>Commands</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>classifier-profile match</td>
<td>The classifier profile defines the criteria for the user-to-network flow</td>
</tr>
</tbody>
</table>

### Callout 6: Marking Profiles

<table>
<thead>
<tr>
<th>Step</th>
<th>Commands</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>marking-profile mark</td>
<td>Necessary only if a profile is needed for non-default mapping of p-bit, IP precedence, DSCP, or CoS classifications to egress priority tags for the user-to-network flow</td>
</tr>
</tbody>
</table>

### Callout 7: Queue Mapping Profiles

<table>
<thead>
<tr>
<th>Step</th>
<th>Commands</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>queue-map-profile map</td>
<td>Necessary only if a profile is needed for non-default mapping of user priorities to queues for the user-to-network flow</td>
</tr>
</tbody>
</table>

### Callout 8: Configuring Policer Profiles

<table>
<thead>
<tr>
<th>Step</th>
<th>Commands</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>policer-profile bandwidth compensation</td>
<td>Necessary only if you need to define non-default bandwidth limits or overhead compensation for the incoming traffic of the user-to-network flow</td>
</tr>
</tbody>
</table>

### Callout 9: Configuring Queue Block Profile Parameters

<table>
<thead>
<tr>
<th>Step</th>
<th>Commands</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>queue-block-profile queue scheduling depth</td>
<td>Necessary only if you need to define non-default queue configuration for the user-to-network flow, or the egress port</td>
</tr>
</tbody>
</table>

### Callout 10: WRED Profiles

<table>
<thead>
<tr>
<th>Step</th>
<th>Commands</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>wred-profile color</td>
<td>Necessary only if you need to define non-default WRED configuration for the queue blocks</td>
</tr>
</tbody>
</table>

### Callout 11: Configuring Flows

<table>
<thead>
<tr>
<th>Step</th>
<th>Commands</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>classifier ingress-port egress-port policer mark vlan-tag shutdown</td>
<td>You must define the flow for the user traffic from the user port to the network port</td>
</tr>
</tbody>
</table>
5.2 Configuring the Host IP Settings

ETX-203A can be managed by a network management station, located on the LAN and connected to one of the unit’s Ethernet ports. In order to establish a proper connection, it is necessary to configure the host IP address, subnet mask, and default gateway. In addition, for management you must define flows between the host and network port with the following conditions (refer to the Quick Start Guide for an example of defining management flows):

- The flow to the host should use classification untagged, or tagged with the management VLAN if applicable
- The flow from the host should forward all traffic (classification “all”), with push action of the management VLAN and priority if applicable
- The flows to/from the host can also use classification VLAN + inner VLAN.

You can obtain the host IP parameters via DHCP if enabled, otherwise you can configure the host IP parameters manually.

Working with DHCP

To facilitate integration of a new device into a DHCP IP network, if DHCP is enabled then ETX-203A requests IP host parameters from the DHCP server upon booting up. ETX-203A is shipped with the DHCP client enabled.
Disabling DHCP

To disable the DHCP client:
1. Navigate to `configure management host 1`.
   The `config>mngmnt>host(1)#` prompt is displayed.
2. Enter `no dhcp`.

   ETX-203A resets the host IP address to 0.0.0.0, while preserving the IP mask and default gateway values. Telnet/SSH connections to ETX-203A are terminated. The unit is not accessible via Internet until you manually configure an IP address and default gateway, unless you entered a default IP address previously with the `dhcp` command.

Enabling DHCP

To enable DHCP, remove the defined host IP address and default gateway, and then enable DHCP.

To enable the DHCP client and acquire IP parameters:
1. Navigate to `configure management host 1`.
   The `config>mngmnt>host(1)#` prompt is displayed.
2. Enter the following commands:
   ```
   no ip-address
   no default-gateway
   ```
   The IP address and mask are set to 0.0.0.0, and the default gateway is removed.

   ETX-203A starts broadcasting requests for an IP address. When the DHCP server is found, ETX-203A receives from it all necessary host IP parameters. If specified, a default IP address is associated with ETX-203A in the event the DHCP server is unavailable.

   **Note** When the IP address lease is about to expire, the DHCP client automatically requests a lease extension.

Setting Host IP Parameters

You can enter the host IP address and default gateway manually when DHCP is disabled. You can also specify the ARP timeout.

To define the IP parameters manually:
1. Navigate to `configure management host 1`.

---

**Note** To enable IP connectivity in DHCP mode, make sure that the relevant port has been made accessible.

**Note** When you navigate to the host context you provide a host index that is always 1.
The config>mngmnt>host(1)# prompt is displayed.

**Note**

*When you navigate to the host context, you provide a host index that is always 1.*

2. Enter all necessary commands according to the tasks listed below.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defining the host IP address</td>
<td>ip-address &lt;host-IP-address&gt;/&lt;IP-mask&gt;</td>
<td>The IP mask is a decimal number that specifies the number of high-order consecutive bits set to 1 in the mask (refer to example below). For example, to define IP address 192.178.1.175 with IP mask 255.255.255.0, enter: ip-address 192.178.1.175/24</td>
</tr>
<tr>
<td>Defining the default gateway IP address</td>
<td>default-gateway &lt;gateway-IP-address&gt;</td>
<td>The default gateway must be in the same subnet as the host</td>
</tr>
<tr>
<td>Specifying the ARP timeout</td>
<td>arp-timeout &lt;seconds&gt;</td>
<td>The value can be 300–1,000,000</td>
</tr>
<tr>
<td>Displaying the host IP settings</td>
<td>show status</td>
<td></td>
</tr>
</tbody>
</table>

### 5.3 Configuring Device Information

The ETX-203A management software allows you to assign a name to the unit, add its description, specify its location to distinguish it from the other devices installed in your system, and assign a contact person.

➢ To configure device information:

1. Navigate to **configure system**.

   The config>system# prompt is displayed.

2. Enter the necessary commands according to the tasks listed below.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assigning device name</td>
<td>name &lt;device-name&gt;</td>
<td>The device name has unlimited length, but if you enter a name with more than 20 characters, the prompt displays only the first 20 characters followed by 0. For example, this command that defines a 25-character device name: ETX-203A# config sys name ETXETXETXETXETX-203A12345 results in this prompt that shows the first 20 characters, followed by 0: ETXETXETXETXETX-203A0#</td>
</tr>
<tr>
<td>Specifying location</td>
<td>location &lt;device-location&gt;</td>
<td></td>
</tr>
<tr>
<td>Specifying contact person</td>
<td>contact &lt;contact-person&gt;</td>
<td></td>
</tr>
<tr>
<td>Task</td>
<td>Command</td>
<td>Comments</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>-----------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Displaying device information, MAC address, and amount of time device has been running</td>
<td>show device-information</td>
<td></td>
</tr>
</tbody>
</table>

**Example**

- To configure device information:
  - Device name – ETX-203A-HAC
  - Location – floor-8
  - Contact – Engineer-1.

```
ETX-203A# configure system
ETX-203A>config>system# name ETX-203A-HAC
ETX-203A-HAC >config>system# location floor-8
ETX-203A-HAC >config>system# contact Engineer-1
ETX-203A-HAC >config>system# show device-information
```

**Description**: ETH NTU: Boot; 1.10, Hw: 0.0, Main Sw: 3.0, Back-up Sw: 3.0  
Name: ETX-203A-HAC  
Location: floor-8  
Contact: Engineer-1  
MAC Address: 00-20-D2-30-CC-9D  
Sysup Time: 000:00:04:10

### 5.4 SNMP Management

SNMP stands for Simple Network Management Protocol and is an application layer protocol that provides a message format for communication between managers and agents.

ETX-203A supports SNMPv3, the latest SNMP version to date. SNMPv3 provides secure access to devices in the network such as ACE units by using authentication and data encryption.

If you intend to manage ETX-203A via SNMPv1, you have to specify the SNMP read, write, and trap communities (SNMPv3 must be disabled). If you wish to use SNMPv3, you have to ensure that it is enabled, then specify the necessary parameters.

Refer to **Setting SNMP Communities** for details on setting the communities, or to **Configuring SNMPv3** for details on setting SNMPv3 parameters.

**Note**

To check if SNMPv3 is enabled or disabled, navigate to **configure management snmp** and type `info detail`, then locate the line in the output that contains either `snmpv3` (SNMPv3 is enabled) or `no snmpv3` (SNMPv3 is not enabled). To enable or disable SNMPv3, refer to **Enabling or Disabling SNMPv3**.
Standards

The supported SNMP versions are based on the following standards:

- RFC 1901, Introduction to Community-Based SNMPv2. SNMPv2 Working Group.
- RFC 2104, Keyed Hashing for Message Authentication.
- RFC 2271, Architecture for Describing SNMP Management Frameworks.
- RFC 2272, message processing and dispatching for the Simple Network Management Protocol (SNMP).
- RFC 2273, SNMPv3 Applications.
- RFC 2274, User-Based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3).
- RFC 2275, View-Based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP).
- RFC 3412, Version 3 Message Processing and Dispatching.
- RFC 3414, User-based Security Model for SNMPv3
- RFC 3416, Update for RFC 1904.

Benefits

The SNMP protocol allows you to remotely manage multiple units from a central workstation using a network management system.

The SNMPv3 protocol allows data to be collected securely from SNMP devices. Confidential information such as SNMP commands can thus be encrypted to prevent unauthorized parties from being able to access them.
**Functional Description**

In an SNMP configuration, one or more administrative computers manage a group of hosts or devices. Each managed system continuously executes a software component called agent, which reports information via SNMP back to the managing workstations.

**Factory Defaults**

The following is the default configuration of the SNMP parameters:

- SNMPv3 not enabled
- SNMP engine ID set to device MAC address
- Read community = "public"
- Write community = "private"
- Trap community = "public"
- No traps masked
- No delay in sending traps.

**Enabling or Disabling SNMPv3**

1. Navigate to `configure management snmp`. The `config>mngmnt>snmp#` prompt is displayed.
2. Type `snmpv3.`

SNMPv3 is enabled, and SNMPv3 commands are available. The manager list is deleted.

**Note**

*If the SNMP management access is set to managers only, the ETX-203A device is not accessible from NMS stations due to the manager list being deleted. To prevent this, you should change the SNMP management access to allow access by all before enabling SNMPv3. Refer to Controlling Management Access for details on changing management access.*

1. Navigate to `configure management snmp`. The `config>mngmnt>snmp#` prompt is displayed.
2. Type `no snmpv3`.

SNMPv3 is disabled, and the commands for setting SNMPv1 communities are available.

**Setting SNMP Communities**

To establish a proper management link when working with SNMPv1, you have to specify the SNMP read, write, and trap communities.
The read, write, and trap communities cannot be set if SNMPv3 is enabled. Refer to Enabling or Disabling SNMPv3 for the procedure to disable it.

You can specify the community with read-only authorization, the community with write authorization, and the community to which ETX-203A sends traps.

To configure ETX-203A communities:

1. Navigate to configure management snmp.

   The `config>mngmnt>snmp#` prompt is displayed.

2. To specify the communities, enter:

   `community [read <read-community>] [write <write-community>] [trap <trap-community>].`

SNMPv3 Default Configuration

The following is the default configuration of the SNMPv3 parameters (refer to Configuring SNMPv3 Parameters for explanations of the parameters):

- SNMP engine ID set to device MAC address
- View named “internet” providing access to IETF MIBs and IEEE MIBs
- View named “restricted” providing access to part of IETF MIBs and IEEE MIBs
- View named “STD_v1” providing access to IETF MIBs and IEEE MIBs, excluding part of SNMPv3 MIB
- User named "initial", with security level no authentication and no privacy
- Group for SNMPv3 named "initial":
  - Security levels: no authentication and no privacy, authentication and no privacy, authentication and privacy
  - User: “initial”
  - Views for read/write/notify: "internet".
- Group for SNMPv1 named “v1_read”:
  - Security level: no authentication and no privacy
  - Read view = “STD_v1”
  - Write view = “”
  - Notify view = “internet”
- Group for SNMPv1 named “v1_write”:
  - Security level: no authentication and no privacy
  - Read view = “STD_v1”
  - Write view = “STD_v1”
  - Notify view = “internet”
- Group for SNMPv1 named “v1_trap”:
  - Security level: no authentication and no privacy
- Read view = ""
- Write view = ""
- Notify view = "internet".
- Target named "OAM_1":
  - Target parameter set = "SNMPv1Param"
  - Tag: "traps"
- Notifications with tag “unmasked” for following traps: agnPowerFailureTrap, agnStatusChangeTrap, agnUploadDataTrap, authenticationFailure, coldStart, ethOamCfmDefectCondition, failedLogin, fallingAlarm, linkDown, linkUp, prtStatusChangeTrap, risingAlarm, successfulLogin, tftpStatusChangeTrap, warmStart
- No delay in sending traps.

**Configuring SNMPv3 Parameters**

ETX-203A supports SNMP version 3, providing secure SNMP access to the device by authenticating and encrypting packets transmitted over the network.

The ETX-203A default configuration provides one standard user named "initial" with no encryption and the lowest security level (refer to **SNMPv3 Default Configuration** for details).

Follow this procedure to configure SNMPv3:

1. Set SNMP engine ID if necessary
2. Add users, specifying authentication protocol and privacy protocol
3. Add groups, specifying security level and protocol
4. Connect users to groups
5. Add notification entries with assigned traps and tags
6. Configure target parameter sets to be used for targets
7. Configure targets (SNMPv3 network management stations to which ETX-203A should send trap notifications), specifying target parameter sets and notification tags
8. If there are devices working with SNMPv1, add communities that work with SNMPv1.

**Note**
The SNMPv3 parameters can be set only when SNMPv3 is enabled (refer to **Enabling or Disabling SNMPv3** for the procedure to enable it).

➢ To configure SNMPv3 parameters:
1. Navigate to configure management snmp.
   - The `config>mngmnt>snmp#` prompt is displayed.
2. Enter all necessary commands according to the tasks listed below.
### SNMP Management

**ETX-203A Ver. 3.0**

When you enter password parameters, they should contain at least eight characters.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Level</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting SNMP engine ID, as MAC address or IP address or string</td>
<td>snmp-engine-id mac [ &lt;mac-address&gt; ]</td>
<td>snmp</td>
<td>If you use the mac option and don’t specify the MAC address, the SNMP engine ID is set to the device MAC address. If you use the ipv4 option and don’t specify the IP address, the SNMP engine ID is set to the device IP address.</td>
</tr>
<tr>
<td></td>
<td>snmp-engine-id ipv4 [ &lt;ip-address&gt; ]</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>snmp-engine-id text &lt;string&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configuring user</td>
<td>user &lt;security-name&gt;</td>
<td>snmp</td>
<td>If you don’t specify the authentication method when creating a user, the default is MD5 with DES privacy protocol. To create a user with no authentication, specify none-auth. Typing no user &lt;security-name&gt; deletes the user.</td>
</tr>
<tr>
<td></td>
<td>[md5-auth [ {des</td>
<td>none} ] ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>user &lt;security-name&gt; [sha-auth [ {des</td>
<td>none} ] ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>user &lt;security-name&gt; [none-auth]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Setting user authentication password and optional key for changes</td>
<td>authentication [ password &lt;password&gt; ] [ key &lt;key-change&gt; ]</td>
<td>snmp&gt;user</td>
<td>Using no authentication disables authentication protocol.</td>
</tr>
<tr>
<td>Setting user privacy password and optional key for changes</td>
<td>privacy [ password &lt;password&gt; ] [ key &lt;key-change&gt; ]</td>
<td>snmp&gt;user</td>
<td>Using no privacy disables privacy protocol.</td>
</tr>
<tr>
<td>Administratively enabling user</td>
<td>no shutdown</td>
<td>snmp&gt;user</td>
<td>• You must define the authentication and privacy method before you can enable the user, unless the user was defined with no authentication (none-auth). • Using shutdown disables the user.</td>
</tr>
</tbody>
</table>
| Configuring group | access-group <group-name> [ any | snmpv1 | | snmp | Using no access-group deletes the group.
<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Level</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting read view of group</td>
<td><code>read-view &lt;read-view-name&gt;</code></td>
<td>snmp&gt;group</td>
<td></td>
</tr>
<tr>
<td>Setting write view of group</td>
<td><code>write-view &lt;write-view-name&gt;</code></td>
<td>snmp&gt;group</td>
<td></td>
</tr>
<tr>
<td>Setting notify view of group</td>
<td><code>notify-view &lt;notify-view-name&gt;</code></td>
<td>snmp&gt;group</td>
<td></td>
</tr>
<tr>
<td>Administratively enabling group</td>
<td>no shutdown</td>
<td>snmp&gt;group</td>
<td>Using <code>shutdown</code> disables the group</td>
</tr>
<tr>
<td>Connecting security name to group (e.g. connecting user or community for SNMPv1 to group)</td>
<td>`security-to-group { any</td>
<td>snmpv1</td>
<td>snmpv2c</td>
</tr>
<tr>
<td>Specifying group to which to connect security name</td>
<td><code>group-name &lt;group-name&gt;</code></td>
<td>snmp&gt;security-to-group</td>
<td></td>
</tr>
<tr>
<td>Administratively enabling security-to-group entity</td>
<td>no shutdown</td>
<td>snmp&gt;security-to-group</td>
<td>Using <code>shutdown</code> disables the security-to-group entity</td>
</tr>
<tr>
<td>Configuring notification</td>
<td><code>notify &lt;notify-name&gt;</code></td>
<td>snmp&gt;</td>
<td></td>
</tr>
<tr>
<td>Assigning trap to notification</td>
<td>`bind { agnPowerFailureTrap</td>
<td>agnStatusChangeTrap</td>
<td>agnUploadDataTrap</td>
</tr>
<tr>
<td>Assigning tag to notification, to be used to identify the notification entry when configuring target</td>
<td><code>tag &lt;tag-value&gt;</code></td>
<td>snmp&gt;notify</td>
<td></td>
</tr>
<tr>
<td>Task</td>
<td>Command</td>
<td>Level</td>
<td>Comments</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
<td>-------</td>
<td>----------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Administratively enabling notification</td>
<td>no shutdown</td>
<td>snmp &gt; notify</td>
<td></td>
</tr>
<tr>
<td>Configuring set of target parameters</td>
<td>target-params &lt;target-param-name&gt;</td>
<td>snmp</td>
<td>Using no target-params removes target parameters</td>
</tr>
<tr>
<td>Specifying message processing model (SNMP version) to be used when generating SNMP messages for the set of target parameters</td>
<td>message-processing-model { snmpv1</td>
<td>snmpv2c</td>
<td>snmpv3 }</td>
</tr>
<tr>
<td>Specifying SNMP version to be used when generating SNMP messages for the set of target parameters</td>
<td>version { any</td>
<td>snmpv1</td>
<td>snmpv2c</td>
</tr>
<tr>
<td>Specifying user on whose behalf SNMP messages are to be generated for the set of target parameters</td>
<td>security [ name &lt;security-name&gt; ] [ level { no-auth-no-priv</td>
<td>auth-no-priv</td>
<td>auth-priv } ]</td>
</tr>
<tr>
<td>Specifying trap synchronization group</td>
<td>trap-sync-group &lt;group-id&gt; [import-trap-masking]</td>
<td>snmp &gt; target</td>
<td>For details on trap synchronization groups, refer to Chapter 6</td>
</tr>
<tr>
<td>Administratively enabling target parameters</td>
<td>no shutdown</td>
<td>snmp &gt; target</td>
<td>Using shutdown disables target parameters</td>
</tr>
<tr>
<td>Configuring target</td>
<td>target &lt;target-name&gt;</td>
<td>snmp</td>
<td>Using no target removes target</td>
</tr>
<tr>
<td>Specifying set of target parameters for target</td>
<td>target-params &lt;target-param-name&gt;</td>
<td>snmp &gt; target</td>
<td></td>
</tr>
<tr>
<td>Assigning tag(s) to target (the tag(s) must be defined in notification entries)</td>
<td>tag-list {tag}</td>
<td>snmp &gt; target</td>
<td>If you specify more than one tag, you must enclose the list with square brackets, however if you are specifying just one tag the brackets are optional</td>
</tr>
<tr>
<td></td>
<td>tag-list [tag]</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>tag-list [tag1,tag2,...,tagn]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Task</td>
<td>Command</td>
<td>Level</td>
<td>Comments</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>-------</td>
<td>----------</td>
</tr>
<tr>
<td>Specifying target address as IP address or OAM port</td>
<td>address udp-domain &lt;ip-address&gt; oam-domain &lt;oam-port&gt;</td>
<td>snmp&gt;target</td>
<td></td>
</tr>
<tr>
<td>Administratively enabling target</td>
<td>no shutdown</td>
<td>snmp&gt;target</td>
<td>Using shutdown disables target</td>
</tr>
<tr>
<td>Configuring community</td>
<td>community &lt;community-identification&gt;</td>
<td>snmp</td>
<td></td>
</tr>
<tr>
<td>Configuring name</td>
<td>name &lt;community-string&gt;</td>
<td>snmp &gt; community</td>
<td></td>
</tr>
<tr>
<td>Configuring security name</td>
<td>sec-name &lt;security-name&gt;</td>
<td>snmp &gt; community</td>
<td></td>
</tr>
<tr>
<td>Configuring transport tag</td>
<td>tag &lt;transport-tag&gt;</td>
<td>snmp &gt; community</td>
<td>This should normally be left set to the default value</td>
</tr>
<tr>
<td>Administratively enabling community</td>
<td>no shutdown</td>
<td>snmp &gt; community</td>
<td>Using shutdown disables community</td>
</tr>
<tr>
<td>Displaying SNMPv3 information, such as the number of times the SNMPv3 engine has booted, and how long since the last boot</td>
<td>show snmpv3 information</td>
<td>snmp</td>
<td></td>
</tr>
</tbody>
</table>

**Example**

To create SNMPv3 user and connect it to group:
- User named “MD5_priv”:
  - Security level – MD5 authentication, DES privacy
- Group named "SecureGroup":
  - All security levels
  - Contains set of views named "internet" (from default configuration).
To create notifications:

- Notification named “TrapData”:
  - Tag = “Data”
  - Bound to agnStatusChangeTrap, agnUploadDataTrap.

- Notification named “TrapPower”:
  - Tag = “Power”
  - Bound to agnPwFailTrap, coldStart.
To create target parameters and target:

- Target parameters named “TargParam1”:
  - Message processing model SNMPv3
  - Version USM
  - User “MD5_priv”
  - Security level authentication and privacy
- Target named “TargNMS1”:
  - Target parameters “TargParam1”
  - Tag list = “Data”, “Power”
  - IP address 192.5.4.3.

```
ETX-203A# configure management snmp
ETX-203A>config>mngmnt>snmp# snmpv3
ETX-203A>config>mngmnt>snmp# target-params TargParam1
ETX-203A>config>mngmnt>snmp>target(TargParam1)$ message-processing-model snmpv3
ETX-203A>config>mngmnt>snmp>target(TargParam1)$ version usm
ETX-203A>config>mngmnt>snmp>target(TargParam1)$ security name MD5_priv level auth-priv
ETX-203A>config>mngmnt>snmp>target(TargParam1)$ no shutdown
ETX-203A>config>mngmnt>snmp>target(TargParam1)$ exit
ETX-203A>config>mngmnt>snmp# target TargNMS1
ETX-203A>config>mngmnt>snmp>target(TargNMS1)$ target-params TargParam1
ETX-203A>config>mngmnt>snmp>target(TargNMS1)$ tag-list [Data,Power]
ETX-203A>config>mngmnt>snmp>target(TargNMS1)$ address udp-domain 192.5.4.3
ETX-203A>config>mngmnt>snmp>target(TargNMS1)$ no shutdown
ETX-203A>config>mngmnt>snmp>target(TargNMS1)$ exit
ETX-203A>config>mngmnt>snmp#
```

To create communities, target parameters, and target for devices in network that are working with SNMPv1:

- Community “read”:
  - Name: “public”
  - Security name: “v1_read” (defined in default configuration)
- Community “write”:
  - Name: “public”
  - Security name: “v1_write” (defined in default configuration)
- Community “trap”:
  - Name: “trapcom”
  - Security name: “v1_trap” (defined in default configuration)
- Target parameters named “snmpv1”:
  - Message processing model SNMPv1
  - Version SNMPv1
  - Security name: “v1_trap”
- Security: level no authentication and no privacy
- Target named “TargNMS1”:
  - Target parameters “snmpv1”
  - Tag list = “unmasked”
  - IP address 192.5.6.7.

```bash
ETX-203A# configure management snmp
ETX-203A>config>mngmnt>snmp# snmpv3
ETX-203A>config>mngmnt>snmp# community read
ETX-203A>config>mngmnt>snmp# community(read)$ name public
ETX-203A>config>mngmnt>snmp# community(read)$ sec-name v1_read
ETX-203A>config>mngmnt>snmp# community(read)$ no shutdown
ETX-203A>config>mngmnt>snmp# community(read)$ exit
ETX-203A>config>mngmnt>snmp# community write
ETX-203A>config>mngmnt>snmp# community(write)$ name public
ETX-203A>config>mngmnt>snmp# community(write)$ sec-name v1_write
ETX-203A>config>mngmnt>snmp# community(write)$ no shutdown
ETX-203A>config>mngmnt>snmp# community(write)$ exit
ETX-203A>config>mngmnt>snmp# community trap
ETX-203A>config>mngmnt>snmp# community(trap)$ name trapcom
ETX-203A>config>mngmnt>snmp# community(trap)$ sec-name v1_trap
ETX-203A>config>mngmnt>snmp# community(trap)$ no shutdown
ETX-203A>config>mngmnt>snmp# community(trap)$ exit
ETX-203A>config>mngmnt>snmp# target-params snmpv1
ETX-203A>config>mngmnt>snmp# target(snmpv1)$ message-processing-model snmpv1
ETX-203A>config>mngmnt>snmp# target(snmpv1)$ version snmpv1
ETX-203A>config>mngmnt>snmp# target(snmpv1)$ security name v1_trap level no-auth-no-priv
ETX-203A>config>mngmnt>snmp# target(snmpv1) no shutdown
ETX-203A>config>mngmnt>snmp# target(snmpv1) exit
ETX-203A>config>mngmnt>snmp# target snmpv1NMS
ETX-203A>config>mngmnt>snmp# target(snmpv1NMS)$ target-params snmpv1
ETX-203A>config>mngmnt>snmp# target(snmpv1NMS)$ target-name snmpv1NMS
ETX-203A>config>mngmnt>snmp# target(snmpv1NMS)$ tag-list unmasked
ETX-203A>config>mngmnt>snmp# target(snmpv1NMS)$ address udp-domain 192.5.6.7
ETX-203A>config>mngmnt>snmp# target(snmpv1NMS)$ no shutdown
ETX-203A>config>mngmnt>snmp# target(snmpv1NMS)$ exit
ETX-203A>config>mngmnt>snmp#
```

To display SNMPv3 information:

```bash
ETX-203A# configure management snmp
ETX-203A>config>mngmnt>snmp# snmpv3
ETX-203A> config>mngmnt>snmp# show snmpv3 information
SNMPv3 : enable
Boots : 2
Boots Time (sec) : 102
EngineID : 800000a4030020d2202416
ETX-203A>config>mngmnt>snmp#
```
5.5 Network Managers

You can configure the network management stations to which the SNMPv1 agent of ETX-203A sends traps, and from which ETX-203A can be managed. You can define up to ten managers. When you define a network manager, you can define a single station or a subnet of stations from which ETX-203A can be managed. Traps are sent only to a single IP address, not to a subnet. You can temporarily prevent a manager station from receiving traps by masking the network manager.

Factory Defaults

By default, no managers are configured.

Configuring Management Subnets

To configure a management subnet, you provide an IP address and mask, where the mask parameter is a decimal number that specifies the number of high-order consecutive bits set to 1 in the mask. For example, to specify mask 255.255.255.0, use 24 as the value for the mask parameter.

You must provide a valid combination of IP address and mask such that the result of masking the IP address with the mask is the specified IP address. In other words, the IP address and the mask should have the same number of low-order consecutive bits set to 0. Refer to Examples to see some valid IP addresses and masks.

To configure a management subnet:

- At the config>mngmnt# prompt, enter `manager <ip-address>/<mask>`.

The subnet is created if it does not already exist, and the prompt `config>mngmnt>manager(<ip-address>/<mask>)#` is displayed.

To remove a management subnet:

- At the config>mngmnt# prompt, enter `no manager <ip-address>/<mask>`.

Examples

To configure a management subnet:

- IP address = 192.178.1.0
- Mask = 255.255.255.0.

```bash
ETX-203A# configure management
ETX-203A(config>mngmnt)# manager 192.178.1.0/24
ETX-203A(config>mngmnt)>manager(192.178.1.0/24)# exit
```

To configure a management subnet:

- IP address = 192.178.1.240
• Mask = 255.255.255.240.

`ETX-203A# configure management`
`ETX-203A>config>mngmnt# manager 192.178.1.240/28`
`ETX-203A>config>mngmnt>manager(192.178.1.240/28)# exit`
`ETX-203A>config>mngmnt#`

➢ To configure a management subnet:

• IP address 192.178.1.252
• Mask 255.255.255.252.

`ETX-203A# configure management`
`ETX-203A>config>mngmnt# manager 192.178.1.252/30`
`ETX-203A>config>mngmnt>manager(192.178.1.252/30)# exit`
`ETX-203A>config>mngmnt#`

**Configuring Network Manager Stations**

To configure a single management station, you provide an IP address, and a mask that is set to 32.

➢ To configure network managers:

1. At the `config>mngmnt#` prompt, enter `manager <ip-address>/32`.
   
   The network manager entry is created if it does not already exist, and the `config>mngmnt>manager(<ip-address>/32)#` prompt is displayed.

2. Enter the necessary commands according to the tasks listed below.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preventing traps from being sent to the network manager</td>
<td><code>trap-mask</code></td>
<td>Type <code>no trap-mask</code> to allow traps to be sent to the network manager</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You can also mask some traps to prevent sending them to all management stations. For details refer to Chapter 6.</td>
</tr>
<tr>
<td>Specifying UDP port to send SNMPv1 traps to the network manager</td>
<td><code>udp-port snmp-trap-port &lt;udp-port-number&gt;</code></td>
<td>The default is port 162.</td>
</tr>
<tr>
<td>Specifying trap synchronization group</td>
<td><code>trap-sync-group &lt;group-id&gt;</code> [import-trap-masking]</td>
<td>For details on trap synchronization groups, refer to Chapter 6</td>
</tr>
</tbody>
</table>

➢ To remove network managers:

• To delete a network manager, at the `config>mngmnt#` prompt enter: `no manager <ip-address>/32`.  

Example

To configure a management station:
- IP address = 192.178.1.4
- Traps masked.

```bash
ETX-203A# configure management
ETX-203A>config>mngmnt# manager 192.178.1.4/32
ETX-203A>config>mngmnt>manager(192.178.1.4/32)# trap-mask
ETX-203A>config>mngmnt>manager(192.178.1.4/32)# exit
ETX-203A>config>mngmnt#
```

5.6 Controlling Management Access

You can enable or disable access to the ETX-203A management system via Telnet, SSH, or SNMP applications. By disabling Telnet, SSH, or SNMP, you prevent unauthorized access to the system when security of the ETX-203A IP address has been compromised. When Telnet, SSH, and SNMP are disabled, ETX-203A can be managed via an ASCII terminal only. In addition, you can limit access to the device to only the defined management stations.

*Table 5-7* lists management access implementation, according to the defined management access and whether network managers are defined.

Factory Defaults

By default, access is enabled via Telnet, SSH, and SNMP.

Configuring Management Access

To configure management access:
- At the *configure management access* prompt enter the necessary commands according to the tasks listed below.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allowing Telnet access</td>
<td>telnet [managers-only]</td>
<td>Typing no telnet blocks access by Telnet</td>
</tr>
<tr>
<td><strong>Note:</strong> If you want to allow Telnet access by managers only, you must enter the command to block Telnet access.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Allowing SSH (Secure Shell) access</td>
<td>ssh [managers-only]</td>
<td>Typing no ssh blocks access by SSH</td>
</tr>
<tr>
<td><strong>Note:</strong> If you want to allow SSH access by managers only, you must first enter the commands to block Telnet and SSH access.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Allowing SNMP access</td>
<td>snmp [managers-only]</td>
<td>Typing no snmp blocks access by SNMP</td>
</tr>
<tr>
<td><strong>Note:</strong> If you want to allow SNMP access by managers only, you must first enter the command to block SNMP access.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 5-7. Management Access Implementation

<table>
<thead>
<tr>
<th>Access Method</th>
<th>Mode</th>
<th>Allowed to Access</th>
<th>ETX-203A</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Network Manager(s)</td>
<td>Network Manager(s)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Defined</td>
<td>not Defined</td>
</tr>
<tr>
<td>Telnet Access</td>
<td>Enable</td>
<td>Anybody</td>
<td>Anybody</td>
</tr>
<tr>
<td></td>
<td>Disable</td>
<td>Nobody</td>
<td>Nobody</td>
</tr>
<tr>
<td></td>
<td>Managers Only</td>
<td>Only defined network managers</td>
<td>Nobody</td>
</tr>
<tr>
<td>SSH Access (Secure Shell)</td>
<td>Enable</td>
<td>Anybody</td>
<td>Anybody</td>
</tr>
<tr>
<td></td>
<td>Disable</td>
<td>Nobody</td>
<td>Nobody</td>
</tr>
<tr>
<td></td>
<td>Managers Only</td>
<td>Only defined network managers</td>
<td>Nobody</td>
</tr>
<tr>
<td>SNMP Access</td>
<td>Enable</td>
<td>Anybody</td>
<td>Anybody</td>
</tr>
<tr>
<td></td>
<td>Disable</td>
<td>Nobody</td>
<td>Nobody</td>
</tr>
<tr>
<td></td>
<td>Managers Only</td>
<td>Only defined network managers</td>
<td>Nobody</td>
</tr>
</tbody>
</table>

### 5.7 Access Policy

The access policy allows specifying up to three user authentication methods (local, RADIUS, TACACS+). If an authentication method is not available or the user is not found, the next method is used if applicable.

**Factory Defaults**

By default, authentication is via the locally stored database *(1st-level local)*.

**Configuring Access Policy**

- To define the access policy:
  - At the `config>mngmnt>access#` prompt, enter the necessary commands according to the tasks listed below.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifying authentication via locally stored database</td>
<td><code>auth-policy 1st-level local</code></td>
<td></td>
</tr>
</tbody>
</table>
### Task | Command | Comments
--- | --- | ---
Specifying authentication method preferably via RADIUS, then optionally TACACS+, then optionally local | auth-policy 1st-level radius [2nd-level tacacs+ [3rd-level {local | none}]] | If su (Superuser) does not exist in the RADIUS server database or the system loses the connection to the RADIUS server, ETX-203A uses the local authentication database to authenticate the user, if 2nd-level is set to local.

Specifying authentication method preferably via TACACS+, then optionally RADIUS, then optionally local | auth-policy 1st-level tacacs+ [2nd-level radius [3rd-level {local | none}]] | If su (Superuser) does not exist in the TACACS+ and RADIUS server databases or the system loses the connection to the TACACS+ and RADIUS servers, ETX-203A uses the local authentication database to authenticate the user, if 2nd-level is set to local.

Specifying authentication method preferably via TACACS+, then optionally local | auth-policy 1st-level tacacs+ [2nd-level {local | none} ] | If su (Superuser) does not exist in the TACACS+ server database or the system loses the connection to the TACACS+ server, ETX-203A uses the local authentication database to authenticate the user, if 2nd-level is set to local.

---

### 5.8 Authentication via RADIUS Server

RADIUS (Remote Authentication Dial-In User Service) is an AAA (authentication, authorization and accounting) client/server protocol that secures networks against unauthorized access. It is used to authenticate users and authorize their access to the requested system or service. The RADIUS client communicates with the RADIUS server using a defined authentication sequence.

#### Standards

RFC 2865, Remote Authentication Dial In User Service (RADIUS)

RFC 2618, RADIUS Authentication Client MIB

#### Benefits

The RADIUS protocol allows centralized authentication and access control, avoiding the need to maintain a local user database on each device on the network.

#### Functional Description

When a login attempt occurs at ETX-203A, it submits an authentication request to the RADIUS server. The RADIUS server checks the database and replies with either **Access Rejected** or **Access Accepted**.
Factory Defaults

By default, no RADIUS servers are defined. When the RADIUS server is first defined, it is configured as shown below.

<table>
<thead>
<tr>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address of server</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>Max number of authentication attempts</td>
<td>2</td>
</tr>
<tr>
<td>Time interval between two authentication attempts</td>
<td>2 seconds</td>
</tr>
<tr>
<td>UDP port used for authentication</td>
<td>1812</td>
</tr>
</tbody>
</table>

Configuring RADIUS Parameters

ETX-203A provides connectivity to up to four RADIUS authentication servers. You have to specify access parameters such as assigning Radius server IDs, specifying the associated server IP addresses and the number of retries, etc.

➢ To define RADIUS parameters:

1. At the config>mngmnt>radius# prompt, type server <server-id> to specify which server to configure.

   The config>mngmnt>radius>server(<server-id>)# prompt is displayed.

2. Enter the necessary commands according to the tasks listed below.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assigning an IP address to the server</td>
<td>address &lt;ip-address&gt;</td>
<td>Possible IP addresses range from 1.1.1.1 to 255.255.255.255</td>
</tr>
<tr>
<td>Defining a non-disclosed string (shared secret) used to encrypt the user password.</td>
<td>key &lt;string&gt; [hash]</td>
<td>The shared secret is a secret key consisting of free text known to the client and the server for encryption. It is hashed if specified.</td>
</tr>
<tr>
<td>Defining the number of authentication request attempts</td>
<td>retry &lt;number-of-retries&gt;</td>
<td>Range 0–10</td>
</tr>
<tr>
<td>Defining timeout (in seconds) for response from RADIUS server</td>
<td>timeout &lt;seconds&gt;</td>
<td>Range 1–5</td>
</tr>
<tr>
<td>Defining the UDP port to be used for authentication</td>
<td>auth-port &lt;udp-port-number&gt;</td>
<td>Range 1–65535</td>
</tr>
<tr>
<td>Administratively enabling server</td>
<td>no shutdown</td>
<td>Type shutdown to administratively disable the server</td>
</tr>
<tr>
<td>Displaying status</td>
<td>show status</td>
<td></td>
</tr>
</tbody>
</table>
Displaying RADIUS Statistics

➢ To display RADIUS statistics:
  • At the config>mngmnt>radius# prompt, enter: show statistics.

RADIUS statistics appear as shown below.

<table>
<thead>
<tr>
<th></th>
<th>Server1</th>
<th>Server2</th>
<th>Server3</th>
<th>Server4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Requests</td>
<td>:0</td>
<td>:0</td>
<td>:0</td>
<td>:0</td>
</tr>
<tr>
<td>Access Retransmits</td>
<td>:0</td>
<td>:0</td>
<td>:0</td>
<td>:0</td>
</tr>
<tr>
<td>Access Accepts</td>
<td>:0</td>
<td>:0</td>
<td>:0</td>
<td>:0</td>
</tr>
<tr>
<td>Access Rejects</td>
<td>:0</td>
<td>:0</td>
<td>:0</td>
<td>:0</td>
</tr>
<tr>
<td>Access Challenges</td>
<td>:0</td>
<td>:0</td>
<td>:0</td>
<td>:0</td>
</tr>
<tr>
<td>Malformed Response</td>
<td>:0</td>
<td>:0</td>
<td>:0</td>
<td>:0</td>
</tr>
<tr>
<td>Bad Authenticators</td>
<td>:0</td>
<td>:0</td>
<td>:0</td>
<td>:0</td>
</tr>
<tr>
<td>Pending Requests</td>
<td>:0</td>
<td>:0</td>
<td>:0</td>
<td>:0</td>
</tr>
<tr>
<td>Timeouts</td>
<td>:0</td>
<td>:0</td>
<td>:0</td>
<td>:0</td>
</tr>
<tr>
<td>Unknown Types</td>
<td>:0</td>
<td>:0</td>
<td>:0</td>
<td>:0</td>
</tr>
<tr>
<td>Packets Dropped</td>
<td>:0</td>
<td>:0</td>
<td>:0</td>
<td>:0</td>
</tr>
</tbody>
</table>

5.9 Authentication via TACACS+ Server

TACACS+ (Terminal Access Controller Access Control System Plus) is a security application that provides access control for routers, network access servers, and other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization, and accounting services. It is used to communicate between the switch and an authentication database. As TACACS+ is based on TCP, implementations are typically resilient against packet loss.

Standards

RFC 1492, An Access Control Protocol, Sometimes Called TACACS

Benefits

The TACACS+ protocol allows centralized authentication and access control, avoiding the need to maintain a local user database on each device on the network. The TACACS+ server encrypts the entire body of the packet but leaves a standard TACACS+ header.

Functional Description

When a login attempt occurs at ETX-203A, it submits an authentication request to the TACACS+ server, which checks the database and then grants or rejects access.
Factory Defaults

By default, no TACACS+ servers are defined. When a TACACS+ server is first defined, it is configured as shown below.

<table>
<thead>
<tr>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>The max number of authentication attempts.</td>
<td>3</td>
</tr>
<tr>
<td>Time interval between two authentication attempts.</td>
<td>5 seconds</td>
</tr>
<tr>
<td>UDP port used for the authentication channel</td>
<td>1812</td>
</tr>
<tr>
<td>Administratively enabled</td>
<td>Disabled (shutdown)</td>
</tr>
</tbody>
</table>

Configuring TACACS+ Parameters

ETX-203A provides connectivity to one TACACS+ authentication server. You have to specify the associated server IP address, number of retries, etc.

Note

If you intend to use TACACS+ for authentication, verify that TACACS+ is selected as level-1 authentication method (see Access Policy).

To define TACACS+ parameters:

1. At the `config>mngmnt>tacacsplus#` prompt, type `server <ip-address>` to specify the server IP address.

   The `config>mngmnt>tacacsplus>server(<ip-address>)#` prompt is displayed.

2. Enter the necessary commands according to the tasks listed below.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defining the number of authentication request attempts</td>
<td><code>retry &lt;number-of-retries&gt;</code></td>
<td>Range 1–10</td>
</tr>
<tr>
<td>Defining timeout (in seconds) for response from TACACS+ server</td>
<td><code>timeout &lt;seconds&gt;</code></td>
<td>Range 1–255</td>
</tr>
<tr>
<td>Administratively enabling server</td>
<td><code>no shutdown</code></td>
<td>Type <code>shutdown</code> to administratively disable the server</td>
</tr>
<tr>
<td>Clearing statistics</td>
<td><code>clear-statistics</code></td>
<td></td>
</tr>
<tr>
<td>Displaying status</td>
<td><code>show status</code></td>
<td></td>
</tr>
<tr>
<td>Displaying statistics</td>
<td><code>show statistics</code></td>
<td></td>
</tr>
</tbody>
</table>

To display TACACS+ status summary:

- At the `config>mngmnt>tacacsplus#` prompt, type: `show status-summary`.

   The status information is displayed.
5.10 Terminal Control Port

You can configure the serial port parameters, which include specifying the data rate, security timeout, and screen size from which you are accessing the device.

Factory Defaults

By default, data rate is set to 9,600 bps.

Configuring Control Port Parameters

➢ To define the control port parameters:

• At the config>terminal# prompt, enter the necessary commands according to the tasks listed below.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifying the desired data rate</td>
<td>baud-rate { 9600bps</td>
<td>19200bps</td>
</tr>
<tr>
<td>Defining whether in case of inactivity, device remains connected or disconnects after a specified time period</td>
<td>timeout forever</td>
<td>timeout limited &lt;minutes&gt;</td>
</tr>
<tr>
<td>Specifying the number of rows to display</td>
<td>length &lt;number-of-rows&gt;</td>
<td>The number of rows can be 0, to indicate no limit on the number of lines displayed, or 20.</td>
</tr>
</tbody>
</table>

5.11 User Access

ETX-203A management software allows you to define new users, their management and access rights. Only superusers (su) can create new users, the regular users are limited to changing their current passwords, even if they were given full management and access rights.

You can specify a user’s password as a text string or as a hashed value, that you obtain by using the info command to display user data.
Notes

- User passwords are stored in a database so that the system can perform password verification when a user attempts to log in. To preserve confidentiality of system passwords stored in text configuration files, the password verification data is typically stored after a one-way hash function is applied to the password, in combination with other data. When a user attempts to log in by entering a password, the same function is applied to the entered value and the result is compared with the stored value.

- A cryptographic hash function is a deterministic procedure that takes an arbitrary block of data and returns a fixed-size bit string, the (cryptographic) hash value, such that any change to the data changes the hash value.

Factory Defaults

By default, the following users exist, with default password 1234:

- su
- tech
- user

➢ To add a new user:

1. Make sure that you are logged on as superuser (su).
2. Navigate to the Management context (config>mngmnt).
3. Define a new user:

   ```
   user <name> [ level { su | tech | user } ]
   [ password <password> [hash] ]
   ```

Example – Defining Users

➢ To define a new user:

- User name = staff
- User password = 1234.

   ```
   ETX-203A# configure management
   ETX-203A>config>mngmnt# user staff level su password 1234
   # Password is encrypted successfully
   ```

➢ To add a new user with a hashed password:

1. Define a new user with a text password.
2. Use `info detail` to display the password hash value.
3. Define another user with the hashed password from the `info` output.

   The second user can log in with the text password defined in step 1.

For example, to add the following users:

- User name = staff1
- User password = 4222
• User name = staff2
• User password = hash of 4222 (user staff2 can log in with password 4222).

```plaintext
ETX-203A# configure management
ETX-203A>config>mngmnt# user staff1 level user password 4222
# Password is encrypted successfully
ETX-203A>config>mngmnt# info detail
    user "staff1" level user password
    "3fda26f8cf4123dcdad0c1bc89ed1e79977acef" hash
    user "su"

ETX-203A>config>mngmnt# user staff2 level user password 3fda26f8cf4123dcdad0c1bc89ed1e79977acef hash
ETX-203A>config>mngmnt# info detail
    user "staff1" level user password
    "3fda26f8cf4123dcdad0c1bc89ed1e79977acef" hash
    user "staff2" level user password
    "3fda26f8cf4123dcdad0c1bc89ed1e79977acef" hash
    user "su"
```

To delete an existing user:
• At the Management context (config>mngmnt), enter `no <user-name>`.
  The specified user is deleted.

To view all connected users:
• At the Management context (config>mngmnt), enter `show users`.
  A list of all connected users is displayed, showing their access level, the type of connection, and the IP address from which they are connected.
Example – Displaying Users

```
ETX-203A# configure management
ETX-203A>config>mngmnt# show users
User                          Access Level   Source         IP-address
-----------------------------------------------------------------------------
  su                            SU             Terminal       0.0.0.0
ETX-203A>config>mngmnt#
```

5.12 Layer 2 Control Processing

ETX-203A can be configured to pass through Layer-2 Control frames (including other vendors’ L2CP frames) across the network, to peer supported protocols, or to discard the L2CP frames. You can perform protocol tunneling, with MAC address swap.

You can create profiles to define the handling of Layer-2 Control Protocol traffic. You then assign the required profile to an Ethernet port or to a flow (refer to Configuring Ethernet Port Parameters and Configuring Flows, respectively).

Standards

IEEE 802.3

Benefits

Layer 2 Control Protocol can be passed or filtered to Ethernet virtual connections.

Factory Defaults

ETX-203A provides a default L2CP profile named L2cpDefaultProfile, configured as follows:

- For MAC hex byte 0x00 through 0x2f, action = tunnel
- Default action = tunnel.

When a new L2CP profile is created, it has the same configuration as L2cpDefaultProfile.

Adding Layer 2 Control Processing Profiles

- To add an L2CP profile:
  1. Navigate to configure port.

```
     The config>port# prompt is displayed.
```
  2. Type:

```
  l2cp-profile <l2cp-profile-name>
```
An L2CP profile with the specified name is created and the `config>port>l2cp-profile<{l2cp-profile-name}>$` prompt is displayed. The new profile is configured by default as described in *Factory Defaults*.

3. Configure the L2CP profile as needed (refer to *Configuring Layer 2 Control Processing Profile Parameters*).

### Deleting Layer 2 Control Processing Profiles

You can delete an L2CP profile only if it is not assigned to any port.

- **To delete an L2CP profile:**
  1. Navigate to `configure port`.
     
     The `config>port#$` prompt is displayed.
  2. Type:
     ```
     no l2cp-profile <l2cp-profile-name>
     ```
     
     The L2CP profile with the specified name is deleted if it is not assigned to any port.

### Configuring Layer 2 Control Processing Profile Parameters

- **To configure an L2CP profile:**
  1. Navigate to `configure port l2cp <l2cp-profile-name>` to select the L2CP profile to configure.
     
     The `config>port>l2cp-profile<{l2cp-profile-name}>#$` prompt is displayed.
  2. Enter all necessary commands according to the tasks listed below.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
</table>
| Specifying the default action for undefined control protocols | `default {discard | tunnel}`                                              | `discard` - L2CP frames are discarded  
|                               |                                                                         | `tunnel` - L2CP frames are forwarded across the network as ordinary data | |
| Specifying the L2CP action for MAC addresses (discard, tunnel, or peer) | `mac <mac-addr-last-byte-value-list> {discard | tunnel | peer}`              | `discard` - L2CP frames are discarded  
|                               |                                                                         | `tunnel` - L2CP frames are forwarded across the network as ordinary data | `peer` - ETX-203A peers with the user equipment to run the protocol. L2CP frames are forwarded to the ETX-203A CPU. Unidentified L2CP frames are forwarded across the network as ordinary data.  
<p>|                               |                                                                         | Typing <code>no mac &lt;mac-addr-last-byte-value-list&gt;</code> removes the action for the specified MAC address |</p>
<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Choosing a protocol for tunneling and specifying MAC swap if desired</td>
<td>protocol {stp</td>
<td>vtp</td>
</tr>
</tbody>
</table>

**Example**

To add L2CP profile named layer2ctrl1 with discard action for hex byte 0x01 and 0x03:

```
ETX-203A# configure port
ETX-203A>config>port# l2cp-profile layer2ctrl1
ETX-203A>config>port>l2cp-profile(layer2ctrl1)$ mac 0x01 discard
ETX-203A>config>port>l2cp-profile(layer2ctrl1)$ mac 0x03 discard
ETX-203A>config>port>l2cp-profile(layer2ctrl1)$ info detail
  mac 0x00  tunnel
  mac 0x01  discard
  mac 0x02  tunnel
  mac 0x03  discard
  mac 0x04  tunnel
  mac 0x05  tunnel
  mac 0x06  tunnel
  mac 0x07  tunnel
  mac 0x08  tunnel
  mac 0x09  tunnel
  mac 0x0a  tunnel
  mac 0x0b  tunnel
  mac 0x0c  tunnel
  mac 0x0d  tunnel
  mac 0x0e  tunnel
  mac 0x0f  tunnel
  mac 0x10  tunnel
  mac 0x11  tunnel
  mac 0x12  tunnel
  mac 0x13  tunnel
  mac 0x14  tunnel
  mac 0x15  tunnel
  mac 0x16  tunnel
  mac 0x17  tunnel
  mac 0x18  tunnel
  mac 0x19  tunnel
  mac 0x1a  tunnel
  mac 0x1b  tunnel
  mac 0x1c  tunnel
  mac 0x1d  tunnel
  mac 0x1e  tunnel
  mac 0x1f  tunnel
  default  tunnel
ETX-203A>config>port>l2cp-profile(layer2ctrl1)$
```
5.13 Ethernet Ports

ETX-203A has two fiber optic or copper Fast or Gigabit Ethernet network ports and up to two fiber optic or copper Fast or Gigabit Ethernet user ports. The second network port can be configured as a user port. The following table shows how to refer to the ports when configuring them with CLI commands.

<table>
<thead>
<tr>
<th>Port</th>
<th>Port Number on Unit</th>
<th>Port in CLI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Net 1</td>
<td>1</td>
<td>Ethernet 1</td>
</tr>
<tr>
<td>Net/User 2</td>
<td>2</td>
<td>Ethernet 2</td>
</tr>
<tr>
<td>User 3</td>
<td>3</td>
<td>Ethernet 3</td>
</tr>
<tr>
<td>User 4</td>
<td>4</td>
<td>Ethernet 4</td>
</tr>
<tr>
<td>MNG-ETH 101</td>
<td>-</td>
<td>Ethernet 101</td>
</tr>
</tbody>
</table>

The following parameters can be configured for the Ethernet ports:

- Port name
- Autonegotiation (electrical ports)
- Maximum advertised capability for autonegotiation procedure
- Data rate and duplex mode, when autonegotiation is disabled
- Administrative status
- Network or user functional mode (second network interface only)
- DHCP request sent when port is activated
- Tag Ethernet Type
- Egress MTU
- Queue group profile
- L2CP handling
- Link OAM EFM (IEEE 802.3-2005) – Refer to OAM EFM
- Loopback – Refer to Testing Ethernet Ports.

**Note**

An Ethernet port where a smart SFP has been provisioned cannot be accessed by the commands in this section.
Configuring Ethernet Port Parameters

To configure the Ethernet port parameters:

1. Navigate to `configure port ethernet <port-num>` to select the Ethernet port to configure.

   The `config>port>eth(<port-num>)#` prompt is displayed.

2. Enter all necessary commands according to the tasks listed below.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assigning description to port</td>
<td>name &lt;string&gt;</td>
<td>Using no before <code>name</code> removes the name</td>
</tr>
<tr>
<td>Enabling autonegotiation</td>
<td>auto-negotiation</td>
<td>Using no before <code>auto-negotiation</code> disables autonegotiation</td>
</tr>
</tbody>
</table>
| Setting maximum advertised capability (highest traffic handling capability to be advertised during the autonegotiation process) | max-capability {10-full-duplex | 100-full-duplex | 1000-full-duplex | 1000-x-full-duplex } | 10-full-duplex – 10baseT full duplex  
100-full-duplex – 100baseT full duplex  
1000-full-duplex – 1000base T full duplex  
1000-x-full-duplex – 1000baseX full duplex  
The values 1000-full-duplex and 1000-x-full-duplex are relevant only for Gigabit Ethernet ports.  
*Note*: This parameter applies only if autonegotiation is enabled. |
| Setting data rate and duplex mode of the Ethernet port, when autonegotiation is disabled | speed-duplex {10-full-duplex | 100-full-duplex | 1000-full-duplex | 1000-x-full-duplex } | 10-full-duplex – 10baseT full duplex  
100-full-duplex – 100baseT full duplex  
1000-full-duplex – 1000base T full duplex  
1000-x-full-duplex – 1000baseX full duplex  
The values 1000-full-duplex and 1000-x-full-duplex are relevant only for Gigabit Ethernet ports |
| Setting the VLAN tagged frame ETH II frame Ethertype (tag protocol identifier) | tag-ethernet-type <0x0000-0xFFFF> | Note: For network and user ports you can configure the values: 0x8100, 0x88a8, 0x9100. For user ports you can configure only 0x8100. |
| Associating a queue group profile with the port | queue-group profile <queue-group-profile-name> | Note: You can associate a network port with a queue group profile containing up to 31 queue blocks, but a user port can be associated only with a queue group profile containing a single queue block. |
### Associating a Layer-2 control processing profile with the port

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
</table>
| Associating a Layer-2 control processing profile with the port | `l2cp profile <l2cp-profile-name>` | - If Ethernet port 2 is configured as a network port, then whenever you assign an L2CP profile to one of the network ports it is automatically assigned to the other network port  
- If you intend to enable LACP (LAG) or link OAM on the port, the associated L2CP profile must specify peer action for MAC 0x02 |

### Specifying conditions for sending DHCP request

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
</table>
| Specifying conditions for sending DHCP request | `dhcp-request {normal | when-up} normal` – DHCP request is sent for the normal reasons, e.g. if the device needs to acquire an IP address or the IP address is about to expire  
`when-up` – In addition to the normal reasons listed above, a DHCP request is sent whenever the port is activated or becomes operational |

### Setting maximum frame size to transmit (frames above the specified size are discarded)

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting maximum frame size to transmit (frames above the specified size are discarded)</td>
<td><code>egress-mtu &lt;64–12288&gt;</code></td>
<td></td>
</tr>
</tbody>
</table>

### Administratively enabling port

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administratively enabling port</td>
<td><code>no shutdown</code></td>
<td>Using <code>shutdown</code> disables the port</td>
</tr>
</tbody>
</table>

### Setting Second Network Interface as Network or User Port

You can change the functional mode of the second network interface from network to user port and vice versa. If it functions as a user port, then redundancy is not possible.

**Note**

*When you change the functional mode, all flows related to the port are deleted.*

To change the functional mode of the second network interface:

1. Navigate to `configure port ethernet 2`.
   
The `config>port>eth2#` prompt is displayed.
2. Enter the command to change the functional mode:
   
   - To change to user port, enter: `functional-mode user`.
   - To change to network port, enter: `functional-mode network`.

The functional mode of the port is changed.
Example

► To change the second network interface functional mode to user port:

ETX-203A# configure port ethernet 2
ETX-203A>config>port>eth(2)# functional-mode user
ETX-203A#

Displaying Ethernet Port Status

You can display the following:

• Summary information showing the status and speed of all Ethernet ports
• Status and configuration of an individual Ethernet port.

► To display the status of all Ethernet ports:

• At the prompt config>port#, enter:
  
  show summary.

  The port status and speeds of the Ethernet ports are displayed. If a port
  is being tested via the loopback command, it is indicated in the
  operational status.

► To display status of an Ethernet port:

• At the prompt config>port>eth(<port-num>)#, enter:
  
  show status.

  The Ethernet port status parameters are displayed.

Examples

► To display the status of all Ethernet ports:

ETX-203A# configure port
ETX-203A>config>port# show summary

<table>
<thead>
<tr>
<th>Port</th>
<th>Number</th>
<th>Name</th>
<th>Admin</th>
<th>Oper</th>
<th>Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet 1</td>
<td>ETH 1</td>
<td>Up</td>
<td>Up</td>
<td>1000000</td>
<td></td>
</tr>
<tr>
<td>Ethernet 1</td>
<td>ETH 2</td>
<td>Up</td>
<td>Up</td>
<td>1000000</td>
<td></td>
</tr>
<tr>
<td>Ethernet 1</td>
<td>ETH 3</td>
<td>Up</td>
<td>Testing</td>
<td>1000000</td>
<td></td>
</tr>
<tr>
<td>Ethernet 1</td>
<td>ETH 4</td>
<td>Up</td>
<td>Up</td>
<td>1000000</td>
<td></td>
</tr>
<tr>
<td>Ethernet 101</td>
<td>MNG-ETH</td>
<td>Up</td>
<td>Up</td>
<td>1000000</td>
<td></td>
</tr>
</tbody>
</table>

ETX-203A>config>port#
To display the status of Ethernet port 3:

```
ETX-203A# configure port ethernet 3
ETX-203A>config>port>eth(3)# show status
Name                  : ETH 3
Administrative Status : Up
Operation Status      : Up
Connector Type        : RJ45
Auto Negotiation      : Other
MAC Address           : 00-20-D2-30-CC-9D
EFM Status   : Disabled
```

```
ETX-203A>config>port>eth(3)#
```

### Testing Ethernet Ports

The physical layer runs at the PHY of the ports. When the loopback is active the data forwarded to a port is looped from the Tx path to the Rx path.

The loopback can be one of the following types:

- **Local** – Loopback is closed towards the user interface (Figure 5-7)
- **Remote** – Loopback is closed towards the network interface (Figure 5-8).

![Figure 5-7. Local Loopback](image)

![Figure 5-8. Remote Loopback](image)

To run a physical layer loopback test:

1. Navigate to `configure port ethernet <port-num>` to select the Ethernet port to test.

   The `config>port>eth(<port-num>)#` prompt is displayed.

2. Enter:

   `loopback {local | remote} [duration <seconds>]`.

   The duration is in seconds, with range 0–86400. Entering 0 or not specifying the duration disables the timer, e.g. the loopback runs forever until you disable it.
While the test is running, entering `show summary` at the `port` level displays the port’s operational status as `Testing` (refer to `Displaying Ethernet Port Status`).

3. To end the loopback test, enter:
   ```
   no loopback.
   ```

**Example**

- To run loopback on Ethernet port 3:
  ```
  ETX-203A# configure port ethernet 3
  ETX-203A>config>port>eth(3)# loopback remote duration 30
  ETX-203A>config>port>eth(3)# show loopback
  Loopback : Remote        Remain (sec)  : 21
  ```

**Displaying Ethernet Port Statistics**

You can display statistics for the Ethernet ports, as well as L2CP statistics. The sampling interval for the Ethernet port statistics can be configured.

**Setting Sampling Interval for Port Statistics**

The sampling interval can be configured from one to 30 minutes. The default is 15 minutes.

- To set the sampling interval:
  ```
  • At the prompt `config>port#`, enter:
    `rate-sampling-window <1–30>`.
  ```
  The sampling interval is set to the specified number of minutes.

**Displaying Port Statistics**

- To display the Ethernet port statistics:
  ```
  • At the prompt `config>port>eth<port-num>#`, enter:
    `show statistics`.
  ```
  Ethernet port statistics are displayed. The counters are described in Table 5-9.
Example

To display the statistics for Ethernet port 2:

```
ETX-203A# configure port ethernet 2
ETX-203A>config>port>eth(2)# show statistics
```

<table>
<thead>
<tr>
<th>Rates Sampling Window</th>
</tr>
</thead>
<tbody>
<tr>
<td>Window Size [Min.]    : 15</td>
</tr>
<tr>
<td>Window Remain Time [Min.] : 0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Running</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rx</td>
</tr>
<tr>
<td>---</td>
</tr>
<tr>
<td>Total Frames : 0</td>
</tr>
<tr>
<td>Total Octets : 0</td>
</tr>
<tr>
<td>Total Frames/Sec : 0</td>
</tr>
<tr>
<td>Total Bits/Sec : 0</td>
</tr>
<tr>
<td>Min. Bits/Sec : 0</td>
</tr>
<tr>
<td>Max. Bits/Sec : 0</td>
</tr>
<tr>
<td>Unicast Frames : 0</td>
</tr>
<tr>
<td>Multicast Frames : 0</td>
</tr>
<tr>
<td>Broadcast Frames : 0</td>
</tr>
<tr>
<td>Error Frames : 0</td>
</tr>
<tr>
<td>L2CP Discarded : 0</td>
</tr>
<tr>
<td>OAM Discarded : 0</td>
</tr>
<tr>
<td>Unknown Protocol Discarded : 0</td>
</tr>
<tr>
<td>CRC Errors : 0</td>
</tr>
<tr>
<td>CRC Errors/Sec : 0</td>
</tr>
<tr>
<td>Jabber Errors : 0</td>
</tr>
<tr>
<td>Oversize Frames : 0</td>
</tr>
<tr>
<td>64 Octets : 0</td>
</tr>
<tr>
<td>65-127 Octets : 0</td>
</tr>
<tr>
<td>128-255 Octets : 0</td>
</tr>
<tr>
<td>256-511 Octets : 0</td>
</tr>
<tr>
<td>512-1023 Octets : 0</td>
</tr>
<tr>
<td>1024-1528 Octets : 0</td>
</tr>
<tr>
<td>1519-2047 Octets : 0</td>
</tr>
<tr>
<td>2048-Max Octets : 0</td>
</tr>
</tbody>
</table>

```
ETX-203A>config>port>eth(2)#
```

Table 5-9. Ethernet Statistics Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Window Size [Min.]</td>
<td>Interval for sampling statistics, user-configurable (see Setting Sampling Interval for Port Statistics)</td>
</tr>
<tr>
<td>Window Remain Time [Min.]</td>
<td>Amount of time remaining in statistics sampling window</td>
</tr>
<tr>
<td>Total Frames</td>
<td>Total number of frames received/transmitted</td>
</tr>
<tr>
<td>Total Octets</td>
<td>Total number of bytes received/transmitted</td>
</tr>
<tr>
<td>Total Frames/Sec</td>
<td>Number of frames received/transmitted per second</td>
</tr>
<tr>
<td>Total Bits/Sec</td>
<td>Number of bits received/transmitted per second</td>
</tr>
</tbody>
</table>
### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Min. Bits/Sec</td>
<td>Minimum number of bits received/transmitted per second</td>
</tr>
<tr>
<td>Max. Bits/Sec</td>
<td>Maximum number of bits received/transmitted per second</td>
</tr>
<tr>
<td>Unicast Frames</td>
<td>Total number of unicast frames received/transmitted</td>
</tr>
<tr>
<td>Multicast Frames</td>
<td>Total number of multicast frames received/transmitted</td>
</tr>
<tr>
<td>Broadcast Frames</td>
<td>Total number of broadcast frames received/transmitted</td>
</tr>
<tr>
<td>Error Frames</td>
<td>Total number of frames with errors received</td>
</tr>
<tr>
<td>L2CP Discarded</td>
<td>Total number of L2CP frames discarded</td>
</tr>
<tr>
<td>OAM Discarded</td>
<td>Total number of OAM frames discarded</td>
</tr>
<tr>
<td>Unknown Protocol Discarded</td>
<td>Total number of frames with unknown protocol discarded</td>
</tr>
<tr>
<td>CRC Errors</td>
<td>Total number of frames received that are an integral number of octets in length, but do not pass the Frame Check Sequence (FCS) check. This count does not include frames received with Frame-Too-Long or Frame-Too-Short error.</td>
</tr>
<tr>
<td>CRC Errors/Sec</td>
<td>Number of frames per second received that are an integral number of octets in length, but do not pass the Frame Check Sequence (FCS) check. This count does not include frames received with Frame-Too-Long or Frame-Too-Short error.</td>
</tr>
<tr>
<td>Jabber Errors</td>
<td>Total number of frames received with jabber errors</td>
</tr>
<tr>
<td>Oversize Frames</td>
<td>Total number of oversized frames received/transmitted</td>
</tr>
<tr>
<td>64 Octets</td>
<td>Total number of received/transmitted 64-byte packets</td>
</tr>
<tr>
<td>65–127 Octets</td>
<td>Total number of received/transmitted 65 to 127-byte packets</td>
</tr>
<tr>
<td>128–255 Octets</td>
<td>Total number of received/transmitted 128 to 255-byte packets</td>
</tr>
<tr>
<td>256–511 Octets</td>
<td>Total number of received/transmitted 256 to 511-byte packets</td>
</tr>
<tr>
<td>512–1023 Octets</td>
<td>Total number of received/transmitted 512 to 1023-byte packets</td>
</tr>
<tr>
<td>1024–1518 Octets</td>
<td>Total number of received/transmitted 1024 to 1518-byte packets</td>
</tr>
<tr>
<td>1519–2047 Octets</td>
<td>Total number of received/transmitted 1519 to 2047-byte packets</td>
</tr>
<tr>
<td>2048–Max Octets</td>
<td>Total number of received/transmitted packets with 2048 bytes and up to maximum</td>
</tr>
</tbody>
</table>

### Displaying Layer-2 Control Processing Statistics

- **To display the Layer-2 control processing statistics for an Ethernet port:**
  - At the prompt `config>port>eth(<port-num>)#`, enter: `show 12cp-statistics`.

L2CP statistics are displayed for the specified port, showing the number of encapsulated and decapsulated packets for each protocol.
Example

To display the L2CP statistics for Ethernet port 3:

```
ETX-203A# configure port ethernet 3
ETX-203A>config>port>eth(3)# show 12cp-statistics
```

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Encapsulated</th>
<th>Decapsulated</th>
</tr>
</thead>
<tbody>
<tr>
<td>STP</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>CDP</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>VTP</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>LLDP</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PVSTP</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

```
ETX-203A>config>port>eth(3)#
```

Clearing Statistics

To clear the statistics for an Ethernet port:

- At the prompt `config>port>eth(<port-num>)#`, enter:
  `clear-statistics`.
  The statistics for the specified port are cleared.

To clear the L2CP statistics for an Ethernet port:

- At the prompt `config>port>eth(<port-num>)#`, enter:
  `clear-12cp-statistics`.
  The L2CP statistics for the specified port are cleared.

5.14 Smart SFPs

ETX-203A supports integrated configuration and management of smart SFPs (such as MiRICi devices) to provide TDM port functionality. The following are supported:

- MiRICi-E1
- MiRICi-T1
- MiRICi-E3
- MiRICi-T3
- MiRICi-155.

The smart SFP is provisioned in the specific Ethernet port where the SFP shall be inserted. After this provisioning, the Ethernet port is no longer available for normal Ethernet port functioning. The TDM port/s are automatically created when the smart SFP is provisioned.

After you provision a smart SFP, you can do the following:

- Define a logical GFP interface over the smart SFP port (refer to *GFP Ports*)
• Defines a logical MAC interface over the GFP interface (refer to *Logical MAC Ports*).
• Create a flow over the logical MAC interface (refer to *Flows*).

**Benefits**

ETX-203A offers the use of a wide variety of TDM E1/T1/E3/T3 OC-3/STM-1 ports via the smart SFP feature.

**Factory Defaults**

By default, no smart SFPs are provisioned.

**Configuring Smart SFPs**

To provision a smart SFP, you use the `smart-sfp` command to specify the Ethernet port, then you assign the type of smart SFP.

> **To configure smart SFPs:**

1. At the `config>port#` prompt, type `smart-sfp <port>`, where `<port>` indicates the Ethernet port where the SFP is (or shall be) inserted (refer to Table 5-8 for the port numbers).

   **Note**  
   *You can provision the smart SFP before you insert it.*

   The smart SFP interface is created if it does not already exist and the `config>port>smart-sfp(<port>)$` prompt is displayed.

2. Enter all necessary commands according to the tasks listed below.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assigning the type of</td>
<td>`type {mirici-e1</td>
<td>mirici-t1</td>
</tr>
<tr>
<td>smart SFP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Resetting smart SFP</td>
<td><code>reset</code></td>
<td></td>
</tr>
<tr>
<td>Displaying interface</td>
<td><code>show status</code></td>
<td>Using <em>shutdown</em> disables the interface</td>
</tr>
<tr>
<td>status</td>
<td></td>
<td><strong>Note:</strong> When the smart SFP interface is created, it is disabled by default.</td>
</tr>
<tr>
<td>Administratively</td>
<td><code>no shutdown</code></td>
<td></td>
</tr>
<tr>
<td>enabling interface</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Example**

This example shows how a smart SFP can be provisioned, and a flow created over the logical MAC port corresponding to a logical GFP port. The smart SFP can be inserted before or after the provisioning.
To provision a smart SFP and corresponding flow:

- Ethernet port 1
- Smart SFP type = MiRICi-E1
- GFP port 1
- Logical MAC port 1
- Flow = flow1, with classification criterion VLAN 1.

Perform the following steps:

1. Provision the smart SFP.

```
ETX-203A# configure port smart-sfp 1
ETX-203A>config>port>smart-sfp(1)$ type mirici-e1
ETX-203A>config>port>smart-sfp(1)$ info detail
  type      mirici-e1
  no shutdown
ETX-203A>config>port>smart-sfp(1)$ exit
```

2. Create the GFP and bind it to the E1 port.

```
ETX-203A>config>port# gfp 1
ETX-203A>config>port>gfp(1)# bind e1 1
ETX-203A>config>port>gfp(1)# info detail
  name    "GFP 1"
  bind    e1    1
  no fcs-payload
ETX-203A>config>port>gfp(1)$ exit
```

3. Create the logical MAC port and bind it to GFP port 1.

```
ETX-203A>config>port# logical-mac 1
ETX-203A>config>port>log-mac(1)$ bind gfp 1
ETX-203A>config>port>log-mac(1)$ no shutdown
ETX-203A>config>port>log-mac(1)$ info detail
  name    "LOGICAL MAC 1"
  no shutdown
  bind    gfp    1
  tag-ethernet-type 0x8100
  egress-mtu 1790
  queue-group profile "DefaultQueueGroup"
  l2cp profile "L2cpDefaultProfile"
ETX-203A>config>port>log-mac(1)$exit all
```

4. Create the flow and activate it.
5. Insert the MiRICi-E1 device in Ethernet port 1.

### 5.15 E1 Ports

E1 ports are available when smart SFPs such as MiRICi-E1 are provisioned and inserted (refer to Smart SFPs).

The European Conference of Postal and Telecommunications Administrations (CEPT) standardized the E-Carrier system, which was then adopted by the International Union Telecommunication Standardization sector (ITU-T), and is used in almost all countries outside the USA, Canada, and Japan.

The most commonly used versions are E1 and E3. E1 circuits are very common in most telephone exchanges and used to connect medium and large companies to remote exchanges. In many cases, E1 connects exchanges with each other.

#### Standards and MIBs

The original CEPT standard G.703 specifies several options for the physical transmission. In practice, mostly the HDB3 format is used.

#### Benefits

E1 lines are high-speed dedicated lines that enable large volume usage.

#### Functional Description

An E1 link operates over a twisted pair of cables. A nominal 3-volt peak signal is encoded with pulses using a method that avoids long periods without polarity changes. The line data rate is 2.048 Mbps at full duplex, which means 2.048 Mbps downstream and 2.048 Mbps upstream. The E1 signal splits into 32 timeslots each of which is allocated 8 bits. Each timeslot sends and receives an 8-bit
sample 8000 times per second (8 x 8000 x 32 = 2,048,000), which is ideal for voice telephone calls where the voice is sampled into an 8-bit number at that data rate and restored at the other end. The timeslots are numbered from 0 to 24.

Factory Defaults

By default, no E1 ports exist.

Configuring E1 Ports

To configure E1 ports:

1. Provision a smart SFP such as MiRICi-E1 and insert it in an Ethernet port (refer to Smart SFPs).
2. At the config>port# prompt, type:
   
   e1 <port>.

   The config>port>e1(<port>)# prompt is displayed.
3. Enter all necessary commands according to the tasks listed below.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
</table>
| Defining the transmission line code | line-code { hdb3 | ami } | • HDB3 – Referred to as High Density Bipolar of order 3 code, it is a telecommunication line code based on AMI and used in E1 lines. It is similar to B8ZS used in T1 lines  
  • AMI – Referred to as Alternate Mark Inversion because a 1 is referred to as a mark and a 0 as a space |
| Specifying the framing mode of the port | line-type { unframed | g732n | g732n-crc } | • unframed – no framing  
  • g732n – G.732N framing with CRC disabled  
  • g732n-crc – G.732N framing with CRC enabled. |
<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
</table>
| Running loopback test on E1 port | `loopback [local | remote | payload ] [start <seconds>] [duration <seconds>] [time-slot <slot>]` | • **local** – Returns the transmitted data at the physical layer to the receiving path  
• **remote** – Returns the received data at the physical layer to the transmitting path  
• **payload** – Adds a header to the data (reframes the data) and returns the received data at the physical layer to the transmitting path  
• **start** – Specifies the time (in seconds) until the loopback starts. Range is 1 to 3600.  
• **duration** – Specifies the duration of the loopback (in seconds). Range is 1 to 3600. If duration is not specified, the loopback test runs forever, until stopped  
• **time-slot** – Specifies the timeslot on the selected port to be included in the loopback  
Use **no loopback** to disable the loopback test. |
| Assigning a name to the port | `name <string>` |  |
| Specifying the attenuation level of the received signal, compensated for by the interface receive path | `rx-sensitivity [short-haul | long-haul]` | • **short-haul** – Low sensitivity  
• **long-haul** – High sensitivity |
| Selecting the transmit clock source | `tx-clock-source [loopback | internal | domain]` | • **loopback** – Clock retrieved from the port’s incoming (Rx) data  
• **internal** – Clock provided by internal oscillator  
• **domain** – Clock retrieved from clock domain |
| Administratively enabling port | `no shutdown` | Using **shutdown** disables the port |
5.16 T1 Ports

T1 ports are available when smart SFPs such as MiRIGi-T1 are provisioned and inserted (refer to Smart SFPs).

The T-carrier signaling scheme was devised by Bell Labs and is a widely used standard in telecommunications in the USA, Canada, and Japan to transmit voice and data between devices. T1, also referred to as DS-1, is a dedicated data line that transmits information at the speed of 1.544 megabits per second (mbps).

Standards and MIBs

The G.703 standard specifies several options for the physical transmission. In practice, mostly the B8ZS format is used.

Benefits

T1 lines are high-speed dedicated lines that enable large volume usage.

Functional Description

A T1 link operates over a twisted pair of cables. A nominal 3-volt peak signal is encoded with pulses using a method that avoids long periods without polarity changes. The line data rate is 1.544 Mbps at full duplex, which means 1.544 Mbps for downstream and 1.544 Mbps for upstream. The T1 signal splits into 24 timeslots each which is allocated 8 bits. Each timeslot sends and receives an 8-bit sample 8000 times per second (8 x 8000 x 24 = 1,544,000), which is ideal for voice telephone calls where the voice is sampled into an 8-bit number at that data rate and restored at the other end. The timeslots are numbered from 0 to 24.
Factory Defaults

By default, no T1 ports exist.

Configuring T1 Ports

To configure T1 ports:

1. Provision a smart SFP such as MiRICi-T1 and insert it in an Ethernet port (refer to Smart SFPs).

2. At the `config>port#` prompt, type `t1 <port>`.
   The `config>port>t1(<port>)#` prompt is displayed.

3. Enter all necessary commands according to the tasks listed below.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Possible Values</th>
</tr>
</thead>
</table>
| Specifying the variety of zero code suppression used for this port | `line-code { ami | b8zs | b7zs }` | • AMI – Referred to as Alternate Mark Inversion because a 1 is referred to as a mark and a 0 as a space  
• B8ZS – Bipolar 8-zero substitution, in which two successive ones (bipolar violations) are inserted whenever the stream of user data contains a string of eight or more consecutive zeros. This insertion is done in a way that allows each of the 24 channels to carry 64 kbps of data.  
• B7ZS – Bipolar 7-zero substitution, in which two successive ones (bipolar violations) are inserted whenever the stream of user data contains a string of eight or more consecutive zeros. This insertion is done in a way that allows each of the 24 channels to carry 56 kbps of data. |
| Specifying the length of the T1 line in DSU mode (in feet) | `line-length {0-133 | 134-266 | 267-399 | 400-533 | 534-655 }` | • unframed – No framing  
• sf – Super Frame (12 T1 frames)  
• esf – Extended Super Frame (24 T1 frames, with on-line performance monitoring and 4 kbps control data link.) |
| Specifying the T1 line type. | `line-type { unframed | esf | sf }` | • unframed – No framing  
• sf – Super Frame (12 T1 frames)  
• esf – Extended Super Frame (24 T1 frames, with on-line performance monitoring and 4 kbps control data link.) |
<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Possible Values</th>
</tr>
</thead>
</table>
| Running loopback test on T1 port          | `loopback [local | remote | payload ] [start <seconds>] [duration <seconds>] [time-slot <slot>]`   | • *local* – Returns the transmitted data at the physical layer to the receiving path  
• *remote* – Returns the received data at the physical layer to the transmitting path  
• *payload* – Adds a header to the data (reframes the data) and returns the received data at the physical layer to the transmitting path  
• *start* – Specifies the time (in seconds) until the loopback starts. Range is 1 to 3600.  
• *duration* – Specifies the duration of the loopback (in seconds). Range is 1 to 3600. If duration is not specified, the loopback test runs forever, until stopped  
• *time-slot* – Specifies the timeslot on the selected port to be included in the loopback  
Use `no loopback` to disable the loopback test. |
| Assigning a name to the port              | `name <string>`                |                                                                                  |
| Specifying attenuation level of the receive signal that is compensated for by the interface receive path | `rx-sensitivity [ short-haul | long-haul ]`                      |                                                                                  |
| Selecting the transmit clock source       | `tx-clock-source [loopback | internal | domain ]`                  | • *loopback* – Clock retrieved from the port’s incoming (Rx) data  
• *internal* – Clock provided by internal oscillator  
• *domain* – Clock retrieved from clock domain |
| Administratively enabling port            | `no shutdown`                  | Using `shutdown` disables the port                                              |
| Displaying alarms for port               | `show alarms`                  |                                                                                  |
| Displaying list of interfaces bound to port | `show bind`                    |                                                                                  |
| Displaying loopback test status          | `show loopback`                |                                                                                  |
| Displaying the port status               | `show status`                  |                                                                                  |
### 5.17 E3 Ports

E3 ports are available when smart SFPs such as MiRiCi-E3 are provisioned and inserted (refer to Smart SFPs).

Groups of E1 circuits are bundled into higher-capacity E3 links, which are mainly used between exchanges, operators, and/or countries, and have a transmission speed of 34.368 Mbps.

#### Standards and MIBs

G.703 specifies several options for the physical transmission.

#### Benefits

E3 lines provide high-capacity circuits.

#### Functional Description

Each E3 signal has 16 E1 channels, and each channel transmits at 2.048 Mbps. E3 links use all 8 bits of a channel.

#### Factory Defaults

By default, no E3 ports exist.

#### Configuring E3 Ports

1. Provision a smart SFP such as MiRiCi-E3 and insert it in an Ethernet port (refer to Smart SFPs).
2. At the `config>port#` prompt, type `e3 <port>`.
   The `config>port>e3{<port>}`# prompt is displayed.
3. Enter all necessary commands according to the tasks listed below.
### Configuration

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Running loopback test on E3 port</td>
<td>`loopback [local</td>
<td>remote ]</td>
</tr>
</tbody>
</table>
  
  [start <seconds> ]  
  
  [duration <seconds>]` |  
  
  • **local** – Returns the transmitted data at the physical layer to the receiving path  
  
  • **remote** – Returns the received data at the physical layer to the transmitting path  
  
  • **start** – Specifies the time (in seconds) until the loopback starts. Range is 1 to 3600.  
  
  • **duration** – Specifies the duration of the loopback (in seconds). Range is 1 to 3600. If duration is not specified, the loopback test runs forever, until stopped.  
  
  Use **no loopback** to disable the loopback test. |
| Assigning a name to the port | `name <string>` |  
  
  Use **no name** to remove the name. |
| Selecting the transmit clock source | `tx-clock-source {loopback | internal | domain }` |  
  
  • **loopback** – Clock retrieved from the port’s incoming (Rx) data  
  
  • **internal** – Clock provided by internal oscillator  
  
  • **domain** – Clock retrieved from clock domain |
| Administratively enabling port | `no shutdown` |  
  
  Using **shutdown** disables the port. |
| Displaying alarms for port | `show alarms` |  
  
  Use **no show alarms** to clear the alarms. |
| Displaying list of interfaces bound to port | `show bind` |  
  
  Use **no show bind** to clear the list. |
| Displaying loopback test status | `show loopback` |  
  
  Use **no show loopback** to clear the status. |
| Displaying the port status | `show status` |  
  
  Use **no show status** to clear the status. |
| Displaying the port statistics | `show statistics current`  
  
  show statistics interval <interval-num>  
  
  show statistics all-intervals  
  
  show statistics all |  
  
  Use **no show statistics** to clear the statistics. |
| Clearing the statistics | `clear-statistics` |  
  
  Use **no clear-statistics** to clear the statistics. |
5.18 T3 Ports

T3 ports are available when smart SFPs such as MiRICi-T3 are provisioned and inserted (refer to *Smart SFPs*).

T3, also referred to as DS-3 (Digital Signal Level 3), equates to 28 T-1 lines or 44.736 million bits per second (roughly 43-45 Mbps upstream/downstream speeds). DS-3s have enough bandwidth to allow very large database transfers over busy wide area networks.

Standards and MIBs

The G.703 standard specifies several options for the physical transmission. In practice, mostly the B3ZS format is used.

Benefits

T3 lines enable high-capacity Ethernet services in remote locations and transparently connect corporate LANs over existing PDH infrastructure.

Functional Description

In North America, DS-3 translates into T-3, which is the equivalent of 28 T-1 channels, each operating at 1.544 Mbps. The 28 T-1s are multiplexed through an M13 (‘Multiplex 1-to-3’ multiplexer), and 188 additional signaling and control bits are added to each T-3 frame. Alternatively, four T-1s are multiplexed to a T-2 frame, then seven T-2 frames are multiplexed, through an M23 (‘Multiplex 2-to-3’ multiplexer). As each frame is transmitted 8,000 times per second, the total T-3 signaling rate is 44.736 Mbps.

Factory Defaults

By default, no T3 ports exist.

Configuring T3 Ports

To configure T3 ports:

1. Provision a smart SFP such as MiRICi-T3 and insert it in an Ethernet port (refer to *Smart SFPs*).
2. At the `config>port#` prompt, type `t3 <port>`. The `config>port>t3(<port>)#` prompt is displayed.
3. Enter all necessary commands according to the tasks listed below.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifying the length (in feet) of the T3 line</td>
<td>`line-length { up-to-225ft</td>
<td>over-225ft }`</td>
</tr>
</tbody>
</table>
### Configuration

#### Specifying type of T3 line

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
</table>
| Specifying type of T3 line | `line-type { m13 | m23 | c-bit-parity }` | - **m13** – 28 DS1 signals are multiplexed into one DS3 signal  
- **m23** – Four DS1 signals are multiplexed into one DS2 signal, then seven DS2 signals are multiplexed into one DS3 signal  
- **c-bit parity** – The c-bit parity framing format is an enhancement of the original M13 application, providing greater management and performance functions. |

#### Running loopback test on T3 port

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
</table>
| Running loopback test on T3 port | `loopback {local | remote } [start <seconds> | [duration <seconds>]]` | - **local** – Returns the transmitted data at the physical layer to the receiving path  
- **remote** – Returns the received data at the physical layer to the transmitting path  
- **start** – Specifies the time (in seconds) until the loopback starts. Range is 1 to 3600.  
- **duration** – Specifies the duration of the loopback (in seconds). Range is 1 to 3600. If duration is not specified, the loopback test runs forever, until stopped.  
Use **no loopback** to disable the loopback test. |

#### Assigning a name to the port

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assigning a name to the port</td>
<td><code>name &lt;string&gt;</code></td>
<td></td>
</tr>
</tbody>
</table>

#### Selecting the transmit clock source

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
</table>
| Selecting the transmit clock source | `tx-clock-source {loopback | internal }` | - **loopback** – Clock retrieved from the port’s incoming (Rx) data  
- **internal** – Clock provided by internal oscillator. |

#### Administratively enabling port

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administratively enabling port</td>
<td><code>no shutdown</code></td>
<td>Using <strong>shutdown</strong> disables the port</td>
</tr>
</tbody>
</table>

#### Displaying alarms for port

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Displaying alarms for port</td>
<td><code>show alarms</code></td>
<td></td>
</tr>
</tbody>
</table>

#### Displaying list of interfaces bound to port

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Displaying list of interfaces bound to port</td>
<td><code>show bind</code></td>
<td></td>
</tr>
</tbody>
</table>

#### Displaying loopback test status

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Displaying loopback test status</td>
<td><code>show loopback</code></td>
<td></td>
</tr>
</tbody>
</table>

#### Displaying the port status

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Displaying the port status</td>
<td><code>show status</code></td>
<td></td>
</tr>
</tbody>
</table>
### 5.19 SDH/SONET Ports

SDH/SONET ports are available when smart SFPs such as MiRICi-155 are provisioned and inserted (refer to Smart SFPs).

SDH (Synchronous Digital Hierarchy) and SONET (Synchronous Optical Network) are standardized transport protocols that transfer multiple digital bit streams over optical fiber using lasers or light-emitting diodes (LEDs). SONET is the United States version and SDH is the international version.

#### Standards and MIBs

SDH is defined by ITU-T G.707, G.781, G.782, G.783, and G.803. SONET is an ANSI standard defined in T1.105 and T1.119.

#### Benefits

SDH and SONET allow many different circuits from different sources to be transported simultaneously within one single framing protocol.

#### Functional Description

SDH is based on STM-1 which has a data rate of 155.52 Mbps, equivalent to STS-3. SONET is based on transmission at speeds of multiples of 51.840 Mbps, or STS-1.

#### Factory Defaults

By default, no SDH/SONET ports exist.

#### Configuring SDH/SONET Ports

To configure SDH/SONET ports:

1. Provision a smart SFP such as MiRICi-155 and insert it in an Ethernet port (refer to Smart SFPs).
2. At the config>port# prompt, type `sdh-sonet <port>`.
   
   The `config>port>sdh-sonet{<port>}#` prompt is displayed.
3. Enter all necessary commands according to the tasks listed below.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifying the cell frame type</td>
<td>`frame-type { sdh</td>
<td>sonet }`</td>
</tr>
</tbody>
</table>
| Running loopback test on port             | `loopback { local | remote }` [start <seconds>] [duration <seconds>] | • local – Returns the transmitted data at the physical layer to the receiving path  
• remote – Returns the received data at the physical layer to the transmitting path  
• start – Specifies the time (in seconds) until the loopback starts  
• duration – Specifies the duration of the loopback (in seconds). If duration is not specified, the loopback test runs forever, until stopped.  
Use no `loopback` to disable the loopback test. |
| Assigning a name to the port              | `name <string>`                             |                                                                                                                                         |
| Defining thresholds:                      | `threshold [ eed { 1e-3 | 1e-4 | 1e-5 } ]` [sd { 1e-5 | 1e-6 | 1e-7 | 1e-8 | 1e-9 } ]` | • EED (Excessive Error Defect) – detected if the equivalent BER (bit error rate) exceeds the selected threshold parameter  
• SD (Degraded Signal Defect) – detected if the equivalent BER exceeds the selected threshold parameter. |
| Enabling/disabling triggering of AIS & RDI if path trace error occurs | `tim-response`                             | Using no `tim-response` disables the triggering |
| Selecting the transmit clock source       | `tx-clock-source { internal | loopback }` | • internal – Clock provided by internal oscillator  
• loopback – Clock retrieved from the port’s incoming (Rx) data. |
<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administratively enabling port</td>
<td><code>no shutdown</code></td>
<td>Using <code>shutdown</code> disables the port</td>
</tr>
<tr>
<td>Displaying list of interfaces bound to</td>
<td><code>show bind</code></td>
<td></td>
</tr>
<tr>
<td>port</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Displaying the port status</td>
<td><code>show status</code></td>
<td></td>
</tr>
<tr>
<td>Displaying the port statistics</td>
<td><code>show statistics current</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>show statistics interval &lt;interval-num&gt;</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>show statistics all-intervals</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>show statistics all</code></td>
<td></td>
</tr>
<tr>
<td>Defining administrative unit group</td>
<td><code>aug &lt;aug-num&gt;</code></td>
<td></td>
</tr>
</tbody>
</table>

**Commands in aug level**

| Configuring J1 path trace               | `j1-pathtrace [direction {rx | tx | rx-tx}] [tx-string <tx-string>] [padding {spaces | nulls}]` | Direction of J1 path trace is defined by `direction`:
|                                          |                                                                         | - rx – Receiving
|                                          |                                                                         | - tx – Transmitting
|                                          |                                                                         | - rx-tx – Receiving and transmitting.
|                                          |                                                                         | Transmit string for trace is defined by `tx-string`.
|                                          |                                                                         | Padding for transmit string is defined by `padding`:
|                                          |                                                                         | - spaces – Space characters
|                                          |                                                                         | - nulls – Null characters. |
| Running loopback test                   | `loopback {local | remote } [start <seconds>] [duration <seconds>]`      | `local` – Returns the transmitted data at the physical layer to the receiving path
|                                          |                                                                         | `remote` – Returns the received data at the physical layer to the transmitting path
|                                          |                                                                         | `start` – Specifies the time (in seconds) until the loopback starts
|                                          |                                                                         | `duration` – Specifies the duration of the loopback (in seconds). If duration is not specified, the loopback test runs forever, until stopped.
<p>|                                          |                                                                         | Use <code>no loopback</code> to disable the loopback test. |</p>
<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifying the payload string to attach to packets</td>
<td><code>payload-label &lt;label-val&gt;</code></td>
<td></td>
</tr>
<tr>
<td>Enabling the sending of remote defect indication (RDI) if payload string mismatch (PLM-P) occurs</td>
<td><code>plm-response</code></td>
<td>Using no <code>plm-response</code> disables the sending of RDI on PLM</td>
</tr>
<tr>
<td>Enabling the sending of remote defect indication (RDI) if trace identifier mismatch payload (TIM-P) occurs</td>
<td><code>tim-response</code></td>
<td>Using no <code>tim-response</code> disables the sending of RDI on TIM</td>
</tr>
<tr>
<td>Defining an OC-3 (STM-1) connection</td>
<td><code>oc3 &lt;oc3-num&gt;</code></td>
<td></td>
</tr>
</tbody>
</table>

### Commands in `oc3` level

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Details</th>
</tr>
</thead>
</table>
| Configuring J1 path trace | `j1-pathtrace [direction {rx | tx | rx-tx}] [tx-string <tx-string>] [padding {spaces | nulls}]` | Direction of J1 path trace is defined by `direction`:
  - `rx` – Receiving
  - `tx` – Transmitting
  - `rx-tx` – Receiving and transmitting.
  Transmit string for trace is defined by `tx-string`.
  Padding for transmit string is defined by `padding`:
  - `spaces` – Space characters
  - `nulls` – Null characters. |
| Running loopback test | `loopback {local | remote } [start <seconds>] [duration <seconds>]` | `local` – Returns the transmitted data at the physical layer to the receiving path
`remote` – Returns the received data at the physical layer to the transmitting path
`start` – Specifies the time (in seconds) until the loopback starts
`duration` – Specifies the duration of the loopback (in seconds). If duration is not specified, the loopback test runs forever, until stopped. Use no `loopback` to disable the loopback test. |
### 5.20 GFP Ports

ETX-203A uses GFP (Generic Framing Procedure) ports to provide a logical link to the TDM ports that become available when smart SFPs are inserted (refer to *Smart SFPs*).

ETX-203A supports up to 16 GFP ports.

#### Factory Defaults

By default, no GFP ports exist. When a GFP port is created, it is configured as shown below.

<table>
<thead>
<tr>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port name</td>
<td>GFP ( \langle n \rangle )</td>
</tr>
<tr>
<td>Enabling/disabling CRC-32 sequence of GFP packet payload</td>
<td>No FCS payload</td>
</tr>
</tbody>
</table>

#### Configuring GFP Logical Ports

1. **To configure GFP logical ports:**
   1. At the `config>port#` prompt, type `gfp <port>`.
      The port is created if it does not already exist, and the `config>port>gfp(\langle port\rangle)#` prompt is displayed.
   2. Enter all necessary commands according to the tasks listed below.
### Task | Command | Comments
---|---|---
Binding GFP port to E1 port | bind e1 <port> | **Note**: Successful only if a smart SFP that provides the E1 port has been provisioned.

Binding GFP port to T1 port | bind t1 <port> | **Note**: Successful only if a smart SFP that provides the T1 port has been provisioned.

Binding GFP port to E3 port | bind e3 <port> | **Note**: Successful only if a smart SFP that provides the E3 port has been provisioned.

Binding GFP port to T3 port | bind t3 <port> | **Note**: Successful only if a smart SFP that provides the T3 port has been provisioned.

Binding GFP port to SDH/SONET port | bind sdh-sonet <port> | **Note**: Successful only if a smart SFP that provides the SDH/SONET port has been provisioned.

Enabling/disabling CRC-32 sequence of GFP packet payload | fcs-payload | Type no fcs-payload to disable

Assigning name to GFP port | name <string> |

Displaying GFP port status | show status |

### Example

- To configure GFP logical port 1:
  - Bind to E1 port 1.

```
ETX-203A>config>port$ gfp 1
ETX-203A>config>port>gfp(1)$ bind e1 1
ETX-203A>config>port>gfp(1)$ info detail
  name  "GFP 1"
  bind  e1  1
  no fcs-payload

ETX-203A>config>port>gfp(1)$ show status
Name          : GFP 1
Administrative Status : Up
Operation Status   : Up
ETX-203A>config>port>gfp(1)$ exit
```

### 5.21 Logical MAC Ports

ETX-203A uses logical MAC ports to connect flows to GFP (Generic Framing Procedure) ports that provide a logical link to the TDM ports that become available when smart SFPs are inserted (refer to **Smart SFPs**).

ETX-203A supports up to 16 logical MAC ports.
Factory Defaults

By default, no logical MAC ports exist. When a logical MAC port is created, it is configured as shown below.

<table>
<thead>
<tr>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port name</td>
<td>LOGICAL MAC &lt;logical-mac-port-number&gt;</td>
</tr>
<tr>
<td>Administrative status</td>
<td>Disabled</td>
</tr>
<tr>
<td>Port to which the MAC is bound</td>
<td>GFP 1</td>
</tr>
<tr>
<td>Ethernet tag protocol identifier</td>
<td>0x8100</td>
</tr>
<tr>
<td>Egress MTU</td>
<td>1790</td>
</tr>
<tr>
<td>Queue group profile</td>
<td>DefaultQueueGroup</td>
</tr>
<tr>
<td>L2CP profile</td>
<td>L2cpDefaultProfile</td>
</tr>
</tbody>
</table>

Configuring Logical MAC ports

To configure logical MAC ports:

1. At the `config>port#` prompt, type `logical-mac <port>`. The port is created if it does not already exist, and the `config>port>log-mac(<port>)#` prompt is displayed.

2. Enter all necessary commands according to the tasks listed below.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Possible Values</th>
</tr>
</thead>
</table>
| Binding logical MAC port to GFP port | `bind gfp <port>`             | • The GFP port must exist  
• Use the `no bind` form to remove the binding                                      |
| Specifying conditions for sending DHCP request | `dhcp-request {never | normal | when-up}` | `never` – DHCP request is never sent  
`normal` – DHCP request is sent for the normal reasons, e.g. if the device needs to acquire an IP address or the IP address is about to expire  
`when-up` – In addition to the normal reasons listed above, a DHCP request is sent whenever the port is activated or becomes operational |
| Setting maximum frame size to transmit (frames above the specified size are discarded) | `egress-mtu <size>` | Maximum size is 12,288  

| Associating a Layer-2 control processing profile with the port | `l2cp profile <l2cp-profile-name>` |                                          |
### Task Command Possible Values

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Possible Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Running loopback test on port</td>
<td>`loopback [local</td>
<td>remote]` [duration &lt;seconds&gt;]</td>
</tr>
<tr>
<td>Assigning a name to the port</td>
<td><code>name &lt;string&gt;</code></td>
<td></td>
</tr>
<tr>
<td>Associating a queue group profile with the port</td>
<td><code>queue-group profile &lt;queue-profile-name&gt;</code></td>
<td></td>
</tr>
<tr>
<td>Setting the VLAN tagged frame ETH II frame Ethertype (tag protocol identifier)</td>
<td><code>tag-ethernet-type &lt;0x0000-0xFFFF&gt;</code></td>
<td>Ethernet type value: 0x0000–0xFFFF</td>
</tr>
<tr>
<td>Administratively enabling port</td>
<td><code>no shutdown</code></td>
<td>Using <code>shutdown</code> disables the port</td>
</tr>
<tr>
<td>Displaying the interfaces that are bound to the port</td>
<td><code>show bind</code></td>
<td></td>
</tr>
<tr>
<td>Displaying port status</td>
<td><code>show status</code></td>
<td></td>
</tr>
<tr>
<td>Displaying port statistics</td>
<td><code>show statistics</code></td>
<td></td>
</tr>
<tr>
<td>Clearing port statistics</td>
<td><code>clear-statistics</code></td>
<td></td>
</tr>
</tbody>
</table>

### Example

To configure logical MAC port 1:

- Bind to GFP port 1.

```
ETX-203A>config>port# logical-mac 1
ETX-203A>config>port>log-mac(1)$ bind gfp 1
ETX-203A>config>port>log-mac(1)$ no shutdown
ETX-203A>config>port>log-mac(1)$ info detail
  name  "LOGICAL MAC 1"
    no shutdown
    bind gfp 1
    tag-ethernet-type 0x8100
    egress-mtu 1790
    queue-group profile "DefaultQueueGroup"
    l2cp profile "L2cpDefaultProfile"
ETX-203A>config>port>log-mac(1)$ show status
Name : LOGICAL MAC 1
Administrative Status : Up
Operational Status : Up
ETX-203A>config>port>log-mac(1)$
```

### 5.22 Network Interface Redundancy

Two network interfaces operate redundant to each other, either as a single logical link (LAG) or two separate links (1:1).

- **Link aggregation (LAG) mode according to IEEE 802.3-2005.** In this mode, both ports receive traffic at the same time and one port transmits. If the
transmitting port fails, ETX-203A switches to the standby link. Both network ports must be enabled. If activated, LACP control frames are periodically transmitted in order to locate failures as they occur.

- **1:1 bidirectional protection (redundancy) mode.** In this mode, only one port is active at a time to carry traffic. If it fails, the second port takes over. The recovery mode (revertive or non-revertive) and the restoration time in revertive mode can be selected according to the application requirements.

![Figure 5-9. Link Aggregation between a Switch and ETX-203A](image)

When deciding whether to operate with LAG or protection, you can consider the following if protection without LACP is acceptable in your application:

- Protection – You can configure parameters such as revertive/non-revertive mode, the restoration time in revertive mode, forcing active link, etc., but the switchover time to the standby link is longer than for LAG
- LAG – The switchover time to the standby link is shorter than for protection, but you can’t configure the parameters mentioned above.

**Standards and MIBs**

IEEE 802.3-2005

**Benefits**

ETX-203A can continue to route traffic even if one of the network ports fails.

**Functional Description**

**Link Aggregation**

The two Gigabit Ethernet ports can be operated as a single logical interface, using link aggregation in accordance with IEEE 802.3-2005. The two ports must be connected to the same switch/router, as shown in Figure 5-10.

The equipment connected to the GbE ports must use compatible switching criteria for redundancy to be available:

- For networks using Layer 2 switching – The criterion is signal loss
- For networks using Layer 3 routing – The router must support IEEE 802.3-2005 or other link aggregation protocol that views the aggregated link as a single logical interface.

![Figure 5-10. Network Link Aggregation Redundancy Mode](image)
Using link aggregation inherently provides redundancy, because if one of the GbE ports fails, the other can continue transferring traffic. Failure of a link is detected by sensing the loss of valid signals, or receiving a failure report via Link Aggregation Control Protocol (LACP) if applicable, in which case all traffic is sent through the other link.

### 1:1 Bidirectional Redundancy

As an alternative to link aggregation, the two ETX-203A network ports can be configured for 1:1 bidirectional mode. With this mode, two topologies can be used:

- Connection of both ports to the same switch/router, as shown in [Figure 5-10](#).
- Connection of the ports to different switch/routers, as illustrated in [Figure 5-11](#). The main advantage of this topology is its higher availability, because each port can be routed along a different path through the network. This topology is also referred to as dual homing.

![Figure 5-11. 1:1 Bidirectional Redundancy Mode (Dual Homing)](image)

With 1:1 bidirectional redundancy mode, at any time only one of the ports is actively carrying traffic, and the other port serves as the backup port. A RAD proprietary redundancy algorithm, based on loss of GbE signal, is used to detect line failure. The protection switching (flipping) time is less than 1 second. It also depends on the network “relearning” time or aging.

The recovery mode after protection switching can be selected in accordance with the application requirements:

- Non-revertive mode – ETX-203A does not automatically flip back after the failed port returns to normal operation, but only when the currently used port fails, or after a manual flip command.
- Revertive mode – ETX-203A flips back to the original port when it returns to normal operation. Flipping back can be delayed by specifying a restoration time, during which alarms are ignored. As a result, ETX-203A starts evaluating the criteria for protection switching (flipping) only after the restoration time expires, thereby ensuring that another flip cannot occur before the specified time expires.

### Factory Defaults

By default, neither LAG nor bidirectional redundancy is enabled.

### Configuring LAG

This section explains how to define a link aggregation group (LAG) and enable link aggregation control protocol (LACP). ETX-203A supports one LAG.
In order to enable LACP for the LAG, the ports bound to the LAG must be associated with an L2CP profile that specifies peer action for MAC 0x02.

To configure the LAG:

1. Navigate to `configure port lag 1`.

   The `config>port>lag(1)#` prompt is displayed.

2. Enter all necessary commands according to the tasks listed below.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assigning an admin key to the LAG to indicate the port speed</td>
<td>`admin-key {giga-ethernet</td>
<td>fast-ethernet}`</td>
</tr>
<tr>
<td>Adding a port to the LAG</td>
<td>`bind {ethernet</td>
<td>giga-ethernet</td>
</tr>
</tbody>
</table>
| Enabling LACP and setting LACP parameters: operation mode (active or passive) and time to wait before sending LACP frames (long or short) | `lacp [tx-activity {active | passive}] [tx-speed {long | short}]` | `tx-activity:`
|                                           |                                              | active – LAG interface periodically transmits LACP frames (LACPDUs) to all links with LACP enabled
|                                           |                                              | passive – LAG interface does not initiate the LACP exchange, but replies to received LACPDUs.
|                                           |                                              | `tx-speed:`
|                                           |                                              | short – Three seconds
|                                           |                                              | long – 90 seconds. |
|                                           |                                              | Defaults:
|                                           |                                              | • If you type `lacp` without specifying `tx-activity`, it is set to `active`
|                                           |                                              | • If you type `lacp` without specifying `tx-speed`, it is set to `short`
<p>|                                           |                                              | Typing <code>no lacp</code> disables LACP protocol |
| Assigning value that determines aggregation precedence. If there are two partner devices competing for the same LAG, LACP compares the priorities for each grouping of ports. The LAG with the lower priority is given precedence. | <code>sys-priority &lt;0–65535&gt;</code> |                                                                                                                                 |</p>
<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
</table>
| Assigning method of distributing traffic within LAG | distribution-method {src-mac | dest-mac | src-or-dest-mac | src-and-dest-mac | src-ip | dest-ip | src-dest-mac-ip | round-robin | source-port | one-to-one} | src-mac – Packets are distributed according to their source MAC addresses  
dest-mac – Packets are distributed according to their destination MAC addresses  
src-or-dest-mac – Packets are distributed according to their source or destination MAC addresses  
src-and-dest-mac – Packets are distributed according to their source and destination MAC addresses  
src-ip – Packets are distributed according to their source IP addresses  
dest-ip – Packets are distributed according to their destination IP addresses  
src-dest-mac-ip – Packets are distributed according to their source and destination MAC and IP addresses  
round-robin – Packets are distributed evenly across all of the links  
source-port – Packets are distributed according to their source port |
| Administratively enabling LAG | no shutdown | Using shutdown disables the LAG |
| Displaying LAG member status | show members-status | |
| Displaying LAG member statistics | show members-statistics | |

**Example**

- To define LAG 1:
  - L2CP profile mac2peer, with mac0x02 set to peer action
  - LAG members – Ethernet ports 1 and 2, with assigned L2CP profile mac2peer
  - LACP operation mode – Active
  - LACP timeout – Short
  - Distribution method – Source port
  - System priority – 40,000.
ETX-203A#configure port l2cp-profile mac2peer
ETX-203A>config>port>l2cp-profile(mac2peer)$ mac 0x02 peer
ETX-203A>config>port>l2cp-profile(mac2peer)$ exit
ETX-203A>config>port# eth 1 l2cp profile mac2peer
ETX-203A>config>port# eth 2 l2cp profile mac2peer
ETX-203A>config>port# lag 1
ETX-203A>config>port>lag(1)$ admin-key giga-ethernet
ETX-203A>config>port>lag(1) $bind ethernet 1
ETX-203A>config>port>lag(1) $bind ethernet 2
ETX-203A>config>port>lag(1) $lACP tx-activity active tx-speed short
ETX-203A>config>port>lag(1) $distribution-method source-port
ETX-203A>config>port>lag(1) sys-priority 40000
ETX-203A>config>port>lag(1) $no shutdown
ETX-203A>config>port>lag(1) $

To display the status of the LAG members:

ETX-203A#configure port lag 1
ETX-203A>config>port>lag(1)# show members-status

<table>
<thead>
<tr>
<th>Actor</th>
<th>Partner</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Number</td>
<td>1</td>
</tr>
<tr>
<td>Collecting</td>
<td>No</td>
</tr>
<tr>
<td>Distributing</td>
<td>No</td>
</tr>
<tr>
<td>Synchronized</td>
<td>No</td>
</tr>
<tr>
<td>System ID</td>
<td>0020D230CC9D</td>
</tr>
<tr>
<td>System Priority</td>
<td>0000000000000</td>
</tr>
<tr>
<td>Operational Key</td>
<td>0</td>
</tr>
<tr>
<td>Tx Activity</td>
<td>Active</td>
</tr>
<tr>
<td>Timeout</td>
<td>Short</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Actor</th>
<th>Partner</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Number</td>
<td>2</td>
</tr>
<tr>
<td>Collecting</td>
<td>No</td>
</tr>
<tr>
<td>Distributing</td>
<td>No</td>
</tr>
<tr>
<td>Synchronized</td>
<td>No</td>
</tr>
<tr>
<td>System ID</td>
<td>0020D230CC9D</td>
</tr>
<tr>
<td>System Priority</td>
<td>0000000000000</td>
</tr>
<tr>
<td>Operational Key</td>
<td>0</td>
</tr>
<tr>
<td>Tx Activity</td>
<td>Active</td>
</tr>
<tr>
<td>Timeout</td>
<td>Short</td>
</tr>
</tbody>
</table>

ETX-203A>config>port>lag(1)#
To display LAG statistics:

```bash
ETX-203A#configure port lag 1
ETX-203A>config>port>lag(1)# show members-statistics
```

```
LACP  
---------------------------------------------------------------
Port Number               : 1
Rx LACP Frames            : 0
Rx Marker Frames          : 0
Rx Marker response Frames : 0
Rx Unknown Frames         : 0
Rx Illegal Frames         : 0
Tx LACP Frames            : 1
Tx Marker Frames          : 0
Tx Marker response Frames : 0
Port Number               : 2
Rx LACP Frames            : 0
Rx Marker Frames          : 0
Rx Marker response Frames : 0
Rx Unknown Frames         : 0
Rx Illegal Frames         : 0
Tx LACP Frames            : 1
Tx Marker Frames          : 0
Tx Marker response Frames : 0
ETX-203A>config>port>lag(1)#
```

### Configuring Link Protection

Configuring a 1:1 protection requires defining an Ethernet group.

#### To define an Ethernet group:

- At the Protection context (config>protection), enter
  `ethernet-group <group id>`.

  The system switches to the context of the specified Ethernet group
  (config>protection>eth-group(<group id>)).

#### To add/remove protection and working ports – in manual mode:

- At the Ethernet Group context (config>protection>eth-group(<group id>)), enter
  `bind ethernet primary <port>`
- To remove protection and working ports, enter
  `no bind ethernet primary`

#### To add/remove protection and working ports – in 1-to-1 mode:

- At the Ethernet Group context (config>protection>eth-group(<group id>)), enter:
  `bind ethernet [primary <port>] [secondary <port>]`
- To remove protection and working ports, enter
  `no bind ethernet primary`
  `no bind ethernet secondary`
To define the operation mode:
- At the Ethernet Group context (config>protection>eth-group(<group id>)), enter `oper-mode {1-to-1|manual}`.

To define the port recovery mode as revertive:
- At the Ethernet Group context (config>protection>eth-group(<group id>)), enter:`revertive`. Traffic is switched back to the primary port after it recovers.

To define the port recovery mode as non-revertive:
- At the Ethernet Group context (config>protection>eth-group(<group id>)), enter:`no revertive`. Traffic continues being transmitted over the secondary port after the primary port recovers.

To define the time between recovery and resumption of transmission
- At the Ethernet Group context (config>protection>eth-group(<group id>)), enter:`wait-to-restore <seconds>`. The primary port resumes transmitting traffic once the specified time has been restored and the specified time has elapsed. You can choose between 1 and 720 seconds.

To define the period of time that the failed link stops transmitting to report the failure:
- At the Ethernet Group context (config>protection>eth-group(<group id>)), enter:`tx-down-duration-upon-flip <seconds>`. The secondary port resumes transmitting after the specified 'reporting' time. You may specify a time in the range between 0 and 30 seconds. This function is useful if there is no autonegotiation between the link end points.

To force a port to transmit:
- At the Ethernet Group context (config>protection>eth-group(<group id>)), enter:`force-active-port ethernet <port>`. The specified port is set to be active. You can choose the primary port (1) or the secondary port (2).
  - **Port 1.** Port 1 is configured as a permanently active link. Even if port 1 fails, the traffic is not switched to the standby port.
  - **Port 2.** Port 2 is configured as a permanently active link. Even if port 2 fails, the traffic is not switched to the standby port.

To specify that neither of the ports is forced to remain active, enter:`no force-active-port`
To display the Ethernet group status:

- At the EthernetGroup context (config>protection>eth-group(<group id>)), enter:
  
  `show status`.

  The Ethernet group status parameters are displayed.

Example

To define link protection:

- Ethernet group 1
- Protection port – Ethernet port 1
- Working port – Ethernet port 2
- Operation mode – One-to-one.

```
ETX-203A#configure protection
ETX-203A>config>protection# ethernet-group 1
ETX-203A>config>protection>eth-group(1)# bind ethernet primary 1 secondary 2
ETX-203A>config>protection>eth-group(1)# oper-mode 1-to-1
ETX-203A>config>protection>eth-group(1)# info detail
  bind   ethernet primary 1 secondary 2
  oper-mode 1-to-1
  revertive
  wait-to-restore 0
  tx-down-duration-upon-flip 0
  no shutdown
ETX-203A> configure protection
```
Standards

ITU-T G.8031

Benefits

The Ethernet linear protection provides a way to protect the flows belonging to an EVC.

Functional Description

The protection is based on an EVC Termination Point (ETP). An ETP has one subscriber port and one or more transport ports. Multiple transport ports are used for protection only. There are two kinds of flows connected to the ETP ports, subscriber flows and transport flows.

- Subscriber flows run between UNIs and ETP subscriber port. You can define classification and policing on subscriber flows. You cannot define actions such as push and pop on subscriber flows, however you can define marking.

- Transport flows run between ETP transport ports and NNIs. You can define actions such as push, pop, and marking on transport flows.

flows entering the ETP assign an internal CoS value to every frame using mapping profiles (priority-to-CoS) or by setting fixed CoS values.

Flows exiting the ETP perform queuing based on the internal CoS value using mapping profiles (CoS-to-queue).

ETP Flow Attributes

The following table shows which attributes you can configure for ETP flows.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Subscriber (UNI to ETP)</th>
<th>Subscriber (ETP to UNI)</th>
<th>Transport (NNI to ETP)</th>
<th>Transport (ETP to NNI)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ingress port</td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
</tr>
<tr>
<td>Egress port</td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
</tr>
<tr>
<td>Classifier profile</td>
<td>Required, with any type of criteria</td>
<td>Required, with criteria: Unclassified VLAN</td>
<td>Required, with criteria: SP VLAN</td>
<td>Required, with criteria: Unclassified</td>
</tr>
<tr>
<td>Policer profile</td>
<td>Optional</td>
<td>Optional</td>
<td>Not allowed</td>
<td>Not allowed</td>
</tr>
<tr>
<td>Queue / block</td>
<td>Not allowed</td>
<td>Required, with queue mapping profile classified by CoS</td>
<td>Not allowed</td>
<td>Required, with queue mapping profile classified by CoS</td>
</tr>
<tr>
<td>CoS</td>
<td>Required, with CoS mapping profile</td>
<td>Not allowed</td>
<td>Required, with CoS mapping profile</td>
<td>Not allowed</td>
</tr>
</tbody>
</table>
### EVC Protection Switching

EVC protection (1:1) is based on the ETP model. One of the transport ports is the working transport entity and the other port serves as the protection transport entity.

Monitoring both working and protection transport entity is done via MEPs exchanging CCMs. In addition the protection transport optionally runs APS protocol.

### Master and Slave ETPs

You can define one master ETP and several slave ETPs. The master ETP must have all the configuration of the protection, same as single ETP. The slave ETPs point to the master ETP via `master` command and bind each port ID to working/protection.

The master ETP index MUST be lower than the index of the slave ETPs. You must create the master ETP before creating the slave ETPs.

### EVC and OAM

On each transport entity you must define a MEP in order to monitor the connection using CCM. The MEPs must be activated so that the protection switching mechanism can monitor both working and protection transport entities. The monitoring is accomplished by exchanging CCMs as defined in ITU-T Rec. Y.1731.

In addition the MEP can be defined to perform other Y.1731 services such as measuring delay and loss on the specific EVC.

### EVC Fault Propagation

You can define fault propagation based on EVC failure detection (ETP operation status) to shut down the UNIs that connect to it. The fault trigger can be on of the following:

- In case of protection: the signal failure trigger MEP for ETP transport ports
- In other cases: the NNI operation status.

### EVC Loopback

A loopback can be activated on any of the transport ports towards the network and on the subscriber port towards the user or network.

---

**Table of Attributes**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Subscriber (UNI to ETP)</th>
<th>Subscriber (ETP to UNI)</th>
<th>Transport (NNI to ETP)</th>
<th>Transport (ETP to NNI)</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN tag (push)</td>
<td>Optional</td>
<td>Not allowed</td>
<td>Not allowed</td>
<td>For at least one of the actions, marking profile classified by CoS</td>
</tr>
<tr>
<td>Mark</td>
<td>Required, with marking profile classified by CoS</td>
<td>Required, with CoS mapping profile</td>
<td>For at least one of the actions, CoS mapping profile</td>
<td></td>
</tr>
<tr>
<td>VLAN tag (pop)</td>
<td>Not allowed</td>
<td>Optional</td>
<td>Not allowed</td>
<td>Not allowed</td>
</tr>
<tr>
<td>Drop</td>
<td>Optional</td>
<td>Optional</td>
<td>Optional</td>
<td>Optional</td>
</tr>
</tbody>
</table>
In most cases you would activate a loop on the subscriber port towards the network, thus you can loop the EVC traffic without affecting protection.

If you wish to run a loop on a specific EVC path when you activate the loop on the transport ports, you have two options:

- Loopback on a transport port affects OAM, as any traffic EVC path redundancy is triggered if present.
- Loopback only data without affecting redundancy.

### Factory Defaults

By default, no ETPs are configured.

When you create an ETP port, by default it is configured as follows:

- Name = “ETP <etp-name> Subscriber Port <port-index>” or “ETP <etp-name> Transport Port <port-index>”, according to whether port is subscriber or transport
- Administratively enabled.

When you first enter the ETP protection level, by default the protection is configured as follows:

```
ETX-203A#configure etps etp ETP1 protection
ETX-203A>config>etps>etp(ETP1)>protection$ info detail
  shutdown
  no master-etp
  mode  bi-directional-1-to-1
  no aps-protocol
  revertive
  wait-to-restore  300
```

### Configuring ETPs

This section describes how to configure ETPs.

- **To configure ETPs:**
  1. Navigate to `configure etps etp <name>` to select the ETP to configure.

     The ETP is created if it does not already exist, and the `config>etps>etp(<name>)#` prompt is displayed.

     2. Enter all necessary commands according to the tasks listed below.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring ETP port</td>
<td>`port [subscriber</td>
<td>transport] &lt;port-id&gt;`</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The port-id range is 1–2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Refer to <code>Configuring ETP Ports</code> for more information</td>
</tr>
<tr>
<td>Configuring ETP protection</td>
<td><code>protection</code></td>
<td>Refer to <code>Configuring ETP Protection</code> for more information</td>
</tr>
</tbody>
</table>
### Configuring ETP Ports

This section describes how to configure ETP ports.

▶ **To configure ETP ports:**

1. Navigate to `configure etps etp <name>` to select the ETP to configure.

   The `config>etps>etp(<name>)#` prompt is displayed.

2. Type the following command to configure a port, where `port-index` can be 1 for subscriber ports, or 1–2 for transport ports:

   ```
   port {subscriber | transport} <port-index>.
   ```

   The prompt is displayed according to whether you typed `subscriber` or `transport`:

   ```
   config>etps>etp(<name>)>port(subscriber/<port-index>)#
   config>etps>etp(<name>)>port(transport/<port-index>)#
   ```

3. Enter all necessary commands according to the tasks listed below.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Displaying ETP status</td>
<td><code>show status</code></td>
<td></td>
</tr>
<tr>
<td>Displaying ETP statistics</td>
<td><code>show statistics running</code></td>
<td></td>
</tr>
<tr>
<td>Displaying flows</td>
<td><code>show flows-summary</code></td>
<td></td>
</tr>
<tr>
<td>Clearing ETP statistics</td>
<td><code>clear-statistics</code></td>
<td></td>
</tr>
</tbody>
</table>

### Example

▶ **To configure an ETP:**

- Name = ETP1
- Port members = subscriber 1, transport 1, transport 2.
Configuring ETP Protection

To configure ETP protection, you define the working and protection ports, as well as other protection parameters.

To configure ETP protection:

1. Navigate to `configure etps etp <name> protection` to configure protection for the selected ETP.

   The `config>etps>etp(<name>)>protection#` prompt is displayed.

2. Enter all necessary commands according to the tasks listed below.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defining APS protocol for ETP</td>
<td><code>aps-protocol</code></td>
<td></td>
</tr>
<tr>
<td>Defining transport port ID for protection or working port</td>
<td>`bind {protection</td>
<td>working} {transport} {protection-port}`</td>
</tr>
<tr>
<td>Clearing the active near end lockout of Protection, Forced Switch, Manual Switch, WTR state, or Exercise command</td>
<td><code>clear</code></td>
<td></td>
</tr>
<tr>
<td>Forcing normal traffic signal to be selected from the protection transport entity, meaning jump to next port even if it is down</td>
<td><code>force-switch</code></td>
<td></td>
</tr>
<tr>
<td>Preventing a working signal from being selected from the protection transport entity, effectively disabling the protection group</td>
<td><code>lockout</code></td>
<td></td>
</tr>
<tr>
<td>Forcing normal traffic signal to be selected from the protection transport entity in the absence of failure of working or protection transport entity, meaning jump to next port only if it is not down</td>
<td><code>manual-switch</code></td>
<td></td>
</tr>
<tr>
<td>Defining master ETP</td>
<td><code>master-etp &lt;etp-name&gt;</code></td>
<td></td>
</tr>
<tr>
<td>Configuring protection mode</td>
<td><code>mode { bi-directional-1-to-1 }</code></td>
<td></td>
</tr>
</tbody>
</table>
5.24 Service Virtual Interface

A service virtual interface (SVI) is a logical port used for flows.

Note ETX-203A supports one SVI.
Configuring Service Virtual Interfaces

You can enable and operate service virtual interfaces as explained below.

To configure the SVI parameters:

1. Navigate to `configure port svi <port-num>` to select the SVI to configure.
   The `config>port>svi(<port-num>)#` prompt is displayed.
2. Enter all necessary commands according to the tasks listed below.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting the port name</td>
<td>name &lt;string&gt;</td>
<td></td>
</tr>
<tr>
<td>Administratively enabling SVI</td>
<td>no shutdown</td>
<td>Using <code>shutdown</code> disables the SVI</td>
</tr>
</tbody>
</table>

5.25 Quality of Service (QoS)

The ETX-203A Quality of Service (QoS) parameters include the following profiles:

- Queue map profiles
- CoS map profiles
- Marking profiles
- Bandwidth profiles
- Queue block profiles
- Queue group profiles.

These profiles can be applied to the traffic flows to ensure the desired flow prioritization.

Standards

The following standards are supported:

- IEEE 802.1p
- IEEE 802.1Q.

Benefits

QoS allows you to optimize bandwidth, avoiding the need to allocate excessive bandwidth to facilitate the necessary bandwidth for traffic at different requirements of speed and quality.

Factory Defaults

Refer to the following sections for each QoS type's specific defaults.
Functional Description

To differentiate traffic, the IEEE 802.1p standard specifies eight classes of service per user-defined queue map profile. These classes of service are associated with priority values between 0 and 7, using the 3-bit user priority field in an IEEE 802.1Q header added to VLAN-tagged frames within an Ethernet frame header. The way traffic is treated when assigned to a specific priority value is only generally defined and left to implementation. The general definitions are as follows:

### Table 5-11. User Priorities

<table>
<thead>
<tr>
<th>User Priority</th>
<th>Traffic Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Best effort</td>
</tr>
<tr>
<td>1</td>
<td>Background</td>
</tr>
<tr>
<td>2</td>
<td>Spare</td>
</tr>
<tr>
<td>3</td>
<td>Excellent effort</td>
</tr>
<tr>
<td>4</td>
<td>Controlled load</td>
</tr>
<tr>
<td>5</td>
<td>Video</td>
</tr>
<tr>
<td>6</td>
<td>Voice</td>
</tr>
<tr>
<td>7</td>
<td>Network control</td>
</tr>
</tbody>
</table>

Queue Mapping Profiles

Queue mapping profiles are used to convert the following user priorities into internal priority queues. ETX-203A supports up to 12 queue mapping profiles.

- **p-bit**, when the ingress traffic is prioritized according to the 802.1p requirements
- **ip-dscp**, when the ingress traffic is prioritized according to DSCP
- **ip-precedence**, when the ingress traffic is prioritized according to IP precedence
- **Class of Service (CoS)**, to queue ETP flow according to internal class of service.

For each profile, you have to define the queue mapping to map the user priority values to the internal queue values. The internal queues are combined into a queue profile, which can be assigned to a queue block.

Factory Defaults

**Default Queue Mapping Profile**

ETX-203A provides a default queue mapping profile named CosProfile1, which can be used when the ingress traffic is prioritized according to the 802.1p requirements. It is defined with classification p-bit, and the following mappings:

- Map p-bit 0 to queue 7
• Map p-bit 1 to queue 6
• Map p-bit 2 to queue 5
• Map p-bit 3 to queue 4
• Map p-bit 4 to queue 3
• Map p-bit 5 to queue 2
• Map p-bit 6 to queue 1
• Map p-bit 7 to queue 0.

**Default Configuration for IP Precedence Classification**

When a new queue mapping profile is created with classification IP precedence, it contains the following mappings:

• Map p-bit 0 to queue 7
• Map p-bit 1 to queue 6
• Map p-bit 2 to queue 5
• Map p-bit 3 to queue 4
• Map p-bit 4 to queue 3
• Map p-bit 5 to queue 2
• Map p-bit 6 to queue 1
• Map p-bit 7 to queue 0.

**Default Configuration for DSCP Classification**

When a new queue mapping profile is created with classification DSCP, it contains the following mappings:

• Map p-bit 0 to queue 7
• Map p-bit 1 to queue 6
• Map p-bit 2 to queue 5
• Map p-bit 3 to queue 4
• Map p-bit 4 to queue 3
• Map p-bit 5 to queue 2
• Map p-bit 6 to queue 1
• Map p-bit 7 through 63 to queue 0.

**Adding Queue Mapping Profiles**

When you create a queue mapping profile, you specify the name and the classification method (p-bit, IP precedence, or DSCP).

➢ **To add a queue mapping profile:**

1. Navigate to `configure qos`.
   
   The `config>qos#` prompt is displayed.
2. Type:

```
queue-map-profile <queue-map-profile-name> classification {p-bit|ip-precedence|ip-dscp|cos}.
```

A queue mapping profile with the specified name and classification method is created and the following prompt is displayed:

```
cfg>qos>queue-map-profile(<queue-map-profile-name>)$.
```

The mappings for the new profile are configured by default as described in *Factory Defaults*.

3. Configure the queue profile mappings as described in *Configuring Queue Mappings*.

### Configuring Queue Mappings

1. Navigate to `config qos queue-map-profile <queue-map-profile-name>` to select the queue mapping profile to configure.

   The following prompt is displayed:
   
   ```
cfg>qos>queue-map-profile(<queue-map-profile-name>)#.
   ```

2. Map the user priorities to queue IDs as necessary:

   - Classification p-bit or IP precedence:
     ```
     map <0-7> to-queue <0-7>
     ```
   
   - Classification DSCP:
     ```
     map <0-63> to-queue <0-7>
     ```
   
   - Classification CoS:
     ```
     map <0-7> to-queue <0-7>.
     ```

### Examples

- To create and configure a queue mapping profile named QMapPbit with classification p-bit:
  
  ```
  ETX-203A# configure qos queue-map-profile QMapPbit classification p-bit
  ETX-203A>config>qos>queue-map-profile(QMapPbit)$ map 0 to 3
  ETX-203A>config>qos>queue-map-profile(QMapPbit)$ map 4 to 2
  ETX-203A>config>qos>queue-map-profile(QMapPbit)$ map 6 to 2
  ETX-203A>config>qos>queue-map-profile(QMapPbit)$ info detail
  map  0 to-queue  3
  map  1 to-queue  6
  map  2 to-queue  5
  map  3 to-queue  4
  map  4..6 to-queue  2
  map  7 to-queue  0
  ```
To create and configure a queue mapping profile named QMapIPprec with classification IP precedence:

- Map priority 2 and 3 to queue 3.

```bash
ETX-203A# configure qos queue-map-profile QMapIPprec classif ip-precedence
ETX-203A>config>qos>queue-map-profile(QMapIPprec)$ map 2 to 3
ETX-203A>config>qos>queue-map-profile(QMapIPprec)$ map 3 to 3
ETX-203A>config>qos>queue-map-profile(QMapIPprec)$ info detail
    map 0 to-queue 7
    map 1 to-queue 6
    map 2..4 to-queue 3
    map 5 to-queue 2
    map 6 to-queue 1
    map 7 to-queue 0
```

To create and configure a queue mapping profile named QMapDSCP with classification DSCP:

- Map priority 7 to queue 6
- Map priority 55 to queue 4
- Map priority 63 to queue 5.

```bash
ETX-203A# configure qos queue-map-profile QMapDSCP classif ip-dscp
ETX-203A>config>qos>queue-map-profile(QMapDSCP)$ map 7 to 6
ETX-203A>config>qos>queue-map-profile(QMapDSCP)$ map 55 to 4
ETX-203A>config>qos>queue-map-profile(QMapDSCP)$ map 63 to 5
ETX-203A>config>qos>queue-map-profile(QMapDSCP)$ info detail
    map 0 to-queue 7
    map 1 to-queue 6
    map 2 to-queue 5
    map 3 to-queue 4
    map 4 to-queue 3
    map 5 to-queue 2
    map 6 to-queue 1
    map 7 to-queue 6
    map 8..54 to-queue 0
    map 55 to-queue 4
    map 56..62 to-queue 0
    map 63 to-queue 5
```

To create and configure a queue mapping profile named QMapCoS with classification CoS:

- Map CoS 6–7 to queue 0
- Map CoS 3–5 to queue 1
- Map CoS 0–2 to queue 2.

```bash
ETX-203A# configure qos queue-map-profile QMapCoS classification cos
ETX-203A>config>qos>queue-map-profile(QMapCoS)$ map 6-7 to-queue 0
ETX-203A>config>qos>queue-map-profile(QMapCoS)$ map 3-5 to-queue 1
ETX-203A>config>qos>queue-map-profile(QMapCoS)$ map 0-2 to-queue 2
ETX-203A>config>qos>queue-map-profile(QMapCoS)$ exit
ETX-203A>config>qos#
```
CoS Mapping Profiles

Class of Service (CoS) mapping profiles map the following user priorities to internal CoS values, for use in ETP flows.

- **p-bit**, when the ingress traffic is prioritized according to the 802.1p requirements
- **ip-dscp**, when the ingress traffic is prioritized according to DSCP
- **ip-precedence**, when the ingress traffic is prioritized according to IP precedence.

Factory Defaults

By default, there are no CoS mapping profiles. When you create a CoS mapping profile, it is configured as follows:

- Classification p-bit
- Mappings:
  - Map 0 to CoS 7
  - Map 1 to CoS 6
  - Map 2 to CoS 5
  - Map 3 to CoS 4
  - Map 4 to CoS 3
  - Map 5 to CoS 2
  - Map 6 to CoS 1
  - Map 7 to CoS 0.

Configuring CoS Mapping Profiles

- To define a CoS profile:
  1. Navigate to the qos context (`config>qos`).
  2. Define a CoS profile and assign a classification to it:

     ```
     cos-map-profile <cos-mapping-profile-name> [classification
     [p-bit | ip-precedence | ip-dscp ]]
     ```

  3. Map the user priority to a CoS value (user priority values 0–7 for p-bit and IP precedence, 0–63 for the other priority types; CoS values 0–7):

     ```
     map <0-7> to <0-7>
     map <0-63> to <0-7>.
     ```
Example

To create and configure a CoS mapping profile named my-p-bit with classification p-bit:

- Map priority 6–7 to CoS 0
- Map priority 3–5 to CoS 1
- Map priority 0–2 to CoS 2.

```
ETX-203A# configure qos cos-map-profile my-p-bit classification p-bit
ETX-203A>config>qos>cos-map-profile(my-p-bit)$ map 6..7 to-cos 0
ETX-203A>config>qos>cos-mapping-profile(my-p-bit)# map 3..5 to-cos 1
ETX-203A>config>qos>cos-mapping-profile(my-p-bit)# map 0..2 to-cos 2
ETX-203A>config>qos>cos-mapping-profile(my-p-bit)# exit
ETX-203A>config>qos#
```

Marking Profiles

Marking profiles map the P-bit, IP precedence, DSCP, or CoS classifications to the egress priority tags. The marking can also be done per color (green and/or yellow), to support color re-marking, optionally specifying the Drop Eligible Indicator (DEI) bit in the frame header. ETX-203A supports up to 12 marking profiles.

Factory Defaults

ETX-203A provides a default non color-aware marking profile named MarkingProfile1, which can be used when the ingress traffic is prioritized according to the 802.1p requirements. It is defined with classification p-bit and method p-bit, and the following markings:

- P-bit 0 => priority 0
- P-bit 1 => priority 1
- P-bit 2 => priority 2
- P-bit 3 => priority 3
- P-bit 4 => priority 4
- P-bit 5 => priority 5
- P-bit 6 => priority 6
- P-bit 7 => priority 7.

When a non color-aware marking profile is created, it has the same configuration as MarkingProfile1.

When a color-aware marking profile is created, it has the following markings for classification methods p-bit and IP precedence:

- mark 0 green to 0
- mark 1 green to 1
- mark 2 green to 2
- mark 3 green to 3
• mark 4 green to 4
• mark 5 green to 5
• mark 6 green to 6
• mark 7 green to 7
• mark 0 yellow to 0
• mark 1 yellow to 1
• mark 2 yellow to 2
• mark 3 yellow to 3
• mark 4 yellow to 4
• mark 5 yellow to 5
• mark 6 yellow to 6
• mark 7 yellow to 7.

When a color-aware marking profile is created, it has the following markings for classification method DSCP:
• mark 0 green to 0
• mark 1 green to 1
• mark 2 green to 2
• mark 3 green to 3
• mark 4 green to 4
• mark 5 green to 5
• mark 6 green to 6
• mark 7 green to 7
• mark 8..63 green to 0
• mark 0..63 yellow to 0.

**Configuring Marking Profiles**

➢ To define a non color-aware marking profile and assign a priority mark to it:

1. Navigate to the qos context (**config**>**qos**).
2. Define a marking profile and assign a classification and a method to it:

```
marking-profile <marking-profile-name>
classification {p-bit | ip-precedence | ip-dscp | cos}
method p-bit
```

3. Map the user priority to a priority marking value (user priority values 0–7 for p-bit, IP precedence, and CoS, 0–63 for DSCP; priority marking values range 0–7):

```
mark <0-7> to <0-7>
mark <0-63> to <0-7>.
```
To define a color-aware marking profile and assign a priority mark to it:

1. Navigate to the qos context (`config>qos`).

2. Define a color-aware marking profile and assign a classification and a method to it:

```plaintext
marking-profile <marking-profile-name>
    [classification {p-bit|ip-precedence|ip-dscp} [method p-bit]]
color-aware green-yellow [dei-set]
```

If you specify `dei-set`, then yellow frames transmitted from ETX-203A are marked via the Drop Eligible Indicator (DEI) bit as eligible to be dropped, and green frames transmitted from ETX-203A are marked as not eligible to be dropped. If you do not specify `dei-set`, then green and yellow frames are marked as not eligible to be dropped.

3. Map the packet color and user priority to a priority marking value (user priority values 0–7 for p-bit and IP precedence, 0–63 for DSCP; priority marking values 0–7), according to whether `dei-set` was specified for marking profile:

```plaintext
dei-set was not specified:
mark <0-7> {all|green|yellow} to <0-7>
mark <0-63> {all|green|yellow} to <0-7>
```

```plaintext
dei-set was specified:
mark <0-7> {green|yellow} to <0-7> dei {green|yellow}
mark <0-63> {green|yellow} to <0-7> dei {green|yellow}
```

**Note**

If DSCP classification is used, then only up to eight green-yellow combinations are available. A green-yellow combination consists of all the priorities that mark to a particular value for green, and to a particular value for yellow. For example, this is a combination that marks to 1 for green and 2 for yellow:

- mark 2 green to 1
- mark 2 yellow to 2
- mark 3 green to 1
- mark 3 yellow to 2
- mark 4 green to 1
- mark 4 yellow to 2
- mark 5 green to 1
- mark 5 yellow to 2

This is a combination that marks to 0 for green and for yellow, as output by info command:

- mark 0..11 green to 0
- mark 13..63 green to 0
- mark 0..19 yellow to 0
- mark 21..63 yellow to 0

**Example**

To create and configure a marking profile named Mark2:

- Color-aware
- Classification method IP precedence
• Mark 2 green to 5
• Mark 4 yellow to 7.

```
ETX-203A# configure qos
ETX-203A>config>qos# marking-profile Mark2 classification ip-precedence
color-aware green-yellow
ETX-203A>config>qos>marking-profile(Mark2)$ mark 2 green to 5
ETX-203A>config>qos>marking-profile(Mark2)$ mark 4 yellow to 7
ETX-203A>config>qos>marking-profile(Mark2)$ info detail
  mark  0  green to  0
  mark  1  green to  1
  mark  2  green to  5
  mark  3  green to  3
  mark  4  green to  4
  mark  5  green to  5
  mark  6  green to  6
  mark  7  green to  7
  mark  0  yellow to  0
  mark  1  yellow to  1
  mark  2  yellow to  2
  mark  3  yellow to  3
  mark  4  yellow to  7
  mark  5  yellow to  5
  mark  6  yellow to  6
  mark  7  yellow to  7
ETX-203A>config>qos>marking-profile(Mark2)$
```

### Bandwidth Profiles

ETX-203A supports the following bandwidth profiles:

- **Shaper profile** – Applied to queue group blocks
- **Policer profile** – Applied to flows
- **Policer aggregate** – Specifies policer profile to apply to a group of up to five traffic flows.

**Note**

*You cannot assign the same name to a shaper profile and a policer profile.*

You can control the egress bandwidth utilization by defining the committed information rate and committed burst size in shaper and policer profiles. You can also define the excessive information rate and the excessive burst size in policer profiles.

**CIR**: Defines the Committed Information Rate (CIR) for the current profile. The CIR specifies a bandwidth with committed service guarantee (“green bucket” rate).

**CBS**: Defines the Committed Burst Size (CBS) for the current profile. The CBS specifies the maximum guaranteed burst size (“green bucket” size).

**EIR**: Defines the Excess Information Rate (EIR). The EIR specifies an extra bandwidth with no service guarantee (“yellow bucket” rate).

**EBS**: Defines the Excess Burst Size (EBS). The EBS specifies the extra burst with no service guarantee (“yellow bucket” size).
Compensation: You can specify the amount of bytes that the shaper or policer can compensate for the layer 1 overhead (preamble and IFG) and the overhead for the added VLAN header in case of stacking.

Factory Defaults
ETX-203A provides default bandwidth profiles, as specified in the following table.

<table>
<thead>
<tr>
<th>Profile Type</th>
<th>Shaper</th>
<th>Policer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile Name</td>
<td>Shaper1</td>
<td>Policer1</td>
</tr>
<tr>
<td>cir</td>
<td>1,000,000</td>
<td>0</td>
</tr>
<tr>
<td>cbs</td>
<td>32,767</td>
<td>0</td>
</tr>
<tr>
<td>eir</td>
<td>–</td>
<td>1,000,000</td>
</tr>
<tr>
<td>ebs</td>
<td>–</td>
<td>32,767</td>
</tr>
<tr>
<td>compensation</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>traffic-type</td>
<td>–</td>
<td>all</td>
</tr>
</tbody>
</table>

Configuring Shaper Profiles
You can define up to 30 shaper profiles.

Adding Shaper Profiles
1. Navigate to configure qos.
   The config>qos# prompt is displayed.
2. Type:
   shaper-profile <shaper-profile-name>.
   A shaper profile with the specified name is created and the config>qos>shaper-profile(<shaper-profile-name>)$ prompt is displayed. The new shaper profile parameters (except for name) are configured by default as described in Factory Defaults.
3. Configure the shaper profile as described in Configuring Shaper Profile Parameters.

Configuring Shaper Profile Parameters
To configure shaper profiles:
1. Navigate to configure qos shaper-profile <shaper-profile-name> to select the shaper profile to configure.
   The config>qos>shaper-profile(<shaper-profile-name>)# prompt is displayed.
2. Enter all necessary commands according to the tasks listed below.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifying the CIR (kbps) and CBS (bytes)</td>
<td><code>bandwidth cir &lt;0–100000&gt; cbs &lt;0–32767&gt;</code></td>
<td>Typing <code>no bandwidth</code> removes the bandwidth limits</td>
</tr>
<tr>
<td>Note: The CIR granularity is 128 kbps. If you</td>
<td></td>
<td></td>
</tr>
<tr>
<td>specify a CIR that is not a multiple of 128</td>
<td></td>
<td></td>
</tr>
<tr>
<td>kbps, the device rounds it down, for example if</td>
<td></td>
<td></td>
</tr>
<tr>
<td>you specify 260 kbps then the device operates</td>
<td></td>
<td></td>
</tr>
<tr>
<td>as if you specified 256 kbps.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Specifying the compensation (bytes)</td>
<td><code>compensation &lt;0–63&gt;</code></td>
<td></td>
</tr>
</tbody>
</table>

**Example**

To create and configure a shaper profile named Shap2:

- CIR = 99,968 Kbps
- CBS = 32,000 bytes
- Compensation = 48.

```
ETX-203A# configure qos shaper-profile Shap2
ETX-203A>config>qos>shaper-profile(Shap2)$ bandwidth cir 99968 cbs 32000
ETX-203A>config>qos>shaper-profile(Shap2)$ compensation 48
ETX-203A>config>qos>shaper-profile(Shap2)$
```

**Configuring Policer Profiles**

You can define up to 60 policer profiles, except if at least one policer profile has total CIR + EIR greater than 133 Mbps, then no more than 16 policer profiles can be defined.

**Adding Policer Profiles**

1. Navigate to `configure qos`.
   - The `config>qos#` prompt is displayed.
2. Type `policer-profile <policer-profile-name>`.
   - A policer profile with the specified name is created and the following prompt is displayed:
     `config>qos>policer-profile(<policer-profile-name>)$`.
   - The new policer profile parameters (except for name) are configured by default as described in *Factory Defaults*.
3. Configure the policer profile as described in *Configuring Policer Profile Parameters*.

**Configuring Policer Profile Parameters**

1. Navigate to `configure qos policer-profile <policer-profile-name>` to select the policer profile to configure.
The `config>qos>policer-profile(<policer-profile-name>)#` prompt is displayed.

2. Enter all necessary commands according to the tasks listed below.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
</table>
| Specifying the CIR (kbps), CBS (bytes), EIR (kbps), and EBS (bytes) bandwidth limits | `bandwidth cir <cir-kbit-sec> cbs <cbs-bytes> eir <eir-kbit-sec> ebs <ebs-bytes>` | Typing `no bandwidth` removes the bandwidth limits  
*Notes:*  
- CIR & EIR allowed values: 0–1,000,000  
- CBS & EBS allowed values: 0, or 64–32,767 |  
1,048,575  
- CIR can be set to zero only if CBS is set to zero  
- EIR can be set to zero only if EBS is set to zero  
- CIR + EIR must not exceed the maximum available bandwidth  
- CBS should be greater than the maximum frame size. |
| Specifying the compensation (bytes) | `compensation <0–63>` |  |
| Specifying the traffic type | `traffic-type all` |  |

**Examples**

- To create and configure a policer profile named Policer4:  
  - CIR = 80,000 Kbps  
  - CBS = 28,000 bytes  
  - EIR = 90,000  
  - EBS = 20,000 bytes  
  - Compensation = 56.  

**Note**  
The EIR 90,000 is rounded by the device as shown below in the `info detail` output, due to the granularity of 512 kbps when the CIR + EIR is greater than 130 Mbps.

```
ETX-203A# configure qos policer-profile Policier4
ETX-203A>config>qos>policer-profile(Policier4)$ bandwidth cir 80000 cbs 28000 eir 90000 ebs 20000
ETX-203A>config>qos>policer-profile(Policier4)$ compensation 56
ETX-203A>config>qos>policer-profile(Policier4)$ info detail
    bandwidth cir 80000 cbs 28000 eir 89984 ebs 20000
    traffic-type all
    compensation 56
ETX-203A>config>qos>policer-profile(Policier4)$
```

- Traffic type = broadcast and multicast.
Configuring Policer Aggregates

You can define up to 30 policer aggregates that specify a policer profile to apply to a group of up to five flows. This is useful if you want to set bandwidth limits that are divided among more than one flow.

Factory Defaults

By default, no policer aggregates exist. When a policer aggregate is created, it has the following configuration:

- No assigned policer profile
- No assigned flows
- Rate sampling window (interval for sampling the associated flow statistics) set to 15 minutes.

Adding Policer Aggregates

1. Navigate to `configure qos`.
   
   The `config>qos#` prompt is displayed.

2. Type:
   ```
   policer-aggregate <policer-aggregate-name>.
   ```
   
   A policer aggregate with the specified name is created and the `config>qos>policer-aggregate(<policer-aggregate-name>)$` prompt is displayed. The new policer aggregate parameters are configured by default as described in Factory Default.

3. Configure the policer aggregate as described in Configuring Policer Aggregate Parameters.

Configuring Policer Aggregate Parameters

1. Navigate to `configure qos policer-aggregate <policer-aggregate-name>` to select the policer aggregate to configure.
   
   The following prompt is displayed:
   ```
   config>qos>policer-aggregate(<policer-aggregate-name>)#.
   ```

2. Enter all necessary commands according to the tasks listed below.

   **Note**
   
   You assign flows to the policer aggregate in the flow level (refer to Configuring Flows for details).

<table>
<thead>
<tr>
<th>Task</th>
<th>Command Description</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assigning policer profile</td>
<td><code>policer profile &lt;policer-profile-name&gt;</code></td>
<td></td>
</tr>
<tr>
<td>Specifying rate sampling window (minutes)</td>
<td><code>rate-sampling-window &lt;1–30&gt;</code></td>
<td></td>
</tr>
<tr>
<td>Displaying the associated flows</td>
<td><code>show flows</code></td>
<td></td>
</tr>
</tbody>
</table>
### Example

To create and configure a policer aggregate named Aggr1:
- Policer profile: Policer4 (created in policer profile example).

```
ETX-203A# configure qos
ETX-203A>config>qos# policer-aggregate Aggr1
ETX-203A>config>qos>policer-aggregate(Aggr1)$ policer profile Policer4
```

### Queue Block Profiles

In order to facilitate congestion management, you can sort traffic by applying queue block profiles to queue block entities. A queue block profile contains entries for queues 0–7, with the following parameters:

- **Scheduling method:**
  - Strict – High-priority queues that are always serviced first. If a lower-priority queue is being serviced and a packet enters a higher queue, that queue is serviced immediately.
  - WFQ (weighted fair queuing) – If one port does not transmit, its unused bandwidth is shared by the ‘transmitting’ queues according to the assigned weight.

In configurations with Strict and WFQ queues, the WFQ frames are transmitted only after the transmission of frames associated with the Strict queues is completed.

**Note** If one of the internal queues is configured to WFQ, queues with a higher queue ID cannot be configured to Strict.

- **Depth** (queue length), in bytes.

**Note** A queue block has 1 MB available, therefore the sum of the depths of its eight queues must be no greater than 1 MB.

### Factory Defaults

ETX-203A provides a default queue block profile named DefaultQueue1, which defines queues 0–7 as follows:

- Congestion avoidance: WRED profile corresponding to queue
- Scheduling method: WFQ, with weight set to 100
- Depth: 50,000.
Adding Queue Block Profiles
You can define up to 32 queue block profiles.

➤ To add a queue block profile:
1. Navigate to configure qos.
   The config>qos# prompt is displayed.
2. Type queue-block-profile <q-blk-profile-name>.
   A queue block profile with the specified name is created and the
   config>qos>queue-block-profile(<q-blk-profile-name>)$ prompt is
   displayed. The queues for the new profile are configured by default as
   described in Factory Defaults.
3. Configure the queue block profile as described in Configuring Queue Block
   Profile Parameters.

Configuring Queue Block Profile Parameters

➤ To configure a queue block profile:
1. Navigate to config qos queue-block-profile <q-blk-profile-name> to select the
   queue block profile to configure.
   The config>qos>queue-block-profile(<q-blk-profile-name>)# prompt is
   displayed.
2. Perform the following for each queue that you wish to configure:
   a. To configure a queue, enter:
      queue <q-ID>.
      The following prompt is displayed:
      config>qos>queue-block-profile(<q-blk-profile-name>)>queue(<q-ID>)#.
   b. Enter all necessary commands according to the tasks listed below.
   c. Type exit to return to the queue block profile context.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting scheduling method</td>
<td>scheduling [ strict</td>
<td>wfq &lt;weight&gt;]</td>
</tr>
<tr>
<td>Specifying queue depth</td>
<td>depth &lt;value&gt;</td>
<td>Allowed range: 0–1048576</td>
</tr>
</tbody>
</table>

Example

➤ To create and configure a queue block profile named QBlockProf1:
- Queue 0 set to strict scheduling and depth 500,000
- Queue 1 set to strict scheduling and depth 200,000
- Queue 7 set to WFQ scheduling with weight 75.
Queue Group Profiles

In order to facilitate congestion management, you can sort traffic by applying one queue group profile per network or user port. You can define up to eight queue group profiles per ETX-203A unit.

Adding Queue Group Profiles

To add a queue group profile:

1. Navigate to `configure qos`.
   
   The `config>qos#` prompt is displayed.

2. Type:
   
   `queue-group-profile <q-grp-profile-name>`.

   A queue group profile with the specified name is created and the `config>qos>queue-group-profile(<q-grp-profile-name>)$` prompt is displayed.

3. Configure the queue group profile as described in `Configuring Queue Group`.

Configuring Queue Group Parameters

To configure a queue group profile:

1. Navigate to `config qos queue-group-profile <q-grp-profile-name>` to select the queue group profile to configure.

   The `config>qos>queue-group-profile(<q-grp-profile-name>)#` prompt is displayed.

2. Select a queue block in level 0 or 1 to configure:

   `queue-block 0/1–31`
   `queue-block 1/1`

   The following prompt is displayed:

   `config>qos>queue-group-profile(<q-grp-profile-name>)>queue-block(<level/ID>)#`. 

---

ETX-203A# configure qos queue-block-profile QBlockProf1
ETX-203A(config)>qos>queue-block-profile(QBlockProf1)$ queue 0
ETX-203A(config)>qos>queue-block-profile(QBlockProf1)>queue(0)$ scheduling strict
ETX-203A(config)>qos>queue-block-profile(QBlockProf1)>queue(0)$ depth 500000
ETX-203A(config)>qos>queue-block-profile(QBlockProf1)>queue(0)$ exit
ETX-203A(config)>qos>queue-block-profile(QBlockProf1)$ queue 1
ETX-203A(config)>qos>queue-block-profile(QBlockProf1)>queue(1)$ scheduling strict
ETX-203A(config)>qos>queue-block-profile(QBlockProf1)>queue(1)$ depth 200000
ETX-203A(config)>qos>queue-block-profile(QBlockProf1)>queue(1)$ exit
ETX-203A(config)>qos>queue-block-profile(QBlockProf1)$ queue 7
ETX-203A(config)>qos>queue-block-profile(QBlockProf1)>queue(7)$ scheduling wfq 75
ETX-203A(config)>qos>queue-block-profile(QBlockProf1)>queue(7)#
3. Enter all necessary commands according to the tasks listed below.
4. If you wish to configure another queue block, type `exit` to return to the queue group profile context, and start again at step 2.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assigning a name to the queue block</td>
<td><code>name &lt;block-name&gt;</code></td>
<td></td>
</tr>
<tr>
<td>Assigning a queue block profile</td>
<td><code>profile &lt;queue-block-profile-name&gt;</code></td>
<td></td>
</tr>
<tr>
<td>Assigning a shaper profile</td>
<td><code>shaper profile &lt;shaper-profile-name&gt;</code></td>
<td>Only for queue blocks in level 0</td>
</tr>
</tbody>
</table>

**Note**

Normally there is no need for you to enter the bind command. When you add a queue block in level 0 to the profile, bind is done automatically. You cannot use the bind command if the queue group contains a single queue block in level 0.

**Example**

**Note**

This example uses the shaper profile and queue block profile created in the examples in the preceding sections.

➢ To create and configure a queue group profile named QGroupProf1:
   - Queue block 0/1:
     - Queue block profile: QBlockProf1
     - Shaper profile: Shap2.

**Note**

Queue blocks 1/1 and 0/2 are automatically created.
ETX-203A# configure qos queue-group-profile QGroupProf1
ETX-203A>config>qos>queue-group-profile(QGroupProf1)$ queue-block 0/1
ETX-203A>config>qos>queue-group-profile(QGroupProf1)>queue-block(0/1)$ profile QBlockProf1
ETX-203A>config>qos>queue-group-profile(QGroupProf1)>queue-block(0/1)$ shaper profile Shap2
ETX-203A>config>qos>queue-group-profile(QGroupProf1)>queue-block(0/1)$ exit
ETX-203A>config>qos>queue-group-profile(QGroupProf1)$ info detail
  queue-block  1/1
    name  "Level1QueueBlock"
    profile "Scheduling2"
  exit
  queue-block  0/1
    name  "Put your string here"
    profile "QBlockProf1"
    bind queue  0 queue-block  1/1
    shaper profile "Shap2"
  exit
  queue-block  0/2
    name  "Put your string here"
    profile "DefaultQueue1"
    bind queue  1 queue-block  1/1
    shaper profile "Shaper1"
  exit

WRED Profiles

The WRED mechanism defines the probability of dropping yellow packets depending on the current queue usage. This avoids traffic congestion and ensures the forwarding of green packets. You can configure the following:

- Minimum threshold – Defines the queue usage at which the WRED mechanism starts to drop yellow packets
- Maximum threshold – Defines the queue usage above which the WRED mechanism drops all yellow packets
- Probability – Determines the percentage of packets to be dropped when the queue usage reaches the maximum threshold

There are eight WRED profiles available, named WREDProfile0 through WREDProfile7. They are bound to the queues automatically: WREDProfile0 is bound to queue 0, WREDProfile1 is bound to queue 1, etc. You cannot delete the WRED profiles, and you cannot add more WRED profiles. The binding of the profiles to the queues is set and cannot be changed, but you can change the profile parameters. You can view the assignment of WRED profiles to queues via the info command in the queue block profile level.

Note

The WRED mechanism is activated only when you use a policer profile with EIR set to a nonzero value.

Factory Defaults

There are eight WRED profiles available, named WREDProfile0 through WREDProfile7, bound to the corresponding queues.
Configuring WRED Profiles

To configure WRED profiles:

1. Navigate to `configure qos` and type `wred-profile WREDProfile<n>` where `n` is 0 through 7.

   The `config>qos>wred-profile(WREDProfile<n>)#` prompt is displayed.

2. Enter:
   ```
   color yellow min <min-threshold> max <max-threshold> [probability <max-probability>].
   ```
   - `min-threshold` – Queue usage minimum threshold in percentage, 0–100
   - `max-threshold` – Queue usage maximum threshold in percentage, 0–100
   - `max-probability` – Percentage of packets to be dropped when the queue usage reaches the maximum limit.

   **Note**
   
   You can configure the parameters for the color yellow only.

Example

To configure WRED profile 4:

- Minimum threshold 64
- Maximum threshold 100
- Probability 50.

```bash
ETX-203A# configure qos wred-profile WREDProfile4
ETX-203A>config>qos>wred-profile(WREDProfile4)# color yellow min 64 max 100 probability 50
ETX-203A>config>qos>wred-profile(WREDProfile4)# info detail
   color yellow min 64 max 100 probability 50
ETX-203A>config>qos>wred-profile(WREDProfile4)#
```

5.26 Flows

ETX-203A supports up to 192 unidirectional Ethernet flows, which can be used to provide E-line or E-LAN service delivery over Metro Ethernet networks. Each Ethernet flow is unidirectional and connects two ports.

This section explains how to define the flows according to specific criteria such as VLAN. You can use classifier profiles to specify the criteria for flows. The classification is per port and is applied to the ingress port of the flow.

Standards

IEEE 802.3x
Benefits

The user traffic can be classified into different Ethernet flows (EVC.CoS) to provide services in a flexible manner.

Functional Description

Packets can be classified by means of their VLAN IDs and other criteria, fully specified in Defining Classifier Profiles.

Classifications that apply to the same port are allowed in the combinations shown in Table 5-13. The priority shown is used to determine which classification is used if incoming packets for the port fit the criteria of more than one classification. Priority 4 is the lowest, priority 1 is the highest. NNI indicates ingress network port, UNI indicates ingress user port.

You can perform marking and tagging actions on the outer and inner VLAN such as adding, replacing, or removing, as well as marking with p-bit. Only certain combinations of actions on the outer and inner VLAN are allowed. If no action is performed for the outer VLAN, then for the inner VLAN there must be no action performed. Table 5-14 shows valid action combinations on ingress frame tags and the resulting egress frame tags and p-bits, according to whether the ingress frame is untagged, contains one VLAN, or is double-tagged. Any combination not shown in the table is not supported.

In the descriptions, VLAN refers to the service provider (outer) VLAN, previously referred to as SP-VLAN, while inner VLAN refers to the Customer Entity VLAN, previously referred to as CE-VLAN.

Table 5-13. Classification Combinations

<table>
<thead>
<tr>
<th>Classification</th>
<th>Other classifications allowed on same ingress port</th>
<th>Range</th>
<th>Max number ranges</th>
<th>Priority</th>
<th>NNI/UNI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unclassified (all-to-one bundling)</td>
<td>VLAN</td>
<td>–</td>
<td>1</td>
<td>4</td>
<td>Both</td>
</tr>
<tr>
<td></td>
<td>VLAN + IP precedence</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>VLAN + DSCP</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>VLAN + VLAN priority</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>VLAN + Non-IP</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>VLAN priority</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IP precedence</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>DSCP</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Source MAC address</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Destination MAC address</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Source IP address</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Destination IP address</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Non-IP</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ethertype</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Untagged</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Classification</td>
<td>Other classifications allowed on same ingress port</td>
<td>Range</td>
<td>Max number ranges</td>
<td>Priority</td>
<td>NNI/UNI</td>
</tr>
<tr>
<td>----------------</td>
<td>---------------------------------------------------</td>
<td>-------</td>
<td>-------------------</td>
<td>----------</td>
<td>--------</td>
</tr>
<tr>
<td>VLAN</td>
<td>VLAN + VLAN priority VLAN + IP precedence VLAN + DSCP VLAN + destination MAC address VLAN + source IP address VLAN + destination IP address VLAN + inner VLAN VLAN + VLAN priority + inner VLAN VLAN + Ethertype Source MAC address Destination MAC address Source IP address Destination IP address Ethertype Unclassified Untagged</td>
<td>0–4094</td>
<td>10</td>
<td>3</td>
<td>Both</td>
</tr>
<tr>
<td>VLAN + VLAN priority</td>
<td>VLAN VLAN + source MAC address VLAN + destination MAC address VLAN + source IP address VLAN + destination IP address VLAN + inner VLAN VLAN + Ethertype Source MAC address Destination MAC address Source IP address Destination IP address Unclassified Ethertype Untagged</td>
<td>0–4094 + 0–7</td>
<td>10</td>
<td>2</td>
<td>Both</td>
</tr>
<tr>
<td>VLAN + IP precedence</td>
<td>VLAN Source MAC address Destination MAC address Source IP address Destination IP address Unclassified Ethertype Non-IP Untagged</td>
<td>0–4094 + 0–7</td>
<td>10</td>
<td>2</td>
<td>Both</td>
</tr>
<tr>
<td>Classification</td>
<td>Other classifications allowed on same ingress port</td>
<td>Range</td>
<td>Max number ranges</td>
<td>Priority</td>
<td>NNI/UNI</td>
</tr>
<tr>
<td>-------------------------</td>
<td>----------------------------------------------------</td>
<td>------------------</td>
<td>-------------------</td>
<td>----------</td>
<td>---------</td>
</tr>
<tr>
<td>VLAN + DSCP</td>
<td>VLAN, Source MAC address, Destination MAC address, Source IP address, Destination IP address, Unclassified, Ethertype, Non-IP, Untagged</td>
<td>0–4094 + 0–63</td>
<td>10</td>
<td>2</td>
<td>Both</td>
</tr>
<tr>
<td>VLAN + source MAC address</td>
<td>VLAN, VLAN + VLAN priority, VLAN + inner VLAN, VLAN + VLAN priority + inner VLAN</td>
<td>0–4094 + MAC address</td>
<td>One VLAN value + one MAC address range</td>
<td>2</td>
<td>Both</td>
</tr>
<tr>
<td>VLAN + destination MAC address</td>
<td>VLAN, VLAN + VLAN priority, VLAN + inner VLAN, VLAN + VLAN priority + inner VLAN</td>
<td>0–4094 + MAC address</td>
<td>One VLAN value + one MAC address range</td>
<td>2</td>
<td>Both</td>
</tr>
<tr>
<td>VLAN + source IP address</td>
<td>VLAN, VLAN + VLAN priority, VLAN + inner VLAN, VLAN + inner VLAN + VLAN priority</td>
<td>0–4094 + IP address</td>
<td>One VLAN value + one IP address range</td>
<td>2</td>
<td>Both</td>
</tr>
<tr>
<td>VLAN + destination IP address</td>
<td>VLAN, VLAN + VLAN priority, VLAN + inner VLAN, VLAN + inner VLAN + VLAN priority</td>
<td>0–4094 + IP address</td>
<td>One VLAN value + one IP address range</td>
<td>2</td>
<td>Both</td>
</tr>
<tr>
<td>VLAN + inner VLAN</td>
<td>VLAN, VLAN + VLAN priority, VLAN + inner VLAN, VLAN + source MAC address, VLAN + destination MAC address, VLAN + source IP address, VLAN + destination IP address, VLAN + Ethertype</td>
<td>Single value for VLAN and range for inner VLAN</td>
<td>10 (for inner range)</td>
<td>3</td>
<td>Both</td>
</tr>
<tr>
<td>VLAN + VLAN priority + inner VLAN</td>
<td>VLAN, VLAN + inner VLAN, VLAN + source MAC address, VLAN + destination MAC address, VLAN + source IP address, VLAN + destination IP address, VLAN + Ethertype</td>
<td>Single value for VLAN and range for inner VLAN</td>
<td>10 (for inner range)</td>
<td>3</td>
<td>Both</td>
</tr>
<tr>
<td>Classification</td>
<td>Other classifications allowed on same ingress port</td>
<td>Range</td>
<td>Max number ranges</td>
<td>Priority</td>
<td>NNI/UNI</td>
</tr>
<tr>
<td>-----------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------</td>
<td>-------</td>
<td>-------------------</td>
<td>----------</td>
<td>---------</td>
</tr>
<tr>
<td>VLAN + non-IP</td>
<td>VLAN, VLAN + IP precedence, VLAN + DSCP, Source MAC address, Destination MAC address, Source IP address, Destination IP address, Ethertype, Untagged</td>
<td>0–4094</td>
<td>10</td>
<td>1</td>
<td>Both</td>
</tr>
<tr>
<td>VLAN + Ethertype</td>
<td>VLAN, VLAN + VLAN priority, VLAN + inner VLAN, VLAN + inner VLAN + VLAN priority, Ethertype value with one VLAN value</td>
<td>Ethertype 0–4094</td>
<td>One Ethertype value</td>
<td>2</td>
<td>Both</td>
</tr>
<tr>
<td>VLAN priority</td>
<td>Unclassified, Source MAC address, Destination MAC address, Source IP address, Destination IP address, Ethertype, Untagged</td>
<td>0–7</td>
<td>5</td>
<td>2</td>
<td>Both</td>
</tr>
<tr>
<td>IP precedence</td>
<td>Unclassified, Source MAC address, Destination MAC address, Source IP address, Destination IP address, Non-IP, Ethertype</td>
<td>0–7</td>
<td>5</td>
<td>2</td>
<td>Both</td>
</tr>
<tr>
<td>DSCP</td>
<td>Unclassified, Source MAC address, Destination MAC address, Source IP address, Destination IP address, Non-IP, Ethertype</td>
<td>0–63</td>
<td>5</td>
<td>2</td>
<td>Both</td>
</tr>
<tr>
<td>Source MAC address</td>
<td>VLAN, VLAN priority, VLAN + VLAN priority, VLAN + IP precedence, VLAN + DSCP, VLAN + DSCP, VLAN + Non-IP, IP precedence, DSCP, Unclassified, Non-IP, Untagged</td>
<td>MAC address 1</td>
<td>1</td>
<td>1</td>
<td>Both</td>
</tr>
<tr>
<td>Classification</td>
<td>Other classifications allowed on same ingress port</td>
<td>Range</td>
<td>Max number ranges</td>
<td>Priority</td>
<td>NNI/UNI</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------</td>
<td>-------</td>
<td>-------------------</td>
<td>----------</td>
<td>---------</td>
</tr>
<tr>
<td>Destination MAC address</td>
<td>VLAN, VLAN priority, VLAN + VLAN priority, VLAN + IP precedence, VLAN + DSCP, VLAN + Non-IP, IP precedence, DSCP, Unclassified, Non-IP, Untagged</td>
<td>MAC address</td>
<td>1</td>
<td>1</td>
<td>Both</td>
</tr>
<tr>
<td>Source IP address</td>
<td>VLAN, VLAN priority, VLAN + VLAN priority, VLAN + IP precedence, VLAN + DSCP, VLAN + Non-IP, IP precedence, DSCP, Unclassified, Non-IP, Untagged</td>
<td>IP address</td>
<td>1</td>
<td>1</td>
<td>Both</td>
</tr>
<tr>
<td>Destination IP address</td>
<td>VLAN, VLAN priority, VLAN + VLAN priority, VLAN + IP precedence, VLAN + DSCP, VLAN + Non-IP, IP precedence, DSCP, Unclassified, Non-IP, Untagged</td>
<td>IP address</td>
<td>1</td>
<td>1</td>
<td>Both</td>
</tr>
<tr>
<td>Non-IP</td>
<td>Unclassified, VLAN + IP precedence, VLAN + DSCP, Source MAC address, Destination MAC address, Source IP address, Destination IP address, Ethertype</td>
<td>-</td>
<td>1</td>
<td>1</td>
<td>Both</td>
</tr>
<tr>
<td>Classification</td>
<td>Other classifications allowed on same ingress port</td>
<td>Range</td>
<td>Max number ranges</td>
<td>Priority</td>
<td>NNI/UNI</td>
</tr>
<tr>
<td>----------------</td>
<td>---------------------------------------------------</td>
<td>-------</td>
<td>-------------------</td>
<td>----------</td>
<td>---------</td>
</tr>
<tr>
<td>Ethertype</td>
<td>Unclassified</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>Both</td>
</tr>
<tr>
<td></td>
<td>VLAN</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>VLAN priority</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>VLAN + VLAN priority</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>VLAN + IP precedence</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>VLAN + DSCP</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>VLAN + non-IP</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IP precedence</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>DSCP</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Non-IP</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Untagged</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>Both</td>
</tr>
<tr>
<td></td>
<td>Unclassified</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>VLAN</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>VLAN priority</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>VLAN + VLAN priority</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>VLAN + DSCP</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Source MAC address</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Destination MAC address</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Source IP address</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Destination IP address</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ethertype</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note 1**

*If you combine the classifications VLAN and VLAN + VLAN priority, the VLANs must be different.*

*For example, the following combination is not allowed:*

- VLAN 100
- VLAN 100 + p-bit 5.

*The following combination is allowed:*

- VLAN 100
- VLAN 200 + p-bit 5.

*You can achieve the combination VLAN 100 and VLAN 100 + p-bit 5 via the following:*

- VLAN 100 + p-bit 0–4, 6–7
- VLAN 100 + p-bit 5.
**Note 2** If you apply two classification profiles with IP address ranges to a port, the profiles must have the same mask.

For example:
The following is valid (mask1 equal to mask2):
Classification #1: 10.10.0.0 –10.10.0.255 - › mask1=255.255.255.0
Classification #2: 20.20.0.0 –20.20.0.255 - › mask2=255.255.255.0

The following is invalid (mask1 not equal to mask2):
Classification #1: 10.10.0.0–0.10.0.255 - › mask1=255.255.255.0
Classification #2: 20.20.0.0 –20.20.255.255 - › mask2=255.255.0.0

### Table 5-14. Valid VLAN Action Combinations

<table>
<thead>
<tr>
<th>Action on:</th>
<th>Egress VLAN(s) and P-bit(s) for Ingress Frame Types:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outer VLAN</td>
<td>Inner VLAN</td>
</tr>
<tr>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Pop</td>
<td>None</td>
</tr>
<tr>
<td>Pop</td>
<td>Mark with VLAN A</td>
</tr>
<tr>
<td>Pop</td>
<td>Pop</td>
</tr>
<tr>
<td>Push VLAN A</td>
<td>None</td>
</tr>
<tr>
<td>Push VLAN A</td>
<td>Mark with VLAN B</td>
</tr>
<tr>
<td>Push VLAN A</td>
<td>Mark with p-bit D</td>
</tr>
<tr>
<td>Push VLAN A</td>
<td>Mark with profile F</td>
</tr>
<tr>
<td>Push VLAN A, mark with profile E</td>
<td>Push VLAN B, mark with p-bit D</td>
</tr>
</tbody>
</table>
### Action on: Egress VLAN(s) and P-bit(s) for Ingress Frame Types:

<table>
<thead>
<tr>
<th>Action on:</th>
<th>Outer VLAN</th>
<th>Inner VLAN</th>
<th>Untagged</th>
<th>One VLAN (X)</th>
<th>Double VLANs (X and Y)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Push VLAN A. mark with profile E</td>
<td>Push VLAN B. mark with profile F</td>
<td>A + p-bit 7 according to E, B + p-bit 7 according to F</td>
<td>A + p-bit according to E, B + p-bit according to F, X</td>
<td>A + p-bit according to E, B + p-bit according to F, X, Y</td>
<td></td>
</tr>
</tbody>
</table>

*Note 1: When an inner marking profile is used, it is applied to the outer p-bits.*

### Factory Defaults

By default, no flows exist.

### Defining Classifier Profiles

You can define up to 64 classifier profiles to apply to flows to ensure the desired flow classification.

**To define a classifier profile:**

1. Navigate to the flows context (config>flows).
2. Define a classifier profile and assign a name to it:

   ```
   classifier-profile <profile-name> match-any
   ```

   The system switches to the context of the classifier profile (`config>flows<classifier-profile>`).
3. Specify the criteria for the classifier profile:

   ```
   [no] match [ vlan <X>.<Y> ] [ inner-vlan <X>.<Y> ]
   [ p-bit <X>.<Y> ] [ inner-p-bit <X>.<Y> ]
   ```
4. When you have completed specifying the criteria, enter `exit` to exit the classifier profile context.

Examples

➤ To create classifier profile with criteria VLAN 100 to VLAN 150:

```
ETX-203A# configure flows classifier-profile v100_150 match-any
ETX-203A>config>flows>classifier-profile(v100_150)$ match vlan 100..150
ETX-203A>config>flows>classifier-profile(v100_150)$ exit all
ETX-203A#
```

➤ To create classifier profile with criteria VLAN 20 and inner VLAN 30:

```
ETX-203A# configure flows classifier-profile v20_inner_30 match-any
ETX-203A>config>flows>classifier-profile(v20_inner_30)$ match vlan 20 inner-vlan 30
ETX-203A>config>flows>classifier-profile(v20_inner_30)$ exit all
ETX-203A#
```

➤ To create classifier profile that matches all criteria:

```
ETX-203A# configure flows classifier-profile all match-any
ETX-203A>config>flows>classifier-profile(all)$ match all
ETX-203A>config>flows>classifier-profile(all)$ exit all
ETX-203A#
```

➤ To create classifier profile with criteria Ethertype 0x8100:

```
ETX-203A# configure flows classifier-profile e8100 match-any
ETX-203A>config>flows>classifier-profile(e8100)$ match ether-type 0x8100
ETX-203A>config>flows>classifier-profile(e8100)$ exit all
ETX-203A#
```

Configuring Flows

➤ To configure flows:

1. Navigate to `config>flows`.

2. Enter `flow <flow-name>`.

   If the flow already exists, the `config>flows>flow(<flow-name>)#` prompt is displayed, otherwise the flow is created and the `config>flows>flow(<flow-name>)$` prompt is displayed.

3. Enter all necessary commands according to the tasks listed below.
### Installation and Operation Manual

**Chapter 5  Configuration**

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Associating the flow with a classifier profile</td>
<td>classifier (&lt;)classifier-profile-name&gt;</td>
<td>Up to three flows can be associated with one classifier profile</td>
</tr>
<tr>
<td>Specifying the ingress port</td>
<td><strong>ingress-port host</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>ingress-port ethernet</strong> (&lt;)port&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>ingress-port etp</strong> (&lt;)etp-name) ([)subscriber</td>
<td>transport] (&lt;)port-number&gt;</td>
</tr>
<tr>
<td></td>
<td><strong>ingress-port logical-mac</strong> (&lt;)port&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>ingress-port svi</strong> (&lt;)port&gt;</td>
<td></td>
</tr>
<tr>
<td>Specifying the egress port, and defining its queues</td>
<td><strong>egress-port host</strong> ([)queue (&lt;)queue-id&gt;])</td>
<td>If a queue mapping profile is used, it must be compatible with the classification criteria of the flow, e.g. if the classification is according to DSCP then the queue mapping should not be according to p-bit.</td>
</tr>
<tr>
<td></td>
<td><strong>egress-port host</strong> ([)queue-map-profile (&lt;)queue-map-profile-name&gt;])</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>egress-port ethernet</strong> (&lt;)port) ([)queue (&lt;)queue-id&gt;] (block (&lt;)level_id)/queue_id&gt;)</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>egress-port etp</strong> (&lt;)etp-name) ([)subscriber</td>
<td>transport] (&lt;)port-number) ([)cos (&lt;)cos-id&gt;])</td>
</tr>
<tr>
<td></td>
<td><strong>egress-port etp</strong> (&lt;)etp-name) ([)subscriber</td>
<td>transport] (&lt;)port-number) ([)cos-map-profile (&lt;)cos-map-profile-name&gt;])</td>
</tr>
<tr>
<td></td>
<td><strong>egress-port logical-mac</strong> (&lt;)port) ([)queue (&lt;)queue-id&gt;] (block (&lt;)level_id)/queue_id&gt;)</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>egress-port logical-mac</strong> (&lt;)port) ([)queue-map-profile (&lt;)queue-map-profile-name&gt;] (block (&lt;)level_id)/queue_id&gt;)</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>egress-port svi</strong> (&lt;)port&gt;</td>
<td></td>
</tr>
<tr>
<td>Associating the flow with a policer profile or policer aggregate</td>
<td><strong>policer profile</strong> (&lt;)policer-profile-name&gt;</td>
<td>Up to five flows can be associated with one policer aggregate</td>
</tr>
<tr>
<td></td>
<td><strong>policer aggregate</strong> (&lt;)policer-aggregate-name&gt;</td>
<td></td>
</tr>
<tr>
<td>Associating a Layer-2 control processing profile with the flow</td>
<td><strong>l2cp profile</strong> (&lt;)l2cp-profile-name&gt;</td>
<td>L2CP profile can be attached only to flows with the following classification types:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• VLAN/VLAN+P-bit</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Outer+Inner VLAN / Outer +P-bit + Inner VLAN</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• P-bits</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• VLAN+Non IP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Untagged.</td>
</tr>
<tr>
<td>Defining marking actions for the flow such as overwriting the VLAN ID or inner VLAN ID or setting the priority</td>
<td><strong>mark all</strong></td>
<td>Refer to the following table for the marking actions</td>
</tr>
<tr>
<td>Task</td>
<td>Command</td>
<td>Comments</td>
</tr>
<tr>
<td>---------------------------------------------------------------------</td>
<td>----------------------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>Adding VLAN ID with p-bit set to specific value, and optionally adding inner VLAN ID with p-bit set to specific value</td>
<td><code>vlan-tag push vlan &lt;sp-vlan&gt; p-bit fixed &lt;fixed-p-bit&gt;</code> [<code>inner-vlan &lt;inner-sp-vlan&gt;</code> <code>p-bit fixed &lt;inner-fixed-p-bit&gt;</code>]</td>
<td></td>
</tr>
<tr>
<td>Adding VLAN ID with p-bit set to specific value, and optionally adding inner VLAN ID with p-bit set via marking profile</td>
<td><code>vlan-tag push vlan &lt;sp-vlan&gt; p-bit fixed &lt;fixed-p-bit&gt;</code> [<code>inner-vlan &lt;inner-sp-vlan&gt;</code> <code>p-bit profile &lt;inner-marking-profile-name&gt;</code>]</td>
<td></td>
</tr>
<tr>
<td>Adding VLAN ID with p-bit set to specific value, and optionally adding inner VLAN ID with p-bit set by copying from the incoming frame</td>
<td><code>vlan-tag push vlan &lt;sp-vlan&gt; p-bit fixed &lt;fixed-p-bit&gt;</code> [<code>inner-vlan &lt;inner-sp-vlan&gt;</code> <code>p-bit copy</code>]</td>
<td></td>
</tr>
<tr>
<td>Adding VLAN ID with p-bit set via marking profile, and optionally adding inner VLAN ID with p-bit set to specific value</td>
<td><code>vlan-tag push vlan &lt;sp-vlan&gt; p-bit profile &lt;marking-profile-name&gt;</code> [<code>inner-vlan &lt;inner-sp-vlan&gt;</code> <code>p-bit fixed &lt;inner-fixed-p-bit&gt;</code>]</td>
<td></td>
</tr>
<tr>
<td>Adding VLAN ID with p-bit set via marking profile, and optionally adding inner VLAN ID with p-bit set via marking profile</td>
<td><code>vlan-tag push vlan &lt;sp-vlan&gt; p-bit profile &lt;marking-profile-name&gt;</code> [<code>inner-vlan &lt;inner-sp-vlan&gt;</code> <code>p-bit profile &lt;inner-marking-profile-name&gt;</code>]</td>
<td></td>
</tr>
<tr>
<td>Adding VLAN ID with p-bit set via marking profile, and optionally adding inner VLAN ID with p-bit set by copying from the incoming frame</td>
<td><code>vlan-tag push vlan &lt;sp-vlan&gt; p-bit profile &lt;marking-profile-name&gt;</code> [<code>inner-vlan &lt;inner-sp-vlan&gt;</code> <code>p-bit copy</code>]</td>
<td></td>
</tr>
<tr>
<td>Adding VLAN ID with p-bit set by copying from the incoming frame, and optionally adding inner VLAN ID with p-bit set to specific value:</td>
<td><code>vlan-tag push vlan &lt;sp-vlan&gt; p-bit copy</code> [<code>inner-vlan &lt;inner-sp-vlan&gt;</code> <code>p-bit fixed &lt;inner-fixed-p-bit&gt;</code>]</td>
<td></td>
</tr>
<tr>
<td>Adding VLAN ID with p-bit set by copying from the incoming frame, and optionally adding inner VLAN ID with p-bit set via marking profile</td>
<td><code>vlan-tag push vlan &lt;sp-vlan&gt; p-bit copy</code> [<code>inner-vlan &lt;inner-sp-vlan&gt;</code> <code>p-bit profile &lt;inner-marking-profile-name&gt;</code>]</td>
<td></td>
</tr>
<tr>
<td>Adding VLAN ID with p-bit set by copying from the incoming frame, and optionally adding inner VLAN ID with p-bit set by copying from the incoming frame</td>
<td><code>vlan-tag push vlan &lt;sp-vlan&gt; p-bit copy</code> [<code>inner-vlan &lt;inner-sp-vlan&gt;</code> <code>p-bit copy</code>]</td>
<td></td>
</tr>
<tr>
<td>Removing VLAN ID, and optionally removing inner VLAN ID</td>
<td><code>vlan-tag pop vlan</code> [<code>inner-vlan</code>]</td>
<td></td>
</tr>
<tr>
<td>Removing pushing of inner VLAN</td>
<td><code>no vlan-tag</code> [<code>push inner-vlan</code>]</td>
<td></td>
</tr>
<tr>
<td>Discarding traffic transmitted via the flow</td>
<td><code>drop</code></td>
<td></td>
</tr>
</tbody>
</table>
### Installation and Operation Manual

#### Chapter 5  Configuration

---

**Administratively enabling the flow**

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
</table>
| Administratively enabling the flow | no shutdown | - You can activate a flow only if it is associated with at least a classifier profile, ingress port, and egress port  
- Flows are created as inactive by default  
- Type `shutdown` to disable the flow |

---

The following marking actions can be performed in the **mark** level, at the `config>flows>flow(<flow-name>)>mark#` prompt.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overwriting VLAN ID with a new value</td>
<td><code>vlan &lt;vlan-value&gt;</code></td>
<td>Typing <code>no vlan</code> removes the overwriting of VLAN ID</td>
</tr>
<tr>
<td>Overwriting inner VLAN ID with a new value</td>
<td><code>inner-vlan &lt;inner-vlan-value&gt;</code></td>
<td>Typing <code>no inner-vlan</code> removes the overwriting of inner VLAN ID</td>
</tr>
<tr>
<td>Overwriting p-bit with a new value</td>
<td><code>p-bit &lt;p-bit-value&gt;</code></td>
<td>Typing <code>no p-bit</code> removes the overwriting of p-bit</td>
</tr>
<tr>
<td>Overwriting inner p-bit with a new value</td>
<td><code>inner-p-bit &lt;inner-p-bit-value&gt;</code></td>
<td>Typing <code>no inner-p-bit</code> removes the overwriting of inner p-bit</td>
</tr>
</tbody>
</table>
| Overwriting p-bit according to marking profile | `marking-profile <marking-profile-name>` | If a marking profile is used, it must be compatible with the classification criteria of the flow, e.g. if the flow classification is according to DSCP then the marking classification should not be according to p bit  
If a color-aware marking profile is applied for the outer VLAN of a flow, then if marking is applied to the inner VLAN, either the same color-aware marking profile must be used for the inner VLAN, or a non-color-aware marking profile must be used for the inner VLAN.  
Typing `no marking-profile` or `no inner-marking-profile` removes the overwriting of marking profile or inner marking profile respectively |
| Overwriting inner p-bit according to marking profile | `inner-marking-profile <inner-marking-profile-name>` | |

---

Exiting the marking context and returning to the flow context | exit | |

---

ETX-203A Ver. 3.0 Flows 5-117
Examples

Traffic Flows

This section provides an example of configuring the following flows:

- **Outgoing traffic from user port ETH 3 to network port ETH 1:**
  - Accept only traffic tagged with VLAN 10
  - Add VLAN 100 with p-bit 5 (this causes VLAN 100 to be the outer VLAN and VLAN 10 to be the inner VLAN).

- **Incoming traffic from network port ETH 1 to user port ETH 3:**
  - Accept only traffic tagged with VLAN 100 and inner VLAN 10
  - Remove the outer VLAN (VLAN 100).

➤ To configure the outgoing flow:

1. Set up a classifier profile to forward frames from VLAN 10:

   ```
   ETX-203A# configure flows
   ETX-203A>config>flows# classifier-profile v10 match-any
   ETX-203A>config>flows>classifier-profile(v10)$ match vlan 10
   ETX-203A>config>flows>classifier-profile(v10)$ exit all
   ETX-203A#
   ```

2. Set up a flow using the previously defined classifier profile, with ingress at ETH 3 and egress at ETH 1, and pushing VLAN 100 with p-bit 5:

   ```
   ETX-203A# configure flows
   ETX-203A>config>flows# flow f10_out
   ETX-203A>config>flows>flow(f10_out)$ classifier v10
   ETX-203A>config>flows>flow(f10_out)$ ingress-port ethernet 3
   ETX-203A>config>flows>flow(f10_out)$ egress-port ethernet 1 queue 0 block 0/1
   ETX-203A>config>flows>flow(f10_out)$ vlan-tag push vlan 100 p-bit fixed 5
   ETX-203A>config>flows>flow(f10_out)$ no shutdown
   ETX-203A>config>flows>flow(f10_out)$ exit all
   ETX-203A#
   ```

➤ To configure the incoming flow:

1. Set up a classifier profile to forward frames from VLAN 100 and inner VLAN 10:

   ```
   ETX-203A# configure flows
   ETX-203A>config>flows# classifier-profile v100_inner_v10 match-any
   ETX-203A>config>flows>classifier-profile(v100_inner_v10)$ match vlan 100 inner-vlan 10
   ETX-203A>config>flows>classifier-profile(v100_inner_v10)$ exit all
   ETX-203A#
   ```
2. Set up a flow using the previously defined classifier profile, with ingress at ETH 1 and egress at ETH 3, and popping the outer VLAN:

```
ETX-203A# configure flows
ETX-203A>config>flows# flow f100_in
ETX-203A>config>flows>flow(f100_in)$ classifier v100_inner_v10
ETX-203A>config>flows>flow(f100_in)$ ingress-port ethernet 1
ETX-203A>config>flows>flow(f100_in)$ egress-port ethernet 3 queue 0 block 0/1
ETX-203A>config>flows>flow(f100_in)$ vlan-tag pop vlan
ETX-203A>config>flows>flow(f100_in)$ no shutdown
ETX-203A>config>flows>flow(f100_in)$ exit all
ETX-203A#
```

### ETP Flows

- To configure ETP flows:
  - Flow sub1:
    - Ingress = ethernet 3
    - Egress = etp ETP1 subscriber 1, CoS mapping profile my-p-bit (refer to CoS Mapping Profiles for details on CoS mapping profiles)
  - Flow trans1:
    - Ingress = etp ETP1 transport 1
    - Egress = ethernet 1, queue 0, block 0/1.

```
ETX-203A# configure flows
ETX-203A>config>flows# flow sub1
ETX-203A>config>flows>flow(sub1)# ingress-port ethernet 3
ETX-203A>config>flows>flow(sub1)# egress-port etp ETP1 subscriber 1 cos-mapping my-p-bit
ETX-203A>config>flows>flow(sub1)# exit
ETX-203A>config>flows# flow trans1
ETX-203A>config>flows>flow(trans1)# ingress-port etp ETP1 transport 1
ETX-203A>config>flows>flow(trans1)# egress-port ethernet 1 queue 0 block 0/1
ETX-203A>config>flows>flow(trans1)# exit
ETX-203A>config>flows#
```

### Testing Flows

You can run application layer loopbacks on a flow, with exchange of source and destination MAC addresses or IP addresses of incoming packets. This applies to all the data associated with the flow.

- To run an application layer loopback test:
  1. Create a flow with the ingress port equal to the egress port.
  2. Navigate to `configure flows flow <flow-name>` to select the above flow.

    The `config>flows>flow<flow-name>#$` prompt is displayed.

    3. Enter:
       ```bash
       test [{mac-swap|ip-swap}] [duration <seconds>] [ttl-force <ttl>].
       ```
The flow is activated, and the TEST LED is turned on. The test runs for the duration specified. If 0 is specified for the duration, the test runs until it is stopped manually.

**Note** Regardless of whether the **mac-swap** or **ip-swap** option is specified, if there is an IP header in the frames, then both MAC and IP address are swapped, otherwise only the MAC is swapped.

➢ To end the test:
1. Navigate to **configure flows flow** `<flow-name>` to select the flow being tested.
   
   The **config>flows>flow(<flow-name>)#** prompt is displayed.

   2. Enter:
   ```
   no test.
   ```

### Displaying Flow Statistics

You can display the number of forwarded and discarded packets and bytes for a flow.

**Note** Refer to [Configuring Policer Aggregate Parameters](#) for information on displaying statistics for flows associated with policer aggregates.

➢ To display the statistics for a flow:
   - At the relevant flow context (**config>flows>flow(<flow-id>)**), enter:
     ```
     show statistics running.
     ```
   
   Flow statistics are displayed.

➢ To clear the statistics for a flow:
   - At the relevant flow context (**config>flows>flow(<flow-id>)**), enter:
     ```
     clear-statistics.
     ```
   
   The statistics for the flow are cleared.

### Example

**Note** This example uses flow f10_out, created in the traffic flow example.
To display flow statistics:

```
ETX-203A# configure flows flow f10_out
ETX-203A>config>flows>flow(f10_out)# show statistics running
```

**Rate Sampling Window**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Window Size</td>
<td>15</td>
</tr>
<tr>
<td>Window Remain</td>
<td>12</td>
</tr>
<tr>
<td>Time [Min.]</td>
<td></td>
</tr>
</tbody>
</table>

**Rx Statistics**

<table>
<thead>
<tr>
<th></th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packets</td>
<td>0</td>
</tr>
<tr>
<td>Bytes</td>
<td>0</td>
</tr>
</tbody>
</table>

**Drop Statistics**

<table>
<thead>
<tr>
<th>Total</th>
<th>Green</th>
<th>Yellow/Red</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packets</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Rate [pps]</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Bytes</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Rate [bps]</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

**Tx Statistics**

<table>
<thead>
<tr>
<th>Total</th>
<th>Green</th>
<th>Yellow</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packets</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Rate [pps]</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Bytes</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Rate [bps]</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

**Pick Measurement**

<table>
<thead>
<tr>
<th>Min.</th>
<th>Max.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tx Bit Rate [bps]</td>
<td>0</td>
</tr>
<tr>
<td>Drop Bit Rate [bps]</td>
<td>0</td>
</tr>
</tbody>
</table>

---

**5.27 Ethernet OAM**

Ethernet OAM (operation, administration, and maintenance) functions provide end-to-end connectivity checks and performance monitoring.

**OAM CFM (Connectivity Fault Management)**

Ethernet Service OAM is a set of functions for managing Ethernet services as specified by the IEEE 802.1ag and ITU-T Y.1731 standards. It allows service providers to operate, administer, and maintain Ethernet services.

The Connectivity Fault Management (CFM) uses an end-to-end Ethernet layer OAM protocol for proactive connectivity monitoring, fault verification, and fault
isolation. These actions are performed using IEEE 802.1ag standard Layer 2 ping, Layer 2 traceroute, and end-to-end connectivity check of Ethernet networks.

ETX-203A can act as a Maintenance Entity Group Intermediate Point (MIP) or Maintenance Entity Group End Point (MEP). If ETX-203A is acting as a MIP, it forwards OAM CFM messages transparently, responding only to OAM link trace (LTM) and unicast OAM loopback (LBM).

To configure the service OAM:
1. Configure general OAM parameters (multicast MAC address)
2. Add and configure maintenance domain(s) (MD).
3. Configure maintenance associations for the added MDs.
4. If ETX-203A is acting as a MIP:
   a. Configure the necessary flows to the unit(s) acting as MEP(s)
   b. Configure the MA classification to correspond to the flows.
   c. Configure the MIP policy (refer to Configuring MIP for an example of MIP configuration).
5. If ETX-203A is acting as a MEP:
   a. Configure MA endpoints, referred as MEPs.
   b. Configure MEP services
   c. Configure Destination NEs.

Standards
IEEE 802.1ag-D8
ITU-T Y.1731

Benefits
Ethernet service providers can monitor their services proactively and guarantee that customers receive the contracted SLA. Fault monitoring and end-to-end performance measurement provide tools for monitoring frame delay, frame delay variation, and frame loss and availability.

Functional Description
ETX-203A provides the OAM (CFM) functions listed below in packet-switched networks:
- Continuity check
- Non-intrusive loopback, used to detect loss of bidirectional continuity.
- Performance measurements (per service).

The device supports:
- Up to 128 maintenance domains (MDs)
- Up to 128 maintenance associations (MAs)
- Up to 128 maintenance endpoints (MEPs). Up to eight MEPs can be configured for an MA (on EVC.cos configuration).
• Up to 512 remote MEPs. Up to 100 remote MEPs can be configured for a MEP.
• Up to 256 services. Up to eight services can be configured for a MEP.
• Up to 255 destination NEs.

**Note**  
The above limits are subject to the limit of 300 received PPS (packets per second). This includes AIS, Linktrace, and other management packets. It does not include continuity check (CC), loopback (LB), delay measurement messages (DMM), or loss measurement messages (LMM).

### Factory Defaults

By default, there are no MDs, MAs, or MEPs.

The default OAM CFM multicast address is 01-80-C2-00-00-30.

When a maintenance domain is created, it has the following default configuration.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>proprietary-cc</td>
<td>no proprietary-cc</td>
<td>Standard OAM protocol</td>
</tr>
<tr>
<td>md-level</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>name</td>
<td>string &quot;MD&lt;mdid&gt;&quot;</td>
<td>For example the default name for maintenance domain 1 is “MD1”.</td>
</tr>
</tbody>
</table>

When a maintenance association is created, it has the following default configuration.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>ccm-interval</td>
<td>1s</td>
<td>Continuity check interval is 1 second</td>
</tr>
<tr>
<td>name</td>
<td>string &quot;MA&lt;maid&gt;&quot;</td>
<td>For example the default name for maintenance association 1 is “MA1”.</td>
</tr>
</tbody>
</table>

When a maintenance endpoint is created, it has the following default configuration.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>classification</td>
<td>vlan 0</td>
<td></td>
</tr>
<tr>
<td>queue</td>
<td>fixed 0 block 0/0</td>
<td></td>
</tr>
<tr>
<td>dest-addr-type</td>
<td>ccm multicast pm unicast</td>
<td>Destination address type for CCM messages – multicast</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Destination address type for performance measurement messages – unicast</td>
</tr>
<tr>
<td>ccm-initiate</td>
<td>ccm-initiate</td>
<td>Initiate continuity check messages</td>
</tr>
<tr>
<td>ccm-priority</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>shutdown</td>
<td>shutdown</td>
<td>Administratively disabled</td>
</tr>
</tbody>
</table>
When a service is created, it has the following default configuration.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>delay-threshold</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>delay-var-threshold</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>classification</td>
<td>priority-bit 0</td>
<td></td>
</tr>
<tr>
<td>dmm-interval</td>
<td>1s</td>
<td></td>
</tr>
<tr>
<td>lmm-interval</td>
<td>1s</td>
<td></td>
</tr>
<tr>
<td>shutdown</td>
<td>shutdown</td>
<td>Administratively disabled</td>
</tr>
</tbody>
</table>

When a destination NE is created, it has the following default configuration.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>remote</td>
<td>mac-address 00-00-00-00-00-00</td>
<td></td>
</tr>
</tbody>
</table>

**Configuring OAM CFM General Parameters**

If necessary you can define multicast MAC address for OAM CFM messages. You can also display OAM CFM information.

➢ To configure the OAM CFM multicast MAC address:

- Navigate to the CFM (Connectivity Fault Management) context (config>oam>cfm) and enter:
  ```
  multicast-addr <mac-address>
  ```

You can display OAM CFM information by typing `show summary`, as shown in the following.

```
ETX-203A# configure oam cfm
ETX-203A# config>oam>cfm# show summary
     md slot/classification     admin status  mep ok/total md/ma/mepid md/ma name     lvl port md/ma/mepid md/ma name slot/port classification admin status mep ok/total
001/001/001   3 eth1 100  enable off 1/1
002/002/8191  3 eth1 0  disable 1/1
002/005/123   3 eth1 100/200 enable off 0/2
002/006/101   3 eth1 untagged enable off 0/3
003/001/001   4 eth1 100.1 enable off 0/1
004/001/001   0 eth1 4000 enable off 0/1
004/002/001   0 eth1 3000/ enable off 0/3
```

You can display information on MIPs by typing `show mips`.

**Configuring Maintenance Domains**

MDs are domains for which the connectivity faults are managed. Each MD is assigned a name that must be unique among all those used or available to an
operator. The MD name facilitates easy identification of administrative responsibility for the maintenance domain.

- **To add a maintenance domain:**
  - At the `config>oam>cfm#` prompt enter:
    
    ```
    maintenance-domain <mdid>
    ```
    
    where `<mdid>` is 1–128.
    
    The maintenance domain is created and the `config>oam>cfm>md(<mdid>)$` prompt is displayed.

- **To delete a maintenance domain:**
  - At the `config>oam>cfm#` prompt enter:
    
    ```
    no maintenance-domain <mdid>
    ```
    
    The maintenance domain is deleted.

- **To configure a maintenance domain:**
  1. Navigate to `config>oam>cfm maintenance-domain <mdid>` to select the maintenance domain to configure.
    
    The `config>oam>cfm>md(<mdid>)#` prompt is displayed
  2. Enter all necessary commands according to the tasks listed below.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring maintenance association for the MD</td>
<td><code>maintenance-association &lt;maid&gt;</code></td>
<td>Refer to Configuring Maintenance Associations</td>
</tr>
<tr>
<td>Specifying the maintenance domain level</td>
<td><code>md-level &lt;md-level&gt;</code></td>
<td>The allowed range for <code>md-level</code> is 0–7. <strong>Note:</strong> If prestandard OAM protocol is being used, the only allowed value for the maintenance domain level is 3.</td>
</tr>
<tr>
<td>Defining MIP policy</td>
<td>`mip-policy { explicit</td>
<td>default}`</td>
</tr>
<tr>
<td>Task</td>
<td>Command</td>
<td>Comments</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>----------</td>
</tr>
</tbody>
</table>
| Specifying the name format and name of the maintenance domain | **name** <md-name-string>  
**name dns** <md-name-string>  
**name mac-and-uint** <md-name-mac> <md-name-uint>  
**no name** | - Maximum length of **md-name-string** is 43 characters  
- Maximum combined length of **md-name-string** and **ma-name-string** (maintenance association name) is 48 characters  
- Format **mac-and-uint** – Specify **md-name-mac** as xx-xx-xx-xx-xx-xx, and **md-name-uint** as an unsigned integer decimal number (0–65535)  
- If prestandard OAM protocol is being used, the maintenance domain must have no name (use command **no name**). |
| Specifying the OAM protocol type | **no proprietary-cc**  
**proprietary-cc** | - Use **no proprietary-cc** for standard OAM protocol  
- Use **proprietary-cc** for prestandard OAM protocol.  
*Note: The MD must have no name (via **no name**) and the level must be 3 before you can set the protocol to prestandard.* |

### Configuring Maintenance Associations

A maintenance domain contains maintenance associations.

- **To add a maintenance association (MA):**
  - At the **config>oam>cfm>md(<mdid>)#** prompt enter:
    - **maintenance-association** <maid>
      - where <maid> is 1–128.
  - The maintenance association is created and the **config>oam>cfm>md(<mdid>)>ma(<maid>)$** prompt is displayed.

- **To delete a maintenance association:**
  - At the **config>oam>cfm>md(<mdid>)#** prompt enter:
    - **no maintenance-association** <maid>
  - The maintenance association is deleted.

- **To configure a maintenance association:**
  1. Navigate to **configure oam cfm maintenance-domain** <mdid> **maintenance-association** <maid> to select the maintenance association to configure.
  - The **config>oam>cfm>md(<mdid>)>ma(<maid>)#** prompt is displayed
  2. Enter all necessary commands according to the tasks listed below.
<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifying the interval between continuity check messages</td>
<td>`ccm-interval {3.33ms</td>
<td>10ms</td>
</tr>
<tr>
<td>Associating the MA with a VLAN</td>
<td><code>classification vlan &lt;vlan-id&gt;</code></td>
<td>Verify that the VLAN is the same as the VLAN associated with the MEP</td>
</tr>
<tr>
<td>Configuring MEP for the MA</td>
<td><code>mep &lt;mepid&gt;</code></td>
<td>Refer to Configuring Maintenance Endpoints</td>
</tr>
</tbody>
</table>
| Defining MIP policy | `mip-policy { explicit | default | defer }` | • Explicit – MIP is automatically created for ports corresponding to VLAN classification of MA, only if a corresponding MEP exists at a lower MD level  
• Default – MIP is automatically created for ports corresponding to VLAN classification of MA  
• Defer – MIP policy is inherited from the MD MIP policy. |
| Specifying the name format and name of the maintenance association | `name string <ma-name-string>`  
`name primary-vid <ma-name-vid>`  
`name uint <ma-name-uint>`  
`name icc <ma-name-icc>` | • Maximum length of `ma-name-string` is 45 characters  
• Maximum combined length of md name string and ma name string is 48 characters  
• Format `primary-vid` – Specify `ma-name-vid` as 1–4094  
• Format `uint` – Specify `ma-name-uint` as an unsigned integer decimal number (0–65535)  
• Format `icc` – Specify `ma-name-icc` as the ITU carrier code that is assigned to the relevant network operator/service provider. The codes are maintained by ITU-T as defined in ITU-T Rec. M.1400  
• If prestandard OAM protocol is being used, the maintenance association must have no name (use command `no name`). |

**Configuring Maintenance Endpoints**

Maintenance endpoints reside at the edge of a maintenance domain. They initiate and respond to CCMs, linktrace requests, and loopbacks to detect, localize, and diagnose connectivity problems.

**Note**

*For every MEP you must configure a flow with the same classification as the MEP, in the direction NNI to UNI, if the MEP is not bound to a port. If the MEP is bound to a port, you must configure a flow with the same classification as the MEP, in the direction UNI to NNI.*

> To add a maintenance endpoint (MEP):

- At the `config>oam>cfm>md(<mdid>)>ma(<maid>)`# prompt, enter:
  ```
  mep <mepid>
  ```
where `<mepid>` is 1–8191.

The MEP is created and the prompt
`config>oam>cfm>md(<mdid>)>ma(<maid>)>mep(<mepid>)$` is displayed.

To delete a maintenance endpoint:
- At the `config>oam>cfm>md(<mdid>)>ma(<maid>)#$` prompt, enter:
  
  `no mep <mepid>`

  The maintenance endpoint is deleted.

*Note* You can remove a maintenance endpoint regardless of whether it contains services.

To configure a maintenance endpoint:

1. Navigate to `configure oam cfm maintenance-domain <mdid> maintenance-association <maid> mep <mepid>` to select the maintenance endpoint to configure.

   The prompt `config>oam>cfm>md(<mdid>)>ma(<maid>)>mep(<mepid>)#$` is displayed.

2. Enter all necessary commands according to the tasks listed below.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defining sending of AIS</td>
<td>ais [ interval [ 1s</td>
<td>1min ] ] [priority &lt;priority&gt;]</td>
</tr>
<tr>
<td>Binding the MEP to an Ethernet port</td>
<td>bind ethernet &lt;port&gt;</td>
<td></td>
</tr>
<tr>
<td>Binding the MEP to an ETP transport port if ETP is used</td>
<td>bind etp &lt;etp-name&gt; transport &lt;port-id&gt;</td>
<td></td>
</tr>
<tr>
<td>Enabling initiation of continuity check messages (CCM)</td>
<td>ccm-initiate</td>
<td>To disable initiating continuity check messages, enter <code>no ccm-initiate</code></td>
</tr>
<tr>
<td>Specifying the priority of CCMs and LTMs transmitted by the MEP</td>
<td>ccm-priority &lt;priority&gt;</td>
<td>The allowed range for <code>&lt;priority&gt;</code> is 0–7</td>
</tr>
<tr>
<td>Associating the MEP with a classifier profile or VLAN</td>
<td>classification vlan &lt;vlan-id&gt;</td>
<td>You can associate more than one MEP to the same VLAN if the MEPs belong to MDs with different levels Verify that the VLAN is the same as the VLAN associated with the MA</td>
</tr>
<tr>
<td></td>
<td>classification profile &lt;profile-name&gt;</td>
<td></td>
</tr>
<tr>
<td>Defining client MD level</td>
<td>client-md-level &lt;md-level&gt;</td>
<td></td>
</tr>
<tr>
<td>Specifying continuity verification method</td>
<td>continuity-verification &lt;cc-based</td>
<td>lb-based&gt;</td>
</tr>
<tr>
<td>Task</td>
<td>Command</td>
<td>Comments</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>----------</td>
</tr>
<tr>
<td>Defining the MAC address type sent in OAM continuity check messages (CCM) and performance measurement messages (PM)</td>
<td>dest-addr-type [ccm {unicast</td>
<td>multicast}] [pm {unicast</td>
</tr>
<tr>
<td>Defining a unicast MAC address if you defined unicast MAC address type for CCM messages with the dest-addr-type command</td>
<td>dest-mac-addr &lt;mac-addr&gt;</td>
<td>MAC address is in format xx-xx-xx-xx-xx-xx</td>
</tr>
<tr>
<td>Defining direction</td>
<td>direction { up</td>
<td>down }</td>
</tr>
<tr>
<td>Defining forwarding method</td>
<td>forwarding-method { e-line</td>
<td>e-lan }</td>
</tr>
<tr>
<td>Defining the queue for the MEP</td>
<td>queue fixed &lt;queue-id&gt; [block &lt;level-id&gt;/&lt;queue-id&gt;] queue queue-mapping &lt;queue-map-profile-name&gt; [block &lt;level-id&gt;/&lt;queue-id&gt;]</td>
<td></td>
</tr>
<tr>
<td>Defining remote MEP with which the MEP communicates</td>
<td>remote-mep &lt;remote-mep-id&gt;</td>
<td>Allowed range for remote MEP is 1–8191. The MEP ID and the remote MEP ID must be different. You can define up to 511 remote MEPs for the local MEP if standard OAM protocol is being used for the MD and the destination address type is multicast, otherwise you can define only one remote MEP.</td>
</tr>
<tr>
<td>Configuring service for the MEP</td>
<td>service &lt;serviceid&gt;</td>
<td>Refer to Configuring Maintenance Endpoint Services</td>
</tr>
<tr>
<td>Displaying MEP status</td>
<td>show status</td>
<td></td>
</tr>
<tr>
<td>Displaying remote MEP status</td>
<td>show remote-mep &lt;remote-mep-id&gt; status</td>
<td></td>
</tr>
<tr>
<td>Administratively enabling MEP</td>
<td>no shutdown</td>
<td>To deactivate the MEP, enter shutdown</td>
</tr>
</tbody>
</table>
Example

Creating MD, MA, and MEP

To create MD, MA, and MEP:

- MD ID 1
- MA ID 1
- MEP ID 1 – Remote MEP ID 2, classification VLAN 100.

```
ETX-203A# configure oam cfm
ETX-203A>config>oam>cfm# maintenance-domain 1
ETX-203A>config>oam>cfm>md(1)$ maintenance-association 1
ETX-203A>config>oam>cfm>md(1)>ma(1)$ classification vlan 100
ETX-203A>config>oam>cfm>md(1)>ma(1)$ mep 1
ETX-203A>config>oam>cfm>md(1)>ma(1)>mep(1)$ classification vlan 100
ETX-203A>config>oam>cfm>md(1)>ma(1)>mep(1)$ queue fixed 1 block 0/1
ETX-203A>config>oam>cfm>md(1)>ma(1)>mep(1)$ remote-mep 2
ETX-203A>config>oam>cfm>md(1)>ma(1)>mep(1)$ no shutdown
```

Displaying MEP Status and remote MEP

The following illustrates displaying MEP status and remote MEP.

```
ETX-203A>config>oam>cfm>md(1)>ma(1)>mep(1)# show status
Port      : Ethernet      1
Direction : Down
Priority  : 0

MD Name               : MD1
MA Name               : MA1
Administrative Status : Up

MEP Defect                                          Status
Rx LCK                                              Off
Rx AIS                                              Off
Cross Connected CCM (Mismatch; Unexpected MD Level) Off
Invalid CCM (Unexpected MEP; Unexpected CCM Period) Off

Remote MEP  Remote MEP Address  Operational Status
-----------------------------------------------------------------------------
4           00-00-00-00-00-00   Fail
```

Configuring MIP

Configure the MIP as follows:

- Verify that you have flows configured between ETX-203A and the device(s) acting as MEP(s) (refer to Flows for information on defining flows).
- Configure the MA classification to the same classification that is used by the flows.
• Configure MIP policy to default.

```plaintext
ETX-203A# configure oam cfm
ETX-203A>config>oam>cfm# maintenance-domain 2
ETX-203A>config>oam>cfm>md(2)# maintenance-association 2
ETX-203A>config>oam>cfm>md(2)>ma(2)$ classification vlan 100
ETX-203A>config>oam>cfm>md(2)>ma(2)$ mip-policy default
ETX-203A>config>oam>cfm>md(2)>ma(2)# exit
ETX-203A>config>oam>cfm>md(2)# exit
ETX-203A>config>oam>cfm# show mips
```

<table>
<thead>
<tr>
<th>Port</th>
<th>VLAN</th>
<th>MD-level</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>100</td>
<td>3</td>
</tr>
</tbody>
</table>

### Configuring Maintenance Endpoint Services

You can configure up to eight services on a MEP, corresponding to each p-bit. Only one service is allowed if the classifier profile associated with the MEP is according to p-bit.

Each service sets delay and delay variation thresholds. If the thresholds are exceeded, the service is declared as degraded. You can also define priority of OAM messages originating from this service.

➤ To add a MEP service:

- At the `config>oam>cfm>md(<mdid>)>ma(<maid>)>mep(<mepid>)$` prompt, enter:

  ```plaintext
  service <serviceid>
  ```

  where `<serviceid>` is 1–8.

  The prompt

  ```plaintext
  config>oam>cfm>md(<mdid>)>ma(<maid>)>mep(<mepid>)>service(<serviceid>)$
  ```

  is displayed.

➤ To configure a MEP service:

1. Navigate to `configure oam cfm maintenance-domain <mdid> maintenance-association <maid> mep <mepid> service <serviceid>` to select the service to configure (`<serviceid>` is 1–8).

   The prompt

   ```plaintext
   config>oam>cfm>md(<mdid>)>ma(<maid>)>mep(<mepid>)>service(<serviceid>)$
   ```

   is displayed.

2. Enter all necessary commands according to the tasks listed below.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
</table>
| Associating this service with a priority  | `classification priority-bit <p-bit>` | The allowed range is 0–7  
|                                           |                                  | **Note:** Only one service can be defined on each p-bit.                |
| Specifying delay threshold in microseconds| `delay-threshold <delay-thresh>` | The allowed range for delay threshold is: 1–5,000,000                   |
### Task | Command | Comments
--- | --- | ---
Specifying delay variation threshold in microseconds | `delay-var-threshold <delay-var-thresh>` | The allowed range for delay variation threshold is: 1–5,000,000

Specifying the interval for delay measurement messages, to be used by all remote NEs defined for service | `dmm-interval {100ms | 1s | 10s}` | 

Specifying the interval for loss measurement messages, to be used by all remote NEs defined for service | `lmm-interval {100ms | 1s | 10s}` | 

Configuring destination NE for service | `dest-ne <dest-ne-index>` | The allowed range is 1–255

Activating the MEP service | `no shutdown` | You can activate a service only if the corresponding MEP is active and you have defined at least one destination NE

### Configuring Destination NEs

For performance measurement it is necessary to know the exact address of the destination NE. You can configure the remote MAC address of the NE or ETX-203A can learn it from the CCM messages.

If the remote MAC address is not configured and needs to be learned, performance measurement messages are sent with all 0s in the MAC address until the address is learned.

- **To add a destination NE:**
  - At the prompt `config>oam>cfm>md(<mdid>)>ma(<maid>)>mep(<mepid>)>service(<serviceid>)#`, enter:
    ```
    dest-ne <dest-ne-index>
    ```
    where `<dest-ne-index>` is 1–255.
    
    The prompt `config>oam>cfm>md(<mdid>)>ma(<maid>)>mep(<mepid>)>service(<serviceid>)>dest-ne(<dest-ne-index>)$` is displayed.

- **To configure a destination NE:**
  1. Navigate to `configure oam cfm maintenance-domain <mdid>
     maintenance-association <maid> mep <mepid> service <serviceid> dest-ne <dest-ne-index>` to select the destination NE to configure.

    The prompt `config>oam>cfm>md(<mdid>)>ma(<maid>)>mep(<mepid>)>service(<serviceid>)>dest-ne(<dest-ne-index>)#` is displayed.
  2. Enter all necessary commands according to the tasks listed below.
### Configuring OAM CFM Service Event Reporting

In addition to the regular OAM statistics collection, ETX-203A supports proactive SLA measurements per OAM service, as per RMON-based RFC 2819. The device sends reports when one of the counters rises above or drops below the set thresholds within the specified sampling period of time. These reports can be sent as SNMP traps to the defined network management stations, or written to the event log.

The following counters can be monitored:

- **Far End Frame Loss Ratio** – Total number of OAM frames lost from local MEP to remote MEP, divided by total number of transmitted OAM frames since the service was activated
- **Near End Frame Loss Ratio** – Total number of OAM frames lost from remote MEP to local MEP, divided by total number of transmitted OAM frames since the service was activated
- **Frames Above Delay** – Number of frames that exceeded delay threshold
- **Frames Above Delay Variation** – Number of frames below or equal delay threshold
- **Far End Unavailability Ratio** – Total number of far end unavailable seconds divided by elapsed time since service was activated
- **Near End Unavailability Ratio** – Total number of near end unavailable seconds divided by elapsed time since service was activated.
To configure the event reporting for a service:

1. Navigate to `configure fault cfm`.

2. Specify the service and counter for which you wish to configure event reporting:

   ```
   service md <mdid> ma <maid> mep <mepid> service <serviceid>
   {above-delay | above-delay-var | far-end-loss-ratio | near-end-loss-ratio | far-end-unavailability-ratio | near-end-unavailability-ratio}
   ```

   The prompt `config>fault>cfm>service(<mdid>/<maid>/<mepid>/<serviceid>)#` is displayed.

3. Specify the type of event reporting for the counter (refer to Table 5-15):

   - For counters `above-delay` and `above-delay-var`:
     ```
     frames-report [event {none | log | trap | logandtrap}]
     [rising-threshold <rising-threshold>] [falling-threshold <falling-threshold>]
     [sampling-interval <value>]
     ```

   - For counters `near-end-loss-ratio` or `far-end-loss-ratio`:
     ```
     frames-report [event {none | log | trap | logandtrap}]
     [rising-threshold {1e-3 | 1e-4 | 1e-5 | 1e-6 | 1e-7 | 1e-8 | 1e-9 | 1e-10}]
     [falling-threshold {1e-3 | 1e-4 | 1e-5 | 1e-6 | 1e-7 | 1e-8 | 1e-9 | 1e-10}]
     ```

   - For counters `near-end-unavailability-ratio` or `far-end-unavailability-ratio`:
     ```
     frames-report [event {none | log | trap | logandtrap}]
     [rising-threshold <rising-threshold>]
     [falling-threshold <falling-threshold>]
     ```

4. Type `no shutdown` to activate the event reporting for the counter.

Table 5-15. Service Event Reporting Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Possible Values</th>
</tr>
</thead>
</table>
| event           | Specifies the type of event reporting | none – The event is not reported
|                 |                              | log – The event is reported via the event log        |
|                 |                              | trap – An SNMP trap is sent to report the event      |
|                 |                              | logandtrap – The event is reported via the event log and an SNMP trap |
### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Possible Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>rising-threshold</td>
<td>A value above rising-threshold within the sampling interval for the particular event is considered as rising event occurred</td>
<td>• For counters above-delay or above-delay-var: 1–60</td>
</tr>
<tr>
<td>falling-threshold</td>
<td>A value below falling-threshold within the sampling interval for the particular event is considered as falling event occurred</td>
<td>• For counters near-end-loss-ratio or far-end-loss-ratio: 1e-3 1e-4 1e-5 1e-6 1e-7 1e-8 1e-9 1e-10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For counters near-end-unavailability-ratio or far-end-unavailability-ratio: 1–100</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> Rising threshold must be greater than falling-threshold.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>sampling-interval</td>
<td>Specifies the interval in seconds over which the data is sampled and compared with the rising and falling thresholds</td>
<td>• Relevant only for counters above-delay or above-delay-var</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Sampling interval value must be at least double rising threshold.</td>
</tr>
</tbody>
</table>

### Example

To configure OAM CFM event reporting:

- Configure counters for the following service, as shown in the table below:
  - Maintenance domain 5
  - Maintenance association 8
  - MEP 3
  - Service 4.

<table>
<thead>
<tr>
<th>Counter</th>
<th>Event Type</th>
<th>Rising Threshold</th>
<th>Falling Threshold</th>
<th>Sampling Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frames Above Delay</td>
<td>Log and trap</td>
<td>4</td>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td>Frames Above Delay Variation</td>
<td>Log</td>
<td>10</td>
<td>5</td>
<td>30</td>
</tr>
<tr>
<td>Far End Frame Loss Ratio</td>
<td>Trap</td>
<td>1e-4</td>
<td>1e-8</td>
<td></td>
</tr>
<tr>
<td>Near End Frame Loss Ratio</td>
<td>Log and trap</td>
<td>1e-9</td>
<td>1e-10</td>
<td></td>
</tr>
<tr>
<td>Far End Unavailability Ratio</td>
<td>Trap</td>
<td>40</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>Near End Unavailability Ratio</td>
<td>Log</td>
<td>50</td>
<td>25</td>
<td></td>
</tr>
</tbody>
</table>
ETX-203A# configure fault cfm
ETX-203A>config>fault>cfm# service md 5 ma 8 mep 3 service 4 above-delay
ETX-203A>config>fault>cfm>service(5/8/3/4/above-delay)$ frames-report event log andtrap rising-threshold 4 falling-threshold 2 sampling-interval 8
ETX-203A>config>fault>cfm>service(5/8/3/4/above-delay)$ no shutdown
ETX-203A>config>fault>cfm>service(5/8/3/4/above-delay)$ exit

ETX-203A>config>fault>cfm# service md 5 ma 8 mep 3 service 4 above-delay-var
ETX-203A>config>fault>cfm>service(5/8/3/4/above-delay-var)$ no shutdown
ETX-203A>config>fault>cfm>service(5/8/3/4/above-delay-var)$ exit

ETX-203A>config>fault>cfm# service md 5 ma 8 mep 3 service 4 far-end-loss-ratio
ETX-203A>config>fault>cfm>service(5/8/3/4/far-end-loss-ratio)$ frames-report event trap rising-threshold 1e-4 falling-threshold 1e-8
ETX-203A>config>fault>cfm>service(5/8/3/4/far-end-loss-ratio)$ no shutdown
ETX-203A>config>fault>cfm>service(5/8/3/4/far-end-loss-ratio)$ exit

ETX-203A>config>fault>cfm# service md 5 ma 8 mep 3 service 4 near-end-loss-ratio
ETX-203A>config>fault>cfm>service(5/8/3/4/near-end-loss-ratio)$ no shutdown
ETX-203A>config>fault>cfm>service(5/8/3/4/near-end-loss-ratio)$ exit

ETX-203A>config>fault>cfm# service md 5 ma 8 mep 3 service 4 far-end-unavailability-ratio
ETX-203A>config>fault>cfm>service(5/8/3/4/far-end-unavailability-ratio)$ no shutdown
ETX-203A>config>fault>cfm>service(5/8/3/4/far-end-unavailability-ratio)$ exit

ETX-203A>config>fault>cfm# service md 5 ma 8 mep 3 service 4 near-end-unavailability-ratio
ETX-203A>config>fault>cfm>service(5/8/3/4/near-end-unavailability-ratio)$ no shutdown
ETX-203A>config>fault>cfm>service(5/8/3/4/near-end-unavailability-ratio)$ exit
ETX-203A>config>fault>cfm# info detail
    service md 5 ma 8 mep 3 service 4 above-delay
    frames-report event logandtrap rising-threshold 4 falling-threshold 2
    sampling-interval 8
    no shutdown
    exit
    service md 5 ma 8 mep 3 service 4 above-delay-var
    frames-report event log rising-threshold 10 falling-threshold 5 sampling-interval 30
    no shutdown
    exit
    service md 5 ma 8 mep 3 service 4 far-end-loss-ratio
    frames-report event trap rising-threshold 1e-4 falling-threshold 1e-8
    no shutdown
    exit
    service md 5 ma 8 mep 3 service 4 near-end-loss-ratio
    frames-report event logandtrap rising-threshold 1e-9 falling-threshold 1e-10
    no shutdown
    exit
    service md 5 ma 8 mep 3 service 4 far-end-unavailability-ratio
    frames-report event trap rising-threshold 40 falling-threshold 20
    no shutdown
    exit
    service md 5 ma 8 mep 3 service 4 near-end-unavailability-ratio
    frames-report event log rising-threshold 50 falling-threshold 25
    no shutdown
    exit

Displaying OAM CFM Statistics

You can display end-to-end performance monitoring data for the OAM services and destination NEs.

ETX-203A measures performance in fixed 15-minute intervals. It also stores performance data for the last 12 hours (48 intervals).

You can view the following types of statistics for services:

- Running - OAM statistics collected since the service was activated
- 12 hours - OAM statistics for the last 12 hours, or the amount of time since the service was activated, if less than 12 hours.
- Interval - OAM statistics for the current interval or a selected interval. You can select an interval only if it has already ended since the service was activated.

When a service is first activated, you can view statistics for only the current interval. The statistics data is shown for the time elapsed since the beginning of the interval. When the current interval ends, it becomes interval 1 and you can select it for viewing interval statistics. After each interval ends, you can select it for viewing interval statistics.

You can view the following types of statistics for destination NEs:

- Running - OAM statistics collected since performance measurement of the NE started
- 12-hour - OAM statistics for the last 12 hours
Interval – OAM statistics for the current interval or a selected interval.

To display the OAM CFM statistics for a service:

1. Navigate to the level corresponding to the OAM service for which you wish to view the statistics (configure oam cfm maintenance-domain <mdid> maintenance-association <maid> mep <mepid> service <serviceid>).

   The following prompt is displayed:
   ```
   config>oam>cfm>md(<mdid>)>ma(<maid>)>mep(<mepid>)>service(<serviceid>)#.
   ```

2. Enter all necessary commands according to the tasks listed below.

   **Note**: The service for which you wish to view the statistics must be active. If the service is not active, the commands to view statistics are not recognized.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Viewing running statistics</td>
<td>show statistics running</td>
<td>The statistics are displayed as listed in Table 5-16 and Table 5-17</td>
</tr>
<tr>
<td>Viewing statistics for the current interval</td>
<td>show statistics current</td>
<td>The statistics for the current interval are displayed as listed in Table 5-16 and Table 5-17</td>
</tr>
</tbody>
</table>
| Viewing the statistics for a selected interval | show statistics interval <interval-num> | - Allowed values for interval-num: 1–48
- The statistics for the selected interval are displayed as listed in Table 5-16 and Table 5-17
- If you specified an interval that has not yet ended since the service was activated, a message is displayed that the interval doesn’t exist. |
<p>| Viewing statistics for the past 12 hours, or the amount of time since the service was activated if less than 12 hours | show statistics [12-hours] | The statistics for the last 12 hours are displayed as listed in Table 5-16 and Table 5-17 |
| Viewing running statistics, statistics for the current interval, statistics for all intervals, and 12-hour statistics | show statistics all | The statistics are displayed as listed in Table 5-16 and Table 5-17 |
| Viewing statistics for all intervals | show statistics all-intervals  | The statistics are displayed as listed in Table 5-16 and Table 5-17 |</p>
<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clearing the statistics for the service</td>
<td>clear-statistics</td>
<td>All statistics data for the service are cleared, including the stored interval data, except for the elapsed time since the start of the current interval</td>
</tr>
</tbody>
</table>

To display the OAM CFM statistics for a destination NE:

1. Navigate to the level corresponding to the destination NE for which you wish to view the statistics: `configure oam cfm maintenance-domain <mdid> maintenance-association <maid> mep <mepid> service <serviceid> dest-ne <dest-ne-index>.

   The following prompt is displayed:
   ```
   config>oam>cfm>md(<mdid>)>ma(<maid>)>mep(<mepid>)>service(<serviceid>)>dest-ne(<dest-ne-index>)#.
   ```

2. Enter all necessary commands according to the tasks listed below.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Viewing running statistics</td>
<td>show statistics running</td>
<td>The statistics are displayed as listed in Table 5-16 and Table 5-17</td>
</tr>
<tr>
<td>Viewing statistics for the current interval</td>
<td>show statistics current</td>
<td>The statistics for the current interval are displayed as listed in Table 5-16 and Table 5-17</td>
</tr>
</tbody>
</table>
| Viewing the statistics for a selected interval | show statistics interval <interval-num> | - Allowed values for interval-num: 1–48
- The statistics for the selected interval are displayed as listed in Table 5-16 and Table 5-17
- If you specified an interval that has not yet ended since the corresponding service was activated, a message is displayed that the interval doesn’t exist. |
<p>| Viewing statistics for 12 hours     | show statistics 12h   | The statistics for the past 12 hours are displayed as listed in Table 5-16 and Table 5-17        |</p>
<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Viewing running statistics, statistics for the current interval,</td>
<td>show statistics all</td>
<td>The statistics are displayed as listed in Table 5-16 and Table 5-17</td>
</tr>
<tr>
<td>statistics for all intervals, and day statistics</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Viewing statistics for all intervals</td>
<td>show statistics all-intervals</td>
<td>The statistics are displayed as listed in Table 5-16 and Table 5-17</td>
</tr>
<tr>
<td>Clearing the statistics for the destination NE</td>
<td>clear-statistics</td>
<td>All statistics data for the destination NE are cleared, including the stored interval data, except for the elapsed time since the start of the current interval</td>
</tr>
</tbody>
</table>

Table 5-16. OAM Statistic Counters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Far End Tx Frames</td>
<td>Total number of OAM frames transmitted from local MEP to remote MEP since the service was activated</td>
</tr>
<tr>
<td>Far End Rx Frames</td>
<td>Total number of OAM frames received by remote MEP since the service was activated</td>
</tr>
<tr>
<td>Far End Lost Frames</td>
<td>Total number of OAM frames lost from local MEP to remote MEP since the service was activated</td>
</tr>
<tr>
<td>Far End Frame Loss Ratio (%)</td>
<td>Total number of OAM frames lost from local MEP to remote MEP, divided by total number of transmitted OAM frames since the service was activated</td>
</tr>
<tr>
<td>Far End Unavailable Seconds (Sec)</td>
<td>Total number of unavailable seconds in remote MEP since the service was activated</td>
</tr>
<tr>
<td>Near End Tx Frames</td>
<td>Total number of OAM frames transmitted from remote MEP to local MEP since the service was activated</td>
</tr>
<tr>
<td>Near End Rx Frames</td>
<td>Total number of OAM frames received by local MEP since the service was activated</td>
</tr>
<tr>
<td>Near End Lost Frames</td>
<td>Total number of OAM frames lost from remote MEP to local MEP since the service was activated</td>
</tr>
<tr>
<td>Near End Frame Loss Ratio (%)</td>
<td>Total number of near end lost OAM frames divided by total number of near end transmitted OAM frames</td>
</tr>
<tr>
<td>Near End Unavailable Seconds (Sec)</td>
<td>Total number of unavailable seconds in local MEP since the service was activated</td>
</tr>
<tr>
<td>Average Two Way Delay (mSec)</td>
<td>Average delay</td>
</tr>
<tr>
<td>Average Two Way Delay Var (mSec)</td>
<td>Average delay variation</td>
</tr>
<tr>
<td>Frames Above Delay Threshold</td>
<td>Number of frames that exceeded delay threshold</td>
</tr>
<tr>
<td>Frames Above Delay Variation Threshold</td>
<td>Number of frames that exceeded delay variation threshold</td>
</tr>
</tbody>
</table>
### Table 5-17. OAM Delay and Loss Measurement Counters for Destination NEs

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transmitted LMMs</td>
<td>Transmitted loss measurement messages</td>
</tr>
<tr>
<td>Transmitted DMMs</td>
<td>Transmitted delay measurement messages</td>
</tr>
<tr>
<td>Transmitted LMRs</td>
<td>Transmitted loss measurement replies</td>
</tr>
<tr>
<td>Transmitted DMRs</td>
<td>Transmitted delay measurement replies</td>
</tr>
<tr>
<td>Received LMMs</td>
<td>Received loss measurement messages</td>
</tr>
<tr>
<td>Received DMMs</td>
<td>Received delay measurement messages</td>
</tr>
<tr>
<td>Received LMRs</td>
<td>Received loss measurement replies</td>
</tr>
<tr>
<td>Received DMRs</td>
<td>Received delay measurement replies</td>
</tr>
</tbody>
</table>

### Example

- To configure OAM CFM and display statistics:
  - Maintenance domain 5
  - Maintenance association 8
  - MEP 3:
    - Classification VLAN 3
    - Queue 1, block 0/1
    - Remote MEP 6
  - Service 4
  - Dest NE 20.
ETX-203A# configure oam cfm
ETX-203A>config>oam>cfm# maintenance-domain 5
ETX-203A>config>oam>cfm>md(5)$ maintenance-association 8
ETX-203A>config>oam>cfm>md(5)>ma(8)$ mep 3
ETX-203A>config>oam>cfm>md(5)>ma(8)>mep(3)$ classification vlan 3
ETX-203A>config>oam>cfm>md(5)>ma(8)>mep(3)$ queue fixed 1 block 0/1
ETX-203A>config>oam>cfm>md(5)>ma(8)>mep(3)$ remote-mep 6
ETX-203A>config>oam>cfm>md(5)>ma(8)>mep(3)$ no shutdown
ETX-203A>config>oam>cfm>md(5)>ma(8)>mep(3)$ service 4
ETX-203A>config>oam>cfm>md(5)>ma(8)>mep(3)>service(4)$ dest-ne 20$
ETX-203A>config>oam>cfm>md(5)>ma(8)>mep(3)>service(4)$ dest-ne(20)$ exit
ETX-203A>config>oam>cfm>md(5)>ma(8)>mep(3)>service(4)$ no shutdown
ETX-203A>config>oam>cfm>md(5)>ma(8)>mep(3)>service(4)$ exit all
ETX-203A>config oam cfm
ETX-203A>config>oam>cfm# info detail
  multicast-addr 01-80-C2-00-00-30
  maintenance-domain 5
  no proprietary-cc
  md-level 3
  name string "MD5"
  maintenance-association 8
  name string "MA8"
  ccm-interval 1s
  mep 3
  classification vlan 3
  queue fixed 1 block 0/1
  remote-mep 6
  dest-addr-type ccm multicast pm unicast
  ccm-initiate
  ccm-priority 0
  no shutdown
  service 4
  service 4
delay-threshold 2
delay-var-threshold 3
classification priority-bit 0
interval 1s
dest-ne 20
  remote mac-address 00-00-00-00-00-00
  pm single-ended-loss
  pm two-way-delay
exit
  no shutdown
exit
exit
exit
```plaintext
ETX-203A>config>oam>cfm# ma 5 ma 8 mep 3 serv 4 dest 20
ETX-203A>config>oam>cfm>md(5)>ma(8)>mep(3)>service(4)>dest-ne(20)# show statistics running

Running Counters

<table>
<thead>
<tr>
<th>Counter</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Far End TX Frames</td>
<td>3684</td>
</tr>
<tr>
<td>Far End RX Frames</td>
<td>3684</td>
</tr>
<tr>
<td>Far End Lost Frames</td>
<td>0</td>
</tr>
<tr>
<td>Far End Unavailable Seconds (Sec)</td>
<td>0</td>
</tr>
<tr>
<td>Near End TX Frames</td>
<td>3684</td>
</tr>
<tr>
<td>Near End RX Frames</td>
<td>3684</td>
</tr>
<tr>
<td>Near End Lost Frames</td>
<td>0</td>
</tr>
<tr>
<td>Near End Unavailable Seconds (Sec)</td>
<td>0</td>
</tr>
<tr>
<td>Current Delay (mSec)</td>
<td>0.001 mSec</td>
</tr>
<tr>
<td>Current Delay Variation (mSec)</td>
<td>0.000 mSec</td>
</tr>
<tr>
<td>Frames Above Delay Threshold</td>
<td>0</td>
</tr>
<tr>
<td>Frames Above Delay Variation Threshold</td>
<td>0</td>
</tr>
<tr>
<td>Elapsed Time (sec)</td>
<td>3647</td>
</tr>
</tbody>
</table>

Loss and Delay Measurements Messages

<table>
<thead>
<tr>
<th>Message Type</th>
<th>Transmitted</th>
<th>Received</th>
</tr>
</thead>
<tbody>
<tr>
<td>LMMs</td>
<td>3561</td>
<td>0</td>
</tr>
<tr>
<td>DMMs</td>
<td>3561</td>
<td>0</td>
</tr>
</tbody>
</table>
```
ETX-203A>config>oam>cfm>md(5)>ma(8)>mep(3)>service(4)>dest-ne(20)# show statistics current
Current
-------------------------------------------------------------------------------
| Far End Tx Frames       | 854     |
| Far End Rx Frames       | 854     |
| Far End Lost Frames     | 0       |
| Far End Frame Loss Ratio (%) | 0.0000% |
| Far End Unavailable Seconds (Sec) | 0      |

Far End Tx Frames       : 855
Far End Rx Frames       : 855
Far End Lost Frames     : 0
Far End Frame Loss Ratio (%) | 0.0000%
Far End Unavailable Seconds (Sec) | 0

Average Two Way Delay (mSec) : 0.001
Average Two Way Delay Var (mSec) : 0.000
Frames Above Delay Threshold : 0
Frames Above Delay Variation Threshold : 0

Elapsed Time (sec) : 847
Loss and Delay Measurements Messages
-------------------------------------------------------------------------------
| Transmitted  |
| LMMs : 826   | 0      |
| DMMs : 826   | 0      |

| Received  |
| LMRs : 826 | 0      |
| DMRs : 826  | 0      |
ETX-203A>config>oam>cfm>md(5)>ma(8)>mep(3)>service(4)>dest-ne(20)# show statist interval 3

<table>
<thead>
<tr>
<th>Interval</th>
<th>Far End Tx Frames</th>
<th>Far End Rx Frames</th>
<th>Far End Lost Frames</th>
<th>Far End Frame Loss Ratio (%)</th>
<th>Far End Unavailable Seconds (Sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>910</td>
<td>910</td>
<td>0</td>
<td>0.0000%</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Near End Tx Frames: 909</td>
<td>Near End Rx Frames: 909</td>
<td>Near End Lost Frames: 0</td>
<td>Near End Frame Loss Ratio (%) 0.0000%</td>
<td>Near End Unavailable Seconds (Sec) 0</td>
</tr>
<tr>
<td></td>
<td>Average Two Way Delay (mSec): 0.001</td>
<td>Average Two Way Delay Var (mSec): 0.000</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

### Loss and Delay Measurements Messages

<table>
<thead>
<tr>
<th>Transmitted</th>
<th>Received</th>
</tr>
</thead>
<tbody>
<tr>
<td>LMMs : 879</td>
<td>LMMs : 879 0</td>
</tr>
<tr>
<td>DMMs : 879</td>
<td>DMMs : 879</td>
</tr>
<tr>
<td>LMRs : 879</td>
<td>LMRs : 879</td>
</tr>
<tr>
<td>DMRs : 879</td>
<td>DMRs : 879</td>
</tr>
</tbody>
</table>

ETX-203A>config>oam>cfm>md(5)>ma(8)>mep(3)>service(4)>dest-ne(20)# show statistics 12h

<table>
<thead>
<tr>
<th>12-Hours</th>
<th>Far End Tx Frames</th>
<th>Far End Rx Frames</th>
<th>Far End Lost Frames</th>
<th>Far End Unavailable Seconds (Sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2830</td>
<td>2830</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Near End Tx Frames: 2829</td>
<td>Near End Rx Frames: 2829</td>
<td>Near End Lost Frames: 0</td>
<td>Near End Unavailable Seconds (Sec) 0</td>
</tr>
<tr>
<td></td>
<td>Average Two Way Delay (mSec): 0.000</td>
<td>Average Two Way Delay Var (mSec): 0.000</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Performing OAM Loopback

This diagnostic utility verifies OAM connectivity on Ethernet connections. You can execute the loopback according to the destination MAC address or the remote MEP number.

**Note**

The option for remote MEP ID is available only if ETX-203A can resolve at least one remote MEP MAC address.

➤ To run an OAM loopback:

- At the `config>oam>cfm>md(<mdid>)>ma(<maid>)>mep(<mepid>)#` prompt, enter all necessary commands according to the tasks listed below.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifying remote MEP by</td>
<td><code>lbm address &lt;mac-address&gt; [repeat &lt;repeat-num&gt;] [data-tlv-length &lt;length-val&gt;]</code></td>
<td>• MAC address is in the format <code>&lt;xx-xx-xx-xx-xx-xx&gt;</code></td>
</tr>
<tr>
<td>MAC address</td>
<td></td>
<td>• Allowed range of <code>repeat-num</code> is 1–50</td>
</tr>
<tr>
<td>Specifying remote MEP by</td>
<td><code>lbm remote-mep &lt;mep-id&gt; [repeat &lt;repeat-num&gt;] [data-tlv-length &lt;length-val&gt;]</code></td>
<td>• Allowed range of <code>data-tlv-length</code> is 0–1900.</td>
</tr>
<tr>
<td>MEP ID</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sending LBM messages to</td>
<td><code>lbm multicast [repeat &lt;repeat-num&gt;]</code></td>
<td></td>
</tr>
<tr>
<td>default multicast MAC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>address</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Checking OAM loopback</td>
<td><code>show lbm-results</code></td>
<td></td>
</tr>
<tr>
<td>results</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Performing OAM Link Trace

This diagnostic utility traces the OAM route to the destination, specified either by the MAC address or the maintenance end point (MEP).

**Note**

The option to specify the destination MEP ID is available only if ETX-203A can resolve at least one remote MEP MAC address.

➤ To run an OAM link trace:

- At the `config>oam>cfm>md(<mdid>)>ma(<maid>)>mep(<mepid>)#` prompt, enter all necessary commands according to the tasks listed below.
### Specifying remote MEP by MAC address

**Command:**
```
linktrace address <mac-address> [ttl <ttl-value>]
```

**Comments:**
- MAC address is in the format `<xx-xx-xx-xx-xx-xx>`
- Allowed range for `ttl-value` is 1–64. This parameter specifies the number of hops. Each unit in the link trace decrements the TTL until it reaches 0, which terminates the link trace.

### Specifying remote MEP by ID

**Command:**
```
linktrace remote-mep <mep-id> [ttl <ttl-value>]
```

### Checking the OAM link trace results

**Command:**
```
show linktrace-results
```

---

## OAM EFM

This section covers the monitoring of the Ethernet links using OAM EFM (OAM Ethernet at the First Mile).

ETX-203A can act as the active or passive side in an IEEE 802.3-2005 application.

When link OAM (EFM) is enabled for a port, you can view its status by displaying the port status (`show status`). You can also display the OAM (EFM) parameters and OAM (EFM) statistics.

### Standards

IEEE 802.3-2005

### Benefits

Ethernet OAM (EFM) provides remote management and fault indication for the Ethernet links. Remote link failure can be detected via OAM (EFM).

### Functional Description

The OAM (EFM) discovery process allows a local data terminating entity (DTE) to detect Ethernet OAM capabilities on a remote DTE. Once Ethernet OAM support is detected, both ends of the link exchange state and configuration information, such as mode, PDU size, loopback support, etc. If both DTEs are satisfied with the settings, OAM is enabled on the link. However, the loss of a link or a failure to receive OAMPDUs for five seconds may cause the discovery process to restart.

DTEs may either be in active or passive mode. DTEs in active mode initiate the ETH-OAM (EFM) communications and can issue queries and commands to a remote device. DTEs in passive mode generally wait for the peer device to initiate OAM communications and respond to commands and queries, but do not initiate them.

A flag in the OAMPDU allows an OAM entity to convey the failure condition Link Fault to its peer. Link Fault refers to the loss of signal detected by the receiver; A Link Fault report is sent once per second with the Information OAMPDU.
Factory Defaults
By default, OAM EFM is not enabled for the Ethernet or logical MAC ports.
By default OAM EFM descriptor 1 is configured as passive.

Configuring OAM EFM
There are two available OAM EFM descriptors. Each can be configured to indicate active or passive OAM EFM.

To configure OAM EFM descriptor:
1. Navigate to configure oam efm.
   The config>oam>efm# prompt is displayed.
2. Enter:
   descriptor <number> {active | passive}.

To configure link OAM (EFM) for Ethernet and logical MAC ports:
1. Navigate to configure port ethernet <port-num> or configure port logical-mac <port-num>, respectively.
   The prompt config>port>eth(<port-num>)# or config>port>log-mac(<port-num>)# is displayed.
2. Enter all necessary commands according to the tasks listed below.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabling link OAM (EFM)</td>
<td>efm descriptor &lt;1–2&gt;</td>
<td>The EFM descriptor must exist before you can assign it to a port</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note: In order for link OAM (EFM) to function properly, the relevant</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ethernet port must be associated with an L2CP profile that specifies</td>
</tr>
<tr>
<td></td>
<td></td>
<td>peer action for MAC 0x02.</td>
</tr>
<tr>
<td>Disabling link OAM (EFM)</td>
<td>no efm</td>
<td></td>
</tr>
<tr>
<td>Displaying link OAM (EFM)</td>
<td>show oam-efm</td>
<td>Note: Relevant only for Ethernet ports, if link OAM (EFM) is enabled.</td>
</tr>
<tr>
<td>parameters</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Displaying link OAM (EFM)</td>
<td>show oam-efm-statistics</td>
<td>Note: Relevant only for Ethernet ports, if link OAM (EFM) is enabled.</td>
</tr>
<tr>
<td>statistics</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Commands in level config&gt;port ethernet &lt;port-num&gt; efm or config&gt;port&gt;log-mac(&lt;port-num&gt;) efm</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enabling loopback</td>
<td>loopback</td>
<td>Type no loopback to disable loopback</td>
</tr>
<tr>
<td>Enabling SNMP tunneling for OAM EFM</td>
<td>snmp-tunneling</td>
<td>Type no snmp-tunneling to disable loopback</td>
</tr>
</tbody>
</table>
Example

To enable active link OAM (EFM) for Ethernet port 1 and display the status:

```
ETX-203A# configure oam efm
ETX-203A>config>oam>efm# descriptor 2 active
ETX-203A>config>oam>efm# exit all
ETX-203A# configure port ethernet 1
ETX-203A>config>port>eth(1)# efm descriptor 2
ETX-203A>config>port>eth(1)>efm# exit
ETX-203A>config>port>eth(1)# show oam-efm

Administrative Status : Enabled
Operational Status    : Link Fault
Loopback Status       : Off

Information
-----------------------------------------------
| Local | Remote |
-----------------------------------------------
| Mode  | Active |
| MAC Address | 00-20-D2-30-CC-9D |
| Unidirectional | Not Supported |
| Vars Retrieval | Supported |
| Link Events     | Supported |
| Loopback        | Supported |
| PDU Size        | 1518 |
| Vendor OUI      | 0x0020D2 |
```

ETX-203A>config>port>eth(1)#

5.28 Fault Propagation

Fault propagation enables you to specify which interfaces to shut down if link failure occurs.

Standards

IEEE 802.1ag-D8
ITU-T Y.1731

Benefits

You can ensure that you are sending packets via links that have not failed. Failures are propagated end-to-end via OAM CFM messages.

Functional Description

In the network-to-user or user-to-network direction, if a link fails for which fault propagation is enabled, the corresponding port shuts down or OAM CFM failure message is sent, thus signaling the connected CPE to stop forwarding frames through the link.
You can enable fault propagation to be triggered by failure detection on a network/user interface, which causes a user-configurable action (such as deactivation or OAM CFM failure message sent) to be performed on a user/network interface. You can enable fault propagation in the network-to-user or user-to-network direction, for a pair of interfaces such as Ethernet ports, MEPs, and ETPs.

You can define the following when you enable fault propagation for a pair of interfaces:

- **Trigger:**
  - If interface where failure is detected is Ethernet port or MEP:
    - LOS – Link down detected
  - If interface where failure is detected is MEP:
    - OAM CFM LOC – Loss of continuity detected
    - OAM CFM RDI – Remote defect indication detected
    - OAM CFM Interface status TLV – Remote port failure detected
- **Action to take when fault propagation is triggered:**
  - If interface where action is performed is Ethernet port:
    - Interface-deactivation
  - If interface where action is performed is MEP:
    - Send OAM CFM interface status TLV to indicate failure.
- **Wait-to-restore time** – The time period before enabling the shut-down interface or ceasing to send OAM CFM interface status once the failed interface has been restored.

**Factory Defaults**

By default, no fault propagation is configured. When you configure fault propagation for a particular interface pair, the default configuration is as follows:

- No trigger defined for fault detection
- No action defined to be performed when fault is detected
- Wait-to-restore time = 0.

**Configuring Fault Propagation**

Follow this procedure to configure fault propagation:

1. Add a fault propagation entry for a pair of interfaces
2. Configure the fault propagation parameters for the entry:
   a. Specify the trigger(s)
   b. Specify the action
   c. Specify the wait-to-restore time if you do not want the default value 0.
Adding Fault Propagation Entry

To add fault propagation for a pair of interfaces:

1. Navigate to `configure fault`.
2. Type the command:
   `fault-propagation <from-interface> to <to-interface>` and enter the desired interfaces, as shown in Table 5-18.

   A prompt is displayed:
   `config>fault>fp(<from-interface>/to/<to-interface>)$`.
3. Configure the fault propagation parameters as needed (refer to Configuring Fault Propagation Parameters).

### Table 5-18. Fault Propagation Command Options

<table>
<thead>
<tr>
<th>From Interface</th>
<th>To Interface</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>MEP</td>
<td>Ethernet port</td>
<td>fault-propagation mep &lt;md-id&gt; &lt;ma-id&gt; &lt;mep-id&gt; to port ethernet &lt;port&gt;</td>
</tr>
<tr>
<td>ETP</td>
<td>Ethernet port</td>
<td>fault-propagation etp &lt;etp-name&gt; to port ethernet &lt;port&gt;</td>
</tr>
<tr>
<td>Ethernet port</td>
<td>MEP</td>
<td>fault-propagation port ethernet &lt;port&gt; to mep &lt;to-mdid&gt; &lt;to-maid&gt; &lt;to-mepid&gt;</td>
</tr>
<tr>
<td>ETP</td>
<td>MEP</td>
<td>fault-propagation etp &lt;etp-name&gt; to mep &lt;to-mdid&gt; &lt;to-maid&gt; &lt;to-mepid&gt;</td>
</tr>
<tr>
<td>MEP</td>
<td>MEP</td>
<td>fault-propagation mep &lt;md-id&gt; &lt;ma-id&gt; &lt;mep-id&gt; to mep &lt;to-mdid&gt; &lt;to-maid&gt; &lt;to-mepid&gt;</td>
</tr>
<tr>
<td>Ethernet port</td>
<td>Ethernet port</td>
<td>fault-propagation port ethernet &lt;port&gt; to port ethernet &lt;port&gt;</td>
</tr>
</tbody>
</table>

Configuring Fault Propagation Parameters

To configure fault propagation parameters:

1. Navigate to `configure fault fault-propagation <from-interface> to <to-interface>` to select the fault propagation entry to configure.

   A prompt is displayed:
   `config>fault>fp(<from-interface>/to/<to-interface>)#`
2. Enter all necessary commands according to the tasks listed below.

### Configuring Fault Propagation Parameters

#### Specifying the trigger(s)

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
</table>
| Specifying the trigger(s) | trigger { los | oam-cfm-loc | oam-cfm-rdi | oam-cfm-if-status-tlv } | Typing `no` before the command removes the specified trigger.  
**Note:** The `los` trigger is allowed only if the from-interface is an Ethernet port or ETP. The OAM CFM triggers are allowed only if the from-interface is a MEP. |
### Task

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifying the action to take when fault propagation is triggered</td>
<td>action-on-group { interface-deactivation</td>
<td>Typing <code>no action-on-group</code> removes the action</td>
</tr>
<tr>
<td></td>
<td>oam-cfm-if-status-tlv }</td>
<td><strong>Note</strong>: The <code>interface-deactivation</code> action is allowed only if the to-interface is an Ethernet port. The <code>oam-cfm-if-status-tlv</code> action is allowed only if the to-interface is a MEP.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Specifying the wait-to-restore time</td>
<td>wait-to-restore (&lt;seconds&gt;)</td>
<td>The range is 0–3600</td>
</tr>
</tbody>
</table>

### Example

- **To enable fault propagation:**
  - From Ethernet port 4
  - To MEP 3 in maintenance association 3 in maintenance domain 2 (this example assumes the MEP has been created)
  - Trigger: LOS
  - Action: Send OAM CFM interface status TLV
  - Wait-to-restore time = 120 seconds.

```
ETX-203A# config fault
ETX-203A>config>fault# fault-propagation port ethernet 4 to mep 2 3 3
ETX-203A>config>fault>fp(port/ethernet/4/to/mep/2/3/3)$ trigger los
ETX-203A>config>fault>fp(port/ethernet/4/to/mep/2/3/3)$ action-on-group oam-cfm-if-status-tlv
ETX-203A>config>fault>fp(port/ethernet/4/to/mep/2/3/3)$ wait-to-restore 120
ETX-203A>config>fault>fp(port/ethernet/4/to/mep/2/3/3)$ info detail
  action-on-group oam-cfm-if-status-tlv
  trigger los
  no trigger oam-cfm-loc
  no trigger oam-cfm-if-status-tlv
  no trigger oam-cfm-rdi
  wait-to-restore 120
ETX-203A>config>fault>fp(port/ethernet/4/to/mep/2/3/3)$
```

- **To enable fault propagation:**
  - From Ethernet port 1
  - To Ethernet port 3
  - Trigger: LOS
  - Action: Shut down Ethernet port
  - Wait-to-restore time = 90 seconds.
For enabling fault propagation:

1. Navigate to configure fault.
2. Type the command: `no fault-propagation <from-interface> to <to-interface>` to select the interfaces for which to disable fault propagation.
The specified fault propagation is disabled.

5.29 Date and Time

You can set the date and time for the ETX-203A internal real-time clock or receive the NTP server clock signal.

Setting the Date and Time

➢ To set the system date and time:

1. Navigate to `configure system date-and-time`.

   The `config>system>date-time#` prompt is displayed.

2. Enter all necessary commands according to the tasks listed below.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifying the desired date format</td>
<td>date-format {yyyy-mm-dd</td>
<td>dd-mm-yyyy</td>
</tr>
<tr>
<td>Defining the date</td>
<td>date &lt;date&gt;</td>
<td>Date is according to the configured date format</td>
</tr>
<tr>
<td>Defining the time zone relative to Greenwich main time (GMT)</td>
<td>zone gmt [&lt;([+</td>
<td>-]&lt;hh&gt;:&lt;mm&gt;]&gt;</td>
</tr>
<tr>
<td>Defining the time</td>
<td>time <a href="">hh:mm[:ss]</a></td>
<td></td>
</tr>
</tbody>
</table>

Example

➢ To set the date and time:

   • Format = mm-dd-yyyy
   • Date = May 17, 2011
   • Time = 5:40pm
   • Zone = GMT –4 hours and 30 minutes.

   ```bash
   ETX-203A#configure system date-and-time
   ETX-203A>config>system>date-time# date-format mm-dd-yyyy
   ETX-203A>config>system>date-time# date 05-17-2011
   ETX-203A>config>system>date-time# time 17:40
   ETX-203A>config>system>date-time# zone gmt -04:30
   ETX-203A>config>system>date-time#
   ```

Displaying the Date and Time

➢ To display the date and time:

   • From the system context `(config>system)`, enter:
     `show time`.
Working with SNTP

This section explains how to receive the clock signal from NTP servers in the network. ETX-203A can synchronize with up to ten servers, sending NTP requests to the servers at user-defined intervals.

You can set one of the active SNTP servers as the preferred server, so that ETX-203A sends NTP requests to the preferred server. If there is no preferred server or if the preferred server does not answer, then ETX-203A sends NTP requests to any enabled servers.

Factory Defaults

The default configuration of the SNTP parameters is:

- No SNTP servers defined
- Polling interval set to 15 minutes.

When an SNTP server is defined, its default configuration is:

- IP address set to 0.0.0.0
- Not preferred
- Administratively disabled (shutdown).

Configuring SNTP Parameters

To configure SNTP parameters:

1. Navigate to `config system date-and-time sntp`.
   
   The `config>system>date-time>sntp#` prompt is displayed.

2. Enter all necessary commands according to the tasks listed below.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabling ETX-203A to listen to NTP broadcast messages to obtain accurate timestamps</td>
<td>broadcast</td>
<td>Type <code>no broadcast</code> to disable broadcast mode.</td>
</tr>
<tr>
<td>Setting polling interval (in minutes) for SNTP requests</td>
<td><code>poll-interval interval &lt;minutes&gt;</code></td>
<td>Allowed range is 1–1440</td>
</tr>
<tr>
<td>Defining and configuring SNTP servers (refer to Defining SNTP Servers and Configuring SNTP Server Parameters)</td>
<td><code>server &lt;server-id&gt;</code></td>
<td></td>
</tr>
<tr>
<td>Displaying SNTP status</td>
<td><code>show status</code></td>
<td></td>
</tr>
</tbody>
</table>

Defining SNTP Servers

To define an SNTP server:

1. Navigate to `config system date-and-time sntp`.
   
   The `config>system>date-time>sntp#` prompt is displayed.

2. Type `server <server-id>` to define an SNTP server with ID `<server-id>`.
The following prompt is displayed: `config>system>date-time>sntp>server<server-id>$. The SNTP server parameters are configured by default as described in Factory Default.

3. Configure the SNTP server parameters as needed, as described in Configuring SNTP Server Parameters.

Configuring SNTP Server Parameters

To configure SNTP server parameters:

1. Navigate to `config system date-and-time sntp`.
   
   The `config>system>date-time>sntp#` prompt is displayed.

2. Type `server <server-id>` to select the SNTP server to configure.
   
   The following prompt is displayed: `config>system>date-time>sntp>server<server-id>#`.

3. Enter all necessary commands according to the tasks listed below.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting the IP address of the server</td>
<td><code>address &lt;IP-address&gt;</code></td>
<td></td>
</tr>
<tr>
<td>Set SNTP server as preferred server.</td>
<td><code>prefer</code></td>
<td>Type <code>no prefer</code> to remove preference</td>
</tr>
<tr>
<td></td>
<td></td>
<td><em>Note: Only one server can be preferred.</em></td>
</tr>
<tr>
<td>Setting UDP port for NTP requests, to a specific UDP port or to default UDP port (123)</td>
<td><code>udp port &lt;udp-port&gt;</code></td>
<td>Allowed range is 1–65535</td>
</tr>
<tr>
<td></td>
<td><code>udp default</code></td>
<td></td>
</tr>
<tr>
<td>Administratively enabling server</td>
<td><code>no shutdown</code></td>
<td>Using <code>shutdown</code> disables the server</td>
</tr>
<tr>
<td>Sending query to server and displaying result</td>
<td><code>query-server</code></td>
<td></td>
</tr>
</tbody>
</table>

Example

To define SNTP server:

- Server ID = 1
- IP address = 192.1.1.1
- Preferred
- Administratively enabled.
5.30 Syslog

ETX-203A uses the Syslog protocol to generate and transport event notification messages over IP networks to Syslog servers. The Syslog operation is compliant with the RFC 3164 requirements.

Configuring Syslog Parameters

To configure syslog parameters:

1. Navigate to the system context (`config>system`).
2. Define syslog device parameters:
   a. Enter:
      
      ```
      syslog device
      ```
      The system switches to the syslog device context (`config>system>syslog(device)`)
   b. Specify the module, task, or function from which syslog messages are sent:
      
      ```
      facility {local1 | local2 | local3 | local4 | local5 | local6 | local7}
      ```
      Default: local1
   c. Specify the UDP port that transmits syslog messages (allowed only if syslog message transmitting is administratively disabled):
      
      ```
      port <udp-port-number>
      ```
d. Specify the severity level. The log messages that contain severity level up to the specified level are transmitted:

\[
\text{severity-level } \{\text{critical | major | minor | warning | event | info | debug}\}
\]

e. Administratively enable the transmitting of syslog messages:

\[
\text{no shutdown}
\]

3. Define syslog server parameters:
   a. Specify the syslog server to receive syslog messages, from 1 to 5:

   \[
   \text{syslog server <server-id>}
   \]

   The system switches to the context of the specified syslog server
   \((\text{config>system>syslog(server <server-ID>))}).\)

   b. Specify the IP address of the server (allowed only if the server is administratively disabled):

   \[
   \text{address } <0.0.0.0–255.255.255.255>
   \]

   c. Specify the UDP port on the server that receives syslog messages (allowed only if the server is administratively disabled):

   \[
   \text{port } <\text{udp-port-number}>
   \]

   Allowed values: 1–65535

d. Administratively enable the server (allowed only if IP address is not 0.0.0.0):

\[
\text{no shutdown}
\]
e. Enter \text{exit} to exit the server context.

The system switches to the system context \((\text{config>system})\).

### Displaying Syslog Statistics

To display syslog statistics:

1. At the system context \((\text{config>system})\), enter:

\[
\text{syslog device}
\]

   The system switches to the syslog device context
   \((\text{config>system>syslog(device)})\)

2. Enter:

\[
\text{show statistics}
\]

3. Syslog statistics appear as shown below. The counters are described in \text{Table 5-19}.\n
   \[
   \begin{tabular}{|l|l|}
   \hline
   \text{ETX-203A>config>system>syslog(device)# show statistics} & \text{Total Tx Messages} : 356 \\
   & \text{Non-queued Dropped Messages} : 265 \\
   \hline
   \end{tabular}
   \]

4. To clear the statistics, enter:

\[
\text{clear-statistics}
\]
Table 5-19. Syslog Statistic Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Tx Messages</td>
<td>The total number of syslog messages transmitted</td>
</tr>
<tr>
<td>Non-queued Dropped Messages</td>
<td>The total number of syslog messages that were dropped before being queued</td>
</tr>
</tbody>
</table>

5.31 Administration

Clearing Device Statistics

You can clear the statistics for Ethernet ports, flows, and OAM services.

➢ To clear the statistics:
  - At the device prompt, enter: `clear-statistics`.
    The statistics for Ethernet ports, flows, and OAM services are cleared.

Working with the Inventory

The ETX-203A inventory table displays the unit’s components, hardware and software revisions, and power supply types. You can display an inventory table that shows all installed components, and you can display more detailed information for each component. You can configure an alias name, asset ID, and serial number for inventory components.

Standards and MIBs

The inventory feature is implemented according to RFC 4133 – Entity MIB (RFC 2737 was made obsolete by RFC 4133 version 3).

Benefits

You can monitor the installed components and hardware/software revisions.

Displaying Inventory Information

➢ To display the inventory table:
  - At the config>system# prompt, enter: `show inventory-table`.
    The inventory table is displayed (refer to Example to see a typical inventory table output).

You can display more information for each installed inventory component. To do so, you need to enter the inventory level with the corresponding inventory component index, which is determined by the position of the corresponding row
in the output of `show inventory-table`, therefore it changes according to what is installed in the unit.

> **To display the inventory component information:**

1. Navigate to `configure system inventory <index>.

2. Enter: `show status`.

Information for the corresponding inventory component is displayed (refer to Table 5-20 for information on the parameters).

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Description of component type, in the form: <code>RAD.&lt;device-name&gt;.&lt;Physical Class&gt;</code>, e.g. <code>RAD.ETX-203A.Port</code></td>
</tr>
<tr>
<td>Contained In</td>
<td>Index of the component that contains the component for which information is being displayed. This is 0 for the chassis, as it is not contained in any component, and 1 for all other components, as they are all contained in the chassis.</td>
</tr>
<tr>
<td>Physical Class</td>
<td>Class of component</td>
</tr>
<tr>
<td></td>
<td>Possible values: Chassis, CPU, Power Supply, Port</td>
</tr>
<tr>
<td>Relative Position</td>
<td>Contains the relative position of this component among other similar components (with the exception of the relative positions for the chassis, management Ethernet port, and clock port). Possible values for the various component types: Chassis – 4294967295, CPU – 1, Power Supply – 1, Network Port – 1 or 2, User Port – 3, 4, Management Ethernet – 101</td>
</tr>
<tr>
<td>Name</td>
<td>Name of component</td>
</tr>
<tr>
<td></td>
<td>Possible values (according to component type): <code>&lt;device-name&gt;</code> – Chassis, CPU, Power Supply, Network Port <code>&lt;n&gt;</code>, User Port <code>&lt;n&gt;</code>, Management Ethernet</td>
</tr>
<tr>
<td>HW Rev</td>
<td>Hardware revision (relevant only for chassis)</td>
</tr>
<tr>
<td>SW Rev</td>
<td>Software revision (relevant only for chassis)</td>
</tr>
<tr>
<td>FW Rev</td>
<td>Firmware revision (relevant only for chassis)</td>
</tr>
<tr>
<td>Serial No.</td>
<td>Serial number (blank if unknown for component)</td>
</tr>
<tr>
<td>MFG Name</td>
<td>Manufacturer name (blank if unknown for component)</td>
</tr>
<tr>
<td>Model Name</td>
<td>Model name (blank if unknown for component)</td>
</tr>
<tr>
<td>Alias</td>
<td>Alias name for component</td>
</tr>
<tr>
<td>Asset ID</td>
<td>Identification information for component</td>
</tr>
</tbody>
</table>
### Parameter Description

**FRU**
Indicates whether this component is a field replaceable unit that can be replaced on site.

For ETX-203A this is normally true only for the chassis.

### Setting Administrative Inventory Information

If necessary, you can configure the alias, asset ID, and serial number for inventory components. To configure the information, you need to enter the `inventory` level with the corresponding inventory component index as determined by the position of the corresponding row in the output of `show inventory-table`.

➢ **To set inventory component information:**

1. Navigate to `configure system inventory <index>`.

   The `config>system>inventor(<index>)#` prompt is displayed.

2. Enter all necessary commands according to the tasks listed below.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assigning user-defined alias to component</td>
<td><code>alias &lt;string&gt;</code></td>
<td>Using <code>no</code> before <code>alias</code> removes the alias.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> Configuring the alias is meaningful only for the chassis component. It can be used by a network manager as a non-volatile identifier for the device.</td>
</tr>
<tr>
<td>Assigning user-specific asset identifier to the component (usually for removable physical components)</td>
<td><code>asset-id &lt;id&gt;</code></td>
<td>Using <code>no</code> before <code>asset-id</code> removes the asset ID.</td>
</tr>
<tr>
<td>Assigning vendor-specific serial number to the component</td>
<td><code>serial-number &lt;string&gt;</code></td>
<td>Using <code>no</code> before <code>serial-number</code> removes the serial number.</td>
</tr>
</tbody>
</table>

### Example

➢ **To display the following inventory information:**

- Inventory table
- Inventory information for the following components:
  - Chassis
  - Power Supply
  - User Port 1.
ETX-203A# configure system
ETX-203A# config>system# show inventory-table

<table>
<thead>
<tr>
<th>Physical Class</th>
<th>Name</th>
<th>HW Rev</th>
<th>SW Rev</th>
<th>FW Rev</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chassis</td>
<td>ETX-203A – Chass</td>
<td>2.00</td>
<td>3.00</td>
<td>1.3.0.0.0.0.1.24</td>
</tr>
<tr>
<td>Power Supply</td>
<td>Power Supply</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port</td>
<td>Network Port 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port</td>
<td>Network Port 2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port</td>
<td>User Port 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port</td>
<td>User Port 2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port</td>
<td>Management Ethernet</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

ETX-203A>config>system# inventory 1
ETX-203A>config>system>inventor(1)# show status
Description : RAD.ETX-203A.Chassis
Contained In : 0
Physical Class : Chassis
Relative Position : 4294967295
Name : ETX-203A – Chassis
HW Rev : 2.00
SW Rev : 3.00
FW Rev : 1.3.0.0.0.0.1.24
Serial Number : 00-20-D2-30-CC-9D
MFG Name : RAD
Model Name : 
Alias : 
Asset ID : 
FRU : True

ETX-203A>config>system>inventor(1)# exit
ETX-203A>config>system# inventory 3
ETX-203A>config>system>inventor(3)# show status
Description : RAD.ETX-203A.Power Supply
Contained In : 1
Physical Class : Power Supply
Relative Position : 1
Name : Power Supply
HW Rev : 
SW Rev : 
FW Rev : 
Serial Number : 
MFG Name : RAD
Model Name : 
Alias : 
Asset ID : 
FRU : False

ETX-203A>config>system>inventor(3)# exit
ETX-203A>config>system# inventory 6
ETX-203A>config>system>inventor(6)# show status
Description       : RAD.ETX-203A.Port
Contained In      : 1
Physical Class    : Port
Relative Position : 3
Name              : User Port 1
HW Rev            :
SW Rev            :
FW Rev            :
Serial Number     :
MFG Name          :
Model Name        :
Alias             :
Asset ID          :
FRU               : False

ETX-203A>config>system>inventor(6)# exit
ETX-203A>config>system#

▶ To set the chassis alias to “ETX-test-unit“:
ETX-203A# configure system
ETX-203A>config>system# inventory 1
ETX-203A>config>system>inventor(1)# alias ETX-test-unit
ETX-203A>config>system>inventor(1) show status
Description       : RAD.ETX-203A.Chassis
Contained In      : 0
Physical Class    : Chassis
Relative Position : 4294967295
Name              : ETX-203A - Chassis
HW Rev            : 2.00
SW Rev            : 3.00
FW Rev            : 1.3.0.0.0.0.1.24
Serial Number     : 00-20-D2-30-CC-9D
MFG Name          : RAD
Model Name        :
Alias             : ETX-test-unit
Asset ID          :
FRU               : True

ETX-203A>config>system>inventor(1)# exit

Displaying Environment

You can display information about the type and status of the power supplies, and the status of the fans.

▶ To display the information:
1. Navigate to configure chassis.
   
   The config>chassis# prompt is displayed.

2. Enter:
   
   show environment.
The information is displayed as shown in the example below.
The power supply type is indicated as AC-DC or -- (if it has failed).
The status for the power supply and fan indicates whether the unit is present and functioning properly, or is absent (does not exist), or has failed.

Example

```
ETX-203A# configure chassis
ETX-203A>config>chassis# show environment
Power Supply     Type      Status
----------------------------------------
1          AC-DC       OK
FAN                      Status
-----------------------------------
1                        OK
ETX-203A>config>chassis#
```

Displaying Software Versions

You can display the active, main, and backup software file versions, dates, and times.

➢ To display the versions:
  • At the file# prompt enter: `show version`.

Example

```
ETX-203A# file
ETX-203A>file# show version
Active  : 3.00  06/01/2011 15:41:46
Main    : 3.00  06/01/2011 15:41:46
Backup  : 3.00d01 21/07/2009 22:19:34
ETX-203A>file#
```

Displaying CPU and Memory Utilization

You can view the CPU and memory buffer usage. Refer to Table 5-21 for a description of the memory buffers.

➢ To display CPU usage:
  • From the system context `config>system`, enter: `show cpu-utilization`.
    The CPU usage is displayed.
ETX-203A>config>system# show cpu-utilization
CPU Utilization

<table>
<thead>
<tr>
<th>Min (%)</th>
<th>Cur (%)</th>
<th>Max (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>26</td>
<td>26</td>
<td>66</td>
</tr>
</tbody>
</table>

ETX-203A>config>system#

To display memory buffer usage:

- From the system context (`config>system`), enter:
  `show buffers`.

The memory buffer usage is displayed.

```
ETX-203A>config>system# show buffers
Pool Name Size (Bytes) Total Buffers Free Buffers Alloc. Failures Free Failures
-----------------------------------------------------------------------------
VLAN  64   100  99   0      0
Huge 8192  100 100   0      0
Large 2048 1000 796   0      0
Medium 512 4000 3975  0      0
Small  64  4000 3979  0      0
Queue 16  8000 8000  0      0
```

---

**Figure 5-12. CPU Usage**

**Figure 5-13. Memory Buffer Usage**

**Table 5-21. Memory Buffers**

<table>
<thead>
<tr>
<th>Buffer</th>
<th>Size</th>
<th>Total Buffers Available</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN</td>
<td>64</td>
<td>100</td>
<td>Unused, except three of the buffers are used for internal functions</td>
</tr>
<tr>
<td>Huge</td>
<td>8192</td>
<td>100</td>
<td>Unused</td>
</tr>
<tr>
<td>Large</td>
<td>2048</td>
<td>1000</td>
<td>OAM CFM and OAM EFM</td>
</tr>
<tr>
<td>Medium</td>
<td>512</td>
<td>4000</td>
<td>Event log and traps</td>
</tr>
<tr>
<td>Small</td>
<td>64</td>
<td>4000</td>
<td>Management traffic</td>
</tr>
<tr>
<td>Queue</td>
<td>16</td>
<td>8000</td>
<td>Application task messages</td>
</tr>
</tbody>
</table>

---

**File Operations**

You can perform the following operations:

- Transfer files via SFTP
- Copy files within the ETX-203A unit
- Display files
- Delete files
- Swap files.

You can copy files via the `copy` command, or via the commands shown in **Table 5-22**. As shown in the table, some commands that reset the device also erase the saved user configuration by copying another file to it before the reset.
### Downloading/Uploading Files

You can download or upload files to the ETX-203A unit via SFTP. Normally the types of files copied are configuration files and software files.

The software files can also be downloaded to ETX-203A via the Boot Manager, using XMODEM or TFTP. For details on upgrading the device software, refer to Chapter 7.

**Note**

TFTP is available only when downloading a software image via the Boot Manager. When you copy files with the `copy` command, you have to use SFTP.

### SFTP Application

The SFTP protocol is used to provide secure file transfers via the product’s Ethernet interface. SFTP is a version of FTP that encrypts commands and data transfers, keeping your data secure and your session private. For SFTP file transfers, an SFTP server application must be installed on the local or remote computer.

A variety of third-party applications offer SFTP server software. For more information, refer to the documentation of these applications.

![Application file is transferred to ETX-203A](image)

**Figure 5-14. Downloading a Software Application File via SFTP**

### Setting up SFTP Server

If you use a local laptop and SFTP is the preferred transfer method, a SFTP server application must be installed on it.

As mentioned above, third-party applications are available and you should refer to their setup documentation.

### Checking the Firewall Settings

SFTP file transfers are carried out through TCP port 22. You should check that the firewall you are using on the server computer allows communication through this port.
To allow communication through port 22 in Windows XP:

1. Double-click the **My Network Places** icon, located on the desktop.
   
   The My Network Places window appears.

2. On the Network Tasks sidebar, click **View network connections**.
   
   The available network connections are displayed.

3. On the Network Tasks sidebar, click **Change Windows Firewall settings**.
   
   The Windows Firewall dialog box appears.

4. Click the **Exceptions** tab.
5. Check whether port 22 appears on the exceptions list. If it does not, click Add Port and add it to the list of exceptions.

**Note**  
Different firewall types require different configuration. Refer to your firewall’s documentation to check how SFTP file transfers can be allowed to pass through it using TCP port 22.

### Using CLI to Download/Upload Files

You use the `copy` command in the `file` context to download/upload files.

➢ To download a file via SFTP:
  - At the `file#` prompt, enter:
    ```
copy sftp://<user>:<password>@<sftp-server-ip-addr>/<source-file> <destination-file>.
```

**Example – Download via SFTP**

- SFTP server address – 192.20.20.20
- SFTP user name – admin
• SFTP password – 1234
• Source file name – ETX-203A.img
• Destination file name – ETX-203A.img.

ETX-203A# file
ETX-203A>file# copy sftp://<admin>:<1234>@192.20.20.20/ETX-203A.img ETX-203A.img

➢ To upload a file via SFTP:
  • At the file# prompt, enter:
    `copy <source-file>
    sftp://<user>:<password>@<sftp-server-ip-addr>/<dest-file>.

Example – Upload via SFTP
• SFTP server address – 192.20.20.20
• SFTP user name – admin
• SFTP password – 1234
• Source file name – db1conf.log
• Destination file name – db1conf.cfg.

ETX-203A# file
ETX-203A>file# copy db1conf.log
sftp://<admin>:<1234>@192.20.20.20/db1conf.cfg

Copying Files Within Device
You can copy files within the ETX-203A unit with the copy command.

➢ To copy files within the device:
  • At the file# prompt, enter:
    `copy <source-file> <dest-file>.

Example
• Source file name – running-config
• Destination file name – startup-config.

ETX-203A# file
ETX-203A>file# copy running-config startup-config

Displaying Files Within Device
The `dir` command is used to display the files within the device.

➢ To display the files within the device:
  • At the file# prompt, enter: `dir`.

    A list of the file names and types is displayed.
Example

```
ETX-203A# file
ETX-203A>file# dir
Type           Name
------------------------------------------------------------
Software       backup-sw
Software       main-sw
Configuration  factory-default
Configuration  startup-config
Configuration  user-default-config
Event Log      logfile
```

Swapping Files

You can swap files, via SFTP or locally.

➢ To swap the files:
  • At the file# prompt, enter the swap command in one of the following forms, according to where the files are located.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Swap &lt;file1&gt; from SFTP server with &lt;file2&gt; located on device</td>
<td>swap sftp://&lt;user&gt;:&lt;password&gt;@&lt;sftp-server-ip-addr&gt;/&lt;file1&gt; &lt;file2&gt;</td>
</tr>
<tr>
<td>Swap &lt;file1&gt; located on device with &lt;file2&gt; from SFTP server</td>
<td>swap &lt;file1&gt; sftp://&lt;user&gt;:&lt;password&gt;@&lt;sftp-server-ip-addr&gt;/&lt;file2&gt;</td>
</tr>
<tr>
<td>Swap &lt;file1&gt; located on device with &lt;file2&gt; located on device</td>
<td>swap &lt;file1&gt; &lt;file2&gt;</td>
</tr>
</tbody>
</table>

Deleting Files

You can delete files. Before deleting the file, make sure the file is not in use.

➢ To delete a file:
  1. At the file# prompt, enter:
     ```
     delete <file-name>
     ```
     You are prompted to confirm the deletion.
  2. Confirm the deletion.

Example

```
ETX-203A# file
ETX-203A>file# delete db2conf.cfg
File will be erased. Are you sure?? [yes/no] _yes
```

Saving Configuration

You must save your configuration if you wish to have it available, as it is not saved automatically. You can save your configuration as follows:

• To save the user configuration in startup-config:
• In any level prompt enter: save
• At the file# prompt enter:
  copy running-config startup-config.
• To save the user default configuration in user-default-config, at the file# prompt enter:
  copy running-config user-default-config.

Reset

ETX-203A supports the following types of reset:

• Reset to factory defaults
• Reset to user defaults
• Overall reset (restart) of the device.

Resetting to Factory Defaults

➢ To reset ETX-203A to factory defaults:
  1. At the admin# prompt enter:
     factory-default.
     A confirmation message is displayed:
     Current configuration will be erased and device will
     reboot with factory default configuration. Are you sure??
     [yes/no]
  2. Enter yes to confirm the reset to factory defaults.
     The factory-default file is copied to the startup-config file. The unit
     resets, and after it completes its startup the factory defaults are loaded.

Resetting to User Defaults

➢ To reset ETX-203A to user defaults:
  1. At the admin# prompt enter:
     user-default.
     A confirmation message is displayed:
     Current configuration will be erased and device will
     reboot with user default configuration. Are you sure??
     [yes/no]
  2. Enter yes to confirm the reset to user defaults.
     The user-default-config file is copied to the startup-config file. The unit
     resets, and after it completes its startup the user defaults are loaded.

Restarting the Unit

If necessary, you can restart ETX-203A without interrupting the power supply.
To restart ETX-203A:

1. At the `admin#` prompt enter:
   
   `reboot`.

   A confirmation message is displayed:
   
   `Device will reboot. Are you sure?? [yes/no]`

2. Enter `yes` to confirm the reset.

   The unit restarts.
Chapter 6
Monitoring and Diagnostics

The following are described in this chapter:

- Detecting problems
- Alarms and traps
- Performing diagnostic tests.

6.1 Detecting Problems

The LED indicators indicate errors on the hardware level.

**LEDs**

If an LED is red, that usually indicates there is a problem. Check the port that is associated with the LED to further investigate the problem. Refer to Chapter 3 for a description of the unit LEDs.

**Alarms and Traps**

Alarms serve as notification of a fault in the device, and are indicated by an entry in the event log, and/or an SNMP trap to a management station. Refer to Handling Events for further details on events and traps.

**Statistic Counters**

Statistic counters provide information on possible abnormal behavior and failures. You can collect statistics on the following:

- Ethernet ports
- Flows
- RADIUS server
- OAM CFM.

For further information, refer to the relevant sections in Chapter 5 and the relevant sections in the troubleshooting chart.
### 6.2 Handling Events

An alarm is an indication of a fault in the device. An event is an occurrence in the device that may be a fault or may be a user login, change in port status, etc. Alarms and events are written in the event log. An SNMP trap can be sent to management stations as the result of an alarm/event.

The event log file can hold up to 2048 events (system messages). All events are

---

#### Working with the Event Log

This section explains how to display and clear the event log.

- **To display the event log:**
  1. Navigate to the **system** context.
  2. Display the event log:
     ```
     show event-log
     ```

     To scroll up and down in the list, use the arrow keys. The events are listed in Table 6-3.

- **To clear the event log:**
  - At the **system** context, enter:
    ```
    clear-event-log
    ```

<table>
<thead>
<tr>
<th>System Events</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLI TEXT FILE ERROR: [STARTUP-CONFIG FILE/USER-DEFAULT-CONFIG FILE]</td>
<td>An error occurred while attempting to load the specified configuration file. When this error occurs, the file is deleted and the unit reboots.</td>
</tr>
<tr>
<td>COLD START</td>
<td>The unit has rebooted</td>
</tr>
<tr>
<td>DYING GASP</td>
<td>The unit lost power and sent indication of dying gasp</td>
</tr>
<tr>
<td>FAN {1,2} ON</td>
<td>The specified fan is on</td>
</tr>
<tr>
<td>FAN {1,2} OFF</td>
<td>The specified fan is off</td>
</tr>
<tr>
<td>FATAL ERROR AT MODULE X, LINE X</td>
<td>Fatal error has been detected at the specified location</td>
</tr>
<tr>
<td>INVALID LOGIN VIA (TELNET/TERMINAL)</td>
<td>Invalid user name and/or password has been detected while initializing the Telnet/terminal management session</td>
</tr>
<tr>
<td>LOGIN VIA (TELNET/TERMINAL)</td>
<td>Login has been performed via Telnet/terminal application</td>
</tr>
<tr>
<td>INVALID LOGIN VIA (TELNET/TERMINAL/SSH)</td>
<td>Invalid user name and/or password has been detected while initializing the Telnet/terminal/SSH management session</td>
</tr>
<tr>
<td>LOGIN VIA (TELNET/TERMINAL/SSH)</td>
<td>Login has been performed via Telnet/terminal/SSH application</td>
</tr>
<tr>
<td>POWER SUPPLY {1,2} ON</td>
<td>The specified power supply is on</td>
</tr>
</tbody>
</table>

---

*Table 6-1. Event List*
<table>
<thead>
<tr>
<th>Event Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>POWER SUPPLY [1,2] OFF</td>
<td>The specified power supply is off because it has failed or is absent</td>
</tr>
<tr>
<td>SYSTEM USER RESET</td>
<td>System reset occurred due to user request</td>
</tr>
<tr>
<td>SYSTEM USER RESET</td>
<td>System reset occurred due to user request or as a result of configuration download</td>
</tr>
<tr>
<td>TEMPERATURE XX[°C] IS OK</td>
<td>The internal temperature has returned to the allowed range after being too low or too high</td>
</tr>
<tr>
<td>TEMPERATURE XX[°C] IS TOO HIGH</td>
<td>The internal temperature has risen above the upper allowed threshold</td>
</tr>
<tr>
<td>TEMPERATURE -XX[°C] IS TOO LOW</td>
<td>The internal temperature has fallen below the lower allowed threshold</td>
</tr>
<tr>
<td>File Transfer Events</td>
<td>Description</td>
</tr>
<tr>
<td>IMAGE/CONFIGURATION DOWNLOAD/UPLOAD</td>
<td>SFTP/TFTP session has been initiated for download/upload action with image/configuration file</td>
</tr>
<tr>
<td>DOWNLOAD/UPLOAD OK</td>
<td>SFTP/TFTP download/upload session has successfully completed</td>
</tr>
<tr>
<td>DOWNLOAD/UPLOAD FAILED/FILE REJECTED</td>
<td>SFTP/TFTP session has failed because the download/upload failed or the file was rejected</td>
</tr>
<tr>
<td>Physical Port Events</td>
<td>Description</td>
</tr>
<tr>
<td>LINK DOWN</td>
<td>Network/user Ethernet port has been disconnected</td>
</tr>
<tr>
<td>LINK UP</td>
<td>Network/user Ethernet port has been connected</td>
</tr>
<tr>
<td>LINK ADMIN DOWN</td>
<td>Network/user Ethernet port has been disabled by the user</td>
</tr>
<tr>
<td>SFP INSTALLED PORT X</td>
<td>SFP has been inserted in specified Ethernet port</td>
</tr>
<tr>
<td>SFP REMOVED PORT X</td>
<td>SFP has been removed from specified Ethernet port</td>
</tr>
<tr>
<td>DHCP Events</td>
<td>Description</td>
</tr>
<tr>
<td>IP X.X.X.X ASSIGNED BY SERVER Y.Y.Y.Y</td>
<td>IP address X.X.X.X has been assigned by DHCP server Y.Y.Y.Y</td>
</tr>
<tr>
<td>IP X.X.X.X IS RELEASED</td>
<td>IP address X.X.X.X has been released by ETX-203A</td>
</tr>
<tr>
<td>OAM CFM Events</td>
<td>Description</td>
</tr>
<tr>
<td>OAM CC OK ON</td>
<td>OAM.ag connectivity check (CC) with remote MEP has been confirmed</td>
</tr>
<tr>
<td>OAM CC MISMERGE ON</td>
<td>OAM.ag CC mismerge for remote MEP has been detected</td>
</tr>
<tr>
<td>OAM CC UNEXPECTED MEP ON</td>
<td>OAM.ag CC unexpected MEP for remote MEP has been detected</td>
</tr>
<tr>
<td>OAM CC UNEXPECTED MEP OFF</td>
<td>OAM.ag CC unexpected MEP for remote MEP event has been canceled</td>
</tr>
<tr>
<td>OAM CC UNEXPECTED PERIOD ON</td>
<td>OAM.ag CC unexpected period for remote MEP has been detected</td>
</tr>
<tr>
<td>OAM CC LOSS OF CONTINUITY</td>
<td>OAM.ag CC continuity loss has been detected for remote MEP</td>
</tr>
<tr>
<td>OAM CC RDI DETECTED ON</td>
<td>OAM.ag CC RDI for remote MEP has been detected</td>
</tr>
<tr>
<td>OAM UNEXPECTED MD LEVEL ON</td>
<td>OAM.ag CC unexpected MD level has been detected</td>
</tr>
<tr>
<td>OAM UNEXPECTED MD LEVEL OFF</td>
<td>OAM.ag CC unexpected MD level event has been canceled</td>
</tr>
</tbody>
</table>
### OAM CFM Service Events

<table>
<thead>
<tr>
<th>Event Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FRAMES ABOVE DELAY DROPPED BELOW</td>
<td>Y.1731 Frame Delay Threshold has been reached (dropped below)</td>
</tr>
<tr>
<td>FRAMES ABOVE DELAY EXCEEDED</td>
<td>Y.1731 Frame Delay Threshold has been reached (exceeded)</td>
</tr>
<tr>
<td>FRAMES ABOVE DELAY VARIATION DROPPED BELOW</td>
<td>Y.1731 Frame Delay Variation Threshold has been reached (dropped below)</td>
</tr>
<tr>
<td>FRAMES ABOVE DELAY VARIATION EXCEEDED</td>
<td>Y.1731 Frame Delay Variation Threshold has been reached (exceeded)</td>
</tr>
<tr>
<td>FRAMES LOSS RATIO DROPPED BELOW</td>
<td>Y.1731 Frame Loss Ratio Threshold has been reached (dropped below)</td>
</tr>
<tr>
<td>FRAMES LOSS RATIO EXCEEDED</td>
<td>Y.1731 Frame Loss Ratio Threshold has been reached (exceeded)</td>
</tr>
<tr>
<td>UNAVAILABILITY RATIO DROPPED BELOW</td>
<td>Y.1731 Unavailability Ratio Threshold has been reached (dropped below)</td>
</tr>
<tr>
<td>UNAVAILABILITY RATIO EXCEEDED</td>
<td>Y.1731 Unavailability Ratio Threshold has been reached (exceeded)</td>
</tr>
</tbody>
</table>

### OAM EFM Events

<table>
<thead>
<tr>
<th>Event Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OAM (802.3ah) REMOTE DYING GASP PORT X</td>
<td>Dying gasp indication has been received from the remote partner on OAM link on port X</td>
</tr>
<tr>
<td>OAM (802.3ah) CONNECTIVITY FAIL PORT X ON</td>
<td>OAM connectivity has been lost on port X</td>
</tr>
<tr>
<td>OAM (802.3ah) CONNECTIVITY FAIL PORT X OFF</td>
<td>OAM connectivity has been restored on port X</td>
</tr>
<tr>
<td>OAM (802.3ah) REMOTE LINK FAIL PORT X ON</td>
<td>Indication of OAM connectivity failure has been received from the remote partner on OAM link on port X</td>
</tr>
<tr>
<td>OAM (802.3ah) REMOTE LINK FAIL PORT X OFF</td>
<td>Indication of OAM connectivity recovery has been received from the remote partner on OAM link on port X</td>
</tr>
<tr>
<td>OAM (802.3ah) REMOTE CRITICAL ERRORS PORT X ON</td>
<td>Indication of critical errors has been received from the remote partner on OAM link on port X</td>
</tr>
<tr>
<td>OAM (802.3ah) REMOTE CRITICAL ERRORS PORT X OFF</td>
<td>Indication of critical error termination has been received from the remote partner on OAM link on port X</td>
</tr>
<tr>
<td>OAM (802.3ah) REMOTE LOOPBACK PORT X ON</td>
<td>Indication of remote loopback activation has been received from the remote partner on OAM link on port X</td>
</tr>
<tr>
<td>OAM (802.3ah) REMOTE LOOPBACK PORT X OFF</td>
<td>Indication of remote loopback deactivation has been received from the remote partner on OAM link on port X</td>
</tr>
</tbody>
</table>
## Working with Traps

The traps are listed in the following table.

### Table 6-2. Trap List

<table>
<thead>
<tr>
<th>Trap</th>
<th>Description</th>
<th>OID</th>
<th>Maskable</th>
</tr>
</thead>
<tbody>
<tr>
<td>aqnDyingGaspTrap</td>
<td>A power failure (dying gasp) has occurred</td>
<td>1.3.6.1.4.1.164.6.1.0.36</td>
<td>Yes</td>
</tr>
<tr>
<td>aqnFanFailureTrap</td>
<td>A fan is on or off</td>
<td>1.3.6.1.4.1.164.6.1.0.14</td>
<td>Yes</td>
</tr>
<tr>
<td>aqnPowerFailureTrap</td>
<td>A power failure has occurred or a power supply status has changed</td>
<td>1.3.6.1.4.1.164.6.1.0.13</td>
<td>Yes</td>
</tr>
<tr>
<td>aqnStatusChangeTrap</td>
<td>SNMP agent status has changed</td>
<td>1.3.6.1.4.1.164.6.1.0.2</td>
<td>Yes</td>
</tr>
<tr>
<td>aqnTempThresholdTrap</td>
<td>The device temperature has left the allowed range, or has returned to the allowed range</td>
<td>1.3.6.1.4.1.164.6.1.0.37</td>
<td>Yes</td>
</tr>
<tr>
<td>aqnUploadDataTrap</td>
<td>Data sent to generic Intervals Statistics Collection application</td>
<td>1.3.6.1.4.1.164.6.1.0.11</td>
<td>Yes</td>
</tr>
<tr>
<td>authenticationFailure</td>
<td>There was an attempt to access the device with the wrong SNMP community</td>
<td>1.3.6.1.6.3.1.1.5.5</td>
<td>Yes</td>
</tr>
<tr>
<td>coldStart</td>
<td>The unit has been restarted</td>
<td>1.3.6.1.6.3.1.1.5.1</td>
<td>Yes</td>
</tr>
<tr>
<td>dot3OamOperStatusChange</td>
<td>OAM (802.3ah) connectivity has been lost or restored</td>
<td>1.3.6.1.4.1.164.3.1.6.1.6.0.1</td>
<td>Yes</td>
</tr>
<tr>
<td>dot3OamPeerEvent</td>
<td>One of the following OAM (802.3ah) indications has been received from remote partner: Connectivity failure Connectivity recovered Critical error started Critical error ended Dying gasp</td>
<td>1.3.6.1.4.1.164.3.1.6.1.6.0.2</td>
<td>Yes</td>
</tr>
<tr>
<td>ethOamCfmDefectCondition</td>
<td>One of the following OAM CFM conditions has occurred:</td>
<td>1.3.6.1.4.1.164.3.1.6.1.3.0.1</td>
<td>Yes</td>
</tr>
<tr>
<td>failedLogin</td>
<td>Failed login to ETX-203A has occurred</td>
<td>1.3.6.1.4.1.164.6.1.0.25</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### Setting the Trap Delay

You can configure a delay before the ETX-203A device sends traps.

**To set trap delay:**

1. Navigate to `configure management snmp`.
2. Enter the delay in seconds (allowed range 0–100):
   
   \[
   \text{trap-delay} \ <\text{seconds}>.
   \]
   
   Traps are sent with the specified delay.

### Masking Traps

You can mask some traps to prevent them from being sent to all management stations.

<table>
<thead>
<tr>
<th>Trap</th>
<th>Description</th>
<th>OID</th>
<th>Maskable</th>
</tr>
</thead>
<tbody>
<tr>
<td>fallingAlarm</td>
<td>An RMON falling event has been triggered, by dropping below one of the following Y.1731 thresholds: Frame Delay Frame Delay Variation Frame Loss Ratio Unavailability Ratio</td>
<td>1.3.6.1.2.1.16.0.2</td>
<td>Yes</td>
</tr>
<tr>
<td>linkDown</td>
<td>Network or user Ethernet port has been disconnected</td>
<td>1.3.6.1.6.3.1.1.5.3</td>
<td>Yes</td>
</tr>
<tr>
<td>linkUp</td>
<td>Network or user Ethernet port has been connected</td>
<td>1.3.6.1.6.3.1.1.5.4</td>
<td>Yes</td>
</tr>
<tr>
<td>prtStatusChangeTrap</td>
<td>An SFP has been inserted into or removed from one of the ports</td>
<td>1.3.6.1.4.1.164.6.1.0.3</td>
<td>Yes</td>
</tr>
<tr>
<td>risingAlarm</td>
<td>An RMON rising event has been triggered, by exceeding one of the following Y.1731 thresholds: Frame Delay Frame Delay Variation Frame Loss Ratio Unavailability Ratio</td>
<td>1.3.6.1.2.1.16.0.1</td>
<td>Yes</td>
</tr>
<tr>
<td>successfulLogin</td>
<td>Successful login to ETX-203A has occurred</td>
<td>1.3.6.1.4.1.164.6.1.0.24</td>
<td>Yes</td>
</tr>
<tr>
<td>tftpStatusChangeTrap</td>
<td>TFTP session status has changed, one of the following has occurred: Connecting Transferring data Ended with timeout Ended OK error</td>
<td>1.3.6.1.4.1.164.6.1.0.1</td>
<td>Yes</td>
</tr>
</tbody>
</table>
To mask traps to all network managers:

1. Navigate to `configure management snmp`.

   The `config>mngmnt>snmp#` prompt is displayed.

2. Enter:


   The specified trap is not sent to any network managers.

   - To mask all the traps, enter `trap-mask all`
   - To unmask all the traps, enter `no trap-mask all` or `no trap-mask`
   - To unmask a specific trap, enter `no trap-mask <trap-name>` where `<trap-name>` is one of the traps specified above.

**Note**

To mask all the traps, enter `trap-mask all`

To unmask all the traps, enter `no trap-mask all` or `no trap-mask`

To unmask a specific trap, enter `no trap-mask <trap-name>` where `<trap-name>` is one of the traps specified above.

---

**Working with Trap Synchronization**

You can add network managers (SNMPv1) or target manager stations (SNMPv3) to groups for trap synchronization. Traps are sent to the groups with sequence IDs to allow the managers to detect when traps have been lost, and request that traps be sent again.

- A trap synchronization group can contain managers of only one type, e.g. you cannot mix SNMPv1 and SNMPv3 managers in a group
- A manager cannot belong to more than one group
- The trap masking must be the same for all managers in a group.

**Adding Network Managers to Trap Synchronization Group (SNMPv1)**

1. Navigate to `configure management manager(<manager-ip-address>/32)`.

   The `config>mngmnt>manager(<manager-ip-address>/32)#` prompt is displayed.

2. Enter:

   - `trap-sync-group <group-id> [import-trap-masking]`. 

---

**Note**

You can also mask all traps to a specific management station. For details refer to Chapter 5.
The manager is added to the specified group. If the group does not exist, it is created. If you specify the `import-trap-masking` parameter, the manager's trap masking is imported from the first manager in the group.

**Note**  
To remove the manager from the group, enter `no trap-sync-group <group-id>`. If the manager was the last in the group, the group is deleted.

**Adding Target Manager Stations to Trap Synchronization Group (SNMPv3)**

To add a target manager station to a trap synchronization group:

1. Navigate to `configure management snmp target(<target-name>)`.  
   The `config>mngmnt>snmp>target(<target-name>)#` prompt is displayed.

2. Enter:
   
   `trap-sync-group <group-id> [import-trap-masking].`

   The manager is added to the specified group. If the group does not exist, it is created. If you specify the `import-trap-masking` parameter, the manager's trap masking is imported from the first manager in the group.

**Note**  
To remove the manager from the group, enter `no trap-sync-group <group-id>`. If the manager was the last in the group, the group is deleted.

**Configuring Trap Synchronization Masking (SNMPv1)**

If a group contains SNMPv1 managers, you can configure the trap masking of the group.

To configure trap masking:

1. Navigate to `configure management trap-sync-group <group-id>`.  
   The `config>mngmnt>trap-sync-group(<group-id>)#` prompt is displayed.

2. To mask or unmask traps:
   - To mask all traps, enter:
     
     `trap-mask all.`

     All traps are masked for the group.
   - To unmask all traps, enter:
     
     `no trap-mask.`

     All traps are unmasked for the group.

**Configuring Trap Synchronization Target Parameters and Tags (SNMPv3)**

If a group contains SNMPv3 managers, you can configure the target parameters and tag list for the group. Refer to Chapter 5 for information on target parameters and tags.
To specify a set of target parameters:
1. Navigate to `configure management trap-sync-group <group-id>`.
   The `config>mngmnt>trap-sync-group(<group-id>)#` prompt is displayed.
2. Enter:
   `target-params <target-param-name>`.
   The specified set of target parameters is assigned to the group.

To specify tags:
1. Navigate to `configure management trap-sync-group <group-id>`.
   The `config>mngmnt>trap-sync-group(<group-id>)#` prompt is displayed.
2. Enter:
   `tag-list <tag-list>`.
   The specified list of tags is assigned to the group.
   To remove the tag list, enter: `no tag-list`.

Displaying Trap Synchronization Information
You can display the trap synchronization information.

To display trap synchronization information:
1. If SNMPv3 is enabled, navigate to `configure management snmp` otherwise navigate to `configure management`.
   The `config>mngmnt#` or `config>mngmnt>snmp#` prompt is displayed respectively.
2. Enter:
   `show trap-sync`.
   The trap synchronization information is displayed.
6.3 Troubleshooting

This section contains a general troubleshooting chart that lists possible failures and provides workarounds.

Troubleshooting Chart

Use this chart to identify the cause of a problem that may arise during operation. For detailed description of the LED indicators functions, refer to Chapter 3.

To correct the reported problem, perform the suggested corrective actions. If a problem cannot be resolved by performing the suggested action, please contact your RAD distributor.

Table 6-3. Troubleshooting Chart

<table>
<thead>
<tr>
<th>Fault/Problem</th>
<th>Probable Cause</th>
<th>Corrective Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>The unit is “dead” (POWER LED is off)</td>
<td>No power</td>
<td>• Verify that both ends of the power cable are properly connected.</td>
</tr>
<tr>
<td></td>
<td>Blown fuse</td>
<td>• Disconnect the power cable from both ends and replace the fuse with another fuse of proper rating.</td>
</tr>
<tr>
<td>The event log reports a fan or power supply error.</td>
<td></td>
<td>• View the inventory file by entering <code>show inventory</code> at the <code>config&gt;system</code> prompt.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Restart the unit.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• In case of failure, replace the entire unit.</td>
</tr>
<tr>
<td>The unit is unreachable</td>
<td>Incorrect management settings</td>
<td>• Using a local serial connection, enable the relevant management access type by entering <code>telnet</code>, <code>snmp</code>, and/or <code>ssh</code> at the <code>config&gt;mngmnt&gt;access</code> prompt.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• View the list of enabled management access types and settings by entering <code>info</code> at the <code>config&gt;mngmnt</code> prompt.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• In case of SNMPv1, verify that the read, write, and trap communities match the setting (public, private) of your management station.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Verify that the management station IP address is included in the manager list.</td>
</tr>
<tr>
<td>Management path disconnected</td>
<td></td>
<td>• In case of remote management, analyze this issue using a local serial connection.</td>
</tr>
</tbody>
</table>
### Fault/Problem | Probable Cause | Corrective Action
---|---|---
Physical link fails to respond | Link may be administratively disabled. | • Administratively enable the link  
• In case of Ethernet links, make sure that the autonegotiation, speed, and duplex modes match the configured values on the access switch/router.

Ethernet LINK LED is off | Ethernet cable problem | • Check the Ethernet cable to see whether a cross or straight cable is needed  
• Check/replace Ethernet cable  
• Verify that the range is within the limits  
• Check the port by connecting the remote end of the cable to a different switch  
• Send the unit for repair.

---

### 6.4 Performing Diagnostic Tests

This section describes general diagnostic tests and RFC-2544 testing. For information on testing ports, flows, and OAM CFM, refer to Chapter 5.

#### RFC-2544 Testing

You can perform BERT testing based on RFC-2544:

- Throughput test – Until binary search convergence
- Packet loss rate – 10% steps
- Latency – Roundtrip frame latency.

#### Standards

RFC-2544, Benchmarking Methodology for Carrier Ethernet Networks

#### Benefits

You can evaluate the performance of network devices to provide performance metrics of the Ethernet network and validate the SLA.
Functional Description

In a bidirectional throughput test, the local ETX-203A generates LBM + data TLV messages towards the far-end device, which responds with LBR messages. The local ETX-203A calculates the round trip throughput.

In a unidirectional throughput test, the local ETX-203A generates 1DM messages towards the far-end device, which verifies the frames and calculates unidirectional throughput. The convergence algorithm is based on a binary search using LMM and LMR messages.

The packet loss test is performed as follows for all selected frame sizes:

- Transmit x frames at a rate of 100% throughput
- Calculate frame loss with the formula: \((tx - rx) / 100 \times tx\)
- Decrease rate by 10% and repeat the test until two trails result in no frame loss.

The latency test is performed as follows:

- Transmit DMM frames at a rate of throughput for 120 seconds
- Calculate the latency using DMM and DMR frames that are transmitted after 60 seconds
- The test result is the average of 20 trials per frame size (40 minutes per frame-size)
- Applicable for round-trip mode.

Factory Defaults

By default, no profiles or tests are defined.

When you create a test profile, it is configured by default as shown below.

```bash
ETX-203A# config test rfc2544
ETX-203A(config)> test rfc2544# profile-name Testprf
ETX-203A(config)> test rfc2544> profile-nam(Testprf)$ inf d
  frame-size  64
  pattern  all-ones
  tlv-type  data
  test-direction  bidirectional
  frames-number-in-burst  200000
  frame-loss-tolerance  20
  binary-search-resolution  10000
  number-of-trials  1
  no learning-frames

ETX-203A(config)> test rfc2544> profile-nam(Testprf)$
```

When you create a test, it is configured by default as shown below.
Performing Tests

To perform RFC-2544 tests, you configure a test profile, which is a template to create test runs. You then configure a test with an associated profile and test parameters, and activate the test.

To configure RFC-2544 test profiles:

1. Navigate to `config test rfc2544`.
   The `config>test>rfc2544#` prompt is displayed.

2. Type:
   ```
   profile-name <name>
   ```
   A test profile with the specified name is created if it does not already exist, and the `config>test>RFC2544> profile-name<name>#$` prompt is displayed.

3. Enter all necessary commands according to the tasks listed below.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define binary search granularity – the minimum step in the binary search (for throughput tests)</td>
<td><code>binary-search-resolution &lt;thousands&gt;</code></td>
<td></td>
</tr>
<tr>
<td>Define frame loss tolerance in 1/1000 units.</td>
<td><code>frame-loss-tolerance &lt;frames-from-1000&gt;</code></td>
<td>If the test reaches that value, the test is considered as completed successfully.</td>
</tr>
<tr>
<td>Define a list of sizes for the test</td>
<td><code>frame-size [64] [128] [256] [512] [1024] [1280] [1518]</code></td>
<td>You must choose at least one.</td>
</tr>
<tr>
<td>Define how many frames in burst</td>
<td><code>frames-number-in-burst &lt;frames&gt;</code></td>
<td></td>
</tr>
<tr>
<td>Define amount and frequency of learning frames</td>
<td>`learning-frames number &lt;value&gt; frequency { once</td>
<td>once-per-trial }`</td>
</tr>
<tr>
<td>Define the number of repeats for this test</td>
<td><code>number-of-trials &lt;value&gt;</code></td>
<td></td>
</tr>
<tr>
<td>Define pattern of test frame payload</td>
<td>`pattern { all-ones</td>
<td>all-zeros-without-crc</td>
</tr>
<tr>
<td>Define if test is unidirectional or bidirectional</td>
<td>`test-direction { unidirectional</td>
<td>bidirectional }`</td>
</tr>
<tr>
<td>Define if TLV type is test or data</td>
<td>`tlv-type { test</td>
<td>data }`</td>
</tr>
</tbody>
</table>
To configure RFC-2544 tests:
1. Navigate to `configure test rfc2544`.
   The `config>test>rfc2544#` prompt is displayed.
2. Type:
   `test <id>`.
   The `config>test>rfc2544> test(<id>)#` prompt is displayed.
3. Enter all necessary commands according to the tasks listed below.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activating the test</td>
<td><code>activate date &lt;dd-mm-yyyy&gt; &lt;hh:mm:ss&gt;</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>activate recurring &lt;hours&gt;</code></td>
<td></td>
</tr>
<tr>
<td>Binding to destination NE</td>
<td><code>bind oam-cfm md &lt;md-id&gt; ma &lt;ma-id&gt; mep &lt;mep-id&gt; service &lt;service-id&gt; dest-ne &lt;dest-ne-id&gt;</code></td>
<td></td>
</tr>
<tr>
<td>Configuring maximum theoretical PPS for test</td>
<td><code>max-rate &lt;value&gt;</code></td>
<td>The maximal theoretical PPS for this test is set to reflect the limitation on this “Channel”.</td>
</tr>
<tr>
<td>Associating a test profile with the test</td>
<td><code>test-profile &lt;test-profile-name&gt;</code></td>
<td></td>
</tr>
<tr>
<td>Defining the type(s) of benchmark test to perform on this run.</td>
<td><code>type [throughput] [latency] [frame-loss]</code></td>
<td></td>
</tr>
<tr>
<td>Displaying test report</td>
<td><code>show report all</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>show report iteration &lt;iteration-number&gt;</code></td>
<td></td>
</tr>
<tr>
<td>Displaying test status</td>
<td><code>show status</code></td>
<td></td>
</tr>
<tr>
<td>Displaying test summary</td>
<td><code>show summary</code></td>
<td></td>
</tr>
</tbody>
</table>

**Running a Ping Test**

You can ping a remote IP host to check the ETX-203A IP connectivity with that host.

To ping an IP host:
1. In any level, start pinging the desired host specifying its IP address and optionally the number of packets to send:
   `ping <1.1.1.1–255.255.255.255> [number-of-packets <0–50>]
2. To stop the ping test, enter:
   `no ping`.

**Tracing the Route**

This diagnostic utility traces the route through the network from ETX-203A to the destination host. The trace route utility supports up to 30 hops.
To trace a route:

- In any level, start the trace route and specify the IP address of the host to which you intend to trace route:
  
  \texttt{trace-route <1.1.1.1–255.255.255.255>}

6.5 Frequently Asked Questions

Q How should management flows be set up?
A The packets to the host are classified according to the management VLAN, then the packets from the host are classified with “Match_all” classifier and `vlan-tag` push command for the required VLAN. Refer to the `Quick Start Guide` for an example of configuring management flows.

Q If I change the second Ethernet port from network to user, what happens to the associated flows?
A When you change the functional mode, all flows related to the port are deleted.

6.6 Technical Support

Technical support for this product can be obtained from the local partner from whom it was purchased.

RADcare Global Professional Services offers a wide variety of service, support and training options, including expert consulting and troubleshooting assistance, online tools, regular training programs, and various equipment coverage options.

For further information, please contact the RAD partner nearest you or one of RAD’s offices worldwide.

RAD Data Communications would like your help in improving its product documentation. Please send us an e-mail with your comments.

Thank you for your assistance!
Chapter 7

Software Upgrade

This chapter explains how to upgrade ETX-203A to software version 3.0.

Software upgrade is required to fix product limitations, enable new features, or to make the unit compatible with other devices that are already running the new software version.

ETX-203A stores two software versions, each of them in one of the two 2.56 MB partitions of its flash memory, which also contains a boot program. The software is stored in compressed format. The main version is decompressed and loaded into the ETX-203A RAM upon power-up. The backup software is kept for backup purposes. If the main software becomes corrupted, you can swap it with the backup. By default, ETX-203A is delivered with active software only.

New software releases are distributed as *.img files, to be downloaded to ETX-203A. When starting a download, ETX-203A erases the current backup and places the new software in the backup partition. When downloading is complete, the unit checks the integrity of the new software file. If it is correct, the backup and active files are swapped. The new software release becomes active and the former active software becomes the backup. If a failure occurs during downloading, the new version is erased. In this case, only one version is left stored in the flash memory. The backup software can be downloaded to the unit and swapped with the main software later.

The information in this chapter includes the following:

- Detailed conditions required for the upgrade
- Any impact the upgrade may have on the system
- Description of downloading options.

**Note** Sometimes you may find it necessary to downgrade by downloading an older software version to ETX-203A. In this case the procedures described in this section can be used to download the software image.

When you downgrade the software, the device configuration cannot be preserved. You must format the flash via the boot menu (Figure 7-3) before downloading the earlier software version.

### 7.1 Impact

ETX-203A continues operating with the previous software version until you manually reset the unit.
7.2 Software Upgrade Options

Application software can be downloaded to ETX-203A via with the file copy command, or via XMODEM or TFTP, using the boot menu.

7.3 Prerequisites

Before starting the upgrade, verify that you have the following:

- For upgrade via SFTP/TFTP:
  - Operational ETX-203A unit with valid IP parameters configured
  - Connection to a PC with a SFTP/TFTP server application and a valid IP address
  - Software image file stored on the PC. The image file (and exact name) can be obtained from the local RAD business partner from whom the device was purchased.

- For upgrade via XMODEM:
  - Operational ETX-203A unit
  - Connection to a PC via HyperTerminal
  - Software image file stored on the PC. The image file (and exact name) can be obtained from the local RAD business partner from whom the device was purchased.

7.4 Upgrading the Device Software via CLI

The recommended software downloading method is to use the file copy command.

Network administrators can use this procedure to distribute new software releases to all the managed ETX-203A units in the network from a central location.

![Figure 7-1. Downloading a Software Application File via SFTP](image)

Use the following procedure to download software release 3.0 to ETX-203A via CLI.

1. Verify that the image file is stored on the PC with the SFTP server application.
2. Verify that the ETX-203A host has valid IP parameters.
3. Ping the PC to verify the connection.
4. Activate the SFTP server application.
5. Download the image file from the PC to ETX-203A.

**Note**  
*Configuration values shown in this chapter are examples only.*

**Verifying the Host Parameters**

In order to be able to establish communication with the SFTP server, the ETX-203A host must have host IP parameters configured according to your network requirements. In addition, flows must be defined to and from the ETX-203A host. Refer to the following manual sections for additional information:

- *Connecting to ASCII Terminal* in Chapter 2
- *Working with Terminal* in Chapter 4
- *Configuring the Host IP Settings* in Chapter 5.

**Pinging the PC**

Check the integrity of the communication link between ETX-203A and the PC by pinging the PC from ETX-203A.

➢ To ping the PC:

1. In any level, start pinging the PC specifying its IP address and optionally the number of packets to send:

   ```
ping <ip-address> [number-of-packets <num-packets>]
   ```

   A reply from the PC indicates a proper communication link.

2. If the ping request times out, check the link between ETX-203A and the PC (physical path, configuration parameters, etc.)

**Activating the SFTP Server**

Once the SFTP server is activated on the PC, it waits for any SFTP file transfer request originating from the product, and carries out the received request automatically.

SFTP file transfers are carried out through TCP port 22. Make sure that the firewall you are using on the server allows communication through this port (refer to *Chapter 5* for details).

**Activating the TFTP Server**

Once the TFTP server is activated on the PC, it waits for any TFTP file transfer request originating from the product, and carries out the received request automatically.
TFTP file transfers are carried out through port 69. Make sure that the firewall you are using on the server allows communication through this port (refer to Chapter 5 for details).

**Note** Configure the connection timeout of the TFTP server to be more than 30 seconds to prevent an automatic disconnection during the backup partition deletion (about 25 seconds).

### Downloading the Software

This procedure is used to replace the current software version with the new software release.

➢ To copy the image file to the ETX-203A unit:

1. Navigate to the file context.
2. Enter:

   ```
   copy sftp://<username>:<password>@<ip-address>/<image-file-name> main-sw
   ```

   Where `<ip-address>` is the IP address of the PC where the SFTP server is installed.

   The software download is performed. When the process is completed, use the `reboot` command in the `admin` context to restart ETX-203A, for the new software version to become active.

### 7.5 Upgrading the Device Software via the Boot Menu

Software downloading can also be performed using the Boot menu. The Boot menu can be reached while ETX-203A performs initialization, for example, after power-up.

You may need to start the loading from the Boot menu if you are unable to use the `file copy` command (for example, because the ETX-203A software has not yet been downloaded or is corrupted).

**Caution** The Boot menu procedures are recommended only for use by authorized personnel, because this menu provides many additional options that are intended for use only by technical support personnel.

Two software downloading options are available from the Boot menu:

- Downloading using the XMODEM protocol. This is usually performed by downloading from a PC directly connected to the CONTROL DCE port of the unit.
• Downloading using TFTP. This is usually performed by downloading from a remote location that provides an IP communication path to an Ethernet port of ETX-203A.

Accessing the Boot Menu

The boot menu can be accessed when the device is powered up, before logging in.

To access the Boot menu:

1. Configure the communication parameters of the selected PC serial port for asynchronous communication with 9,600 bps, no parity, one start bit, eight data bits and one stop bit. Turn all types of flow control off.
2. Turn off ETX-203A.
3. Activate the terminal application.
4. Turn on ETX-203A and immediately start pressing the <Enter> key several times in sequence until you see Boot screen.

The boot screen is shown. A typical screen is shown below (the exact version and date displayed by your ETX-203A unit may be different).

| Note | If you miss the timing, ETX-203A performs a regular reboot process (this process starts with Loading and ends with a message to press <Enter> a few times to display the login screen). |
Using the XMODEM Protocol

Use the following procedure to download software release 3.0 to ETX-203A via XMODEM.

To download software release via XMODEM:

1. Verify that the image file is stored on the PC with the terminal application.
2. From the Boot menu (Figure 7-3), select Download Files or an Application by XMODEM.
   A message is displayed that requests the partition number to which the new software is to be downloaded, and offers a recommended value.
3. If there is no special reason to select a different value, type the recommended number and then press <<Enter>>. A typical display is shown below:

   Select Copy number for download ( 1 )
   Select: 1

   The process starts, and the following is displayed:

   Erasing Partition please wait ....
   Please start the XMODEM download.

4. Start the transfer in accordance with the program you are using. For example, if you are using the Windows HyperTerminal utility:
   - Select Transfer in the HyperTerminal menu bar, and then select Send File on the Transfer menu.
     The Send File window is displayed:
     - Select the prescribed ETX-203A software file name (you may use the Browse function to find it).
     - In the Protocol field, select Xmodem.
     - When ready, press Send in the Send File window.
You can now monitor the progress of the downloading in the **Send File** window.

**Note**  *If downloading fails, repeat the whole procedure.*

When the downloading process has successfully completed, a sequence of messages similar to the following is displayed:

<table>
<thead>
<tr>
<th>Loading ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decompressing to RAM.</td>
</tr>
<tr>
<td>Processing archive: FLASH</td>
</tr>
<tr>
<td>Extracting ETX-203A.BIN.</td>
</tr>
<tr>
<td>.......................................................................................... CRC OK</td>
</tr>
<tr>
<td>Running ...</td>
</tr>
<tr>
<td>******************************************</td>
</tr>
<tr>
<td>* In order to start working - press the ENTER button for few times*</td>
</tr>
<tr>
<td>******************************************</td>
</tr>
</tbody>
</table>

5. At this stage, press the `<Enter>` key several times to go to the login screen.

**Using TFTP**

Use the following procedure to download software release 3.0 to ETX-203A via TFTP.

➢ **To download software release via TFTP:**

1. From the Boot menu (*Figure 7-3*), select **Download Files or an Application by TFTP**.

   The following message is displayed:

   ```
   Enter TFTP timeout in case of failure [20 sec]:
   ```

2. Enter the amount of time to wait for the TFTP server.

   The following message is displayed:

   ```
   Enter the target file name []:
   ```

3. Enter the name of the software image file.

   The following message is displayed:

   ```
   Enter the server IP address []:
   ```

4. Enter the IP address of the PC where the TFTP server is installed.

   If no errors are detected, the downloading process starts, and the screen displays its progress. After the image has been downloaded, use the **reboot** command in the **admin** context to reset ETX-203A in order to load the new release.
7.6 Verifying Upgrade Results

To verify that the upgrade was successful, log on to ETX-203A via HyperTerminal to view the Inventory table (show inventory-table at prompt config#system#), and verify the active software version in the SW Rev column.
Chapter 8

Configuring Typical Applications

This chapter provides detailed instructions for setting up a typical application using ETX-203A units. Refer to Chapter 5 for a detailed description of all configuration options available for ETX-203A.

8.1 Ethernet Private Line Application

Figure 8-1 illustrates a point-to-point application of an Ethernet private line over a WAN.

![Figure 8-1. Point-to-Point Ethernet Private Line over Wide Area Network](image)

In this application, ETX-203A (A) receives Ethernet user traffic separated by VLAN at both Gigabit Ethernet user ports, and transmits it over separate VLANs through the Wide Area network. ETX-203A (B) receives the user traffic separated by VLAN from the Wide Area network user traffic separated by VLAN, and transmits it via both Gigabit Ethernet user ports, separated by VLAN.

You must configure the following to deploy ETX-203A units in this application:

1. System parameters (host IP, default gateway)
2. Classifier profiles

The default policer and queue map profiles are used when creating the flows. Refer to the descriptions of creating profiles in Chapter 5 for information on the default profiles.

<table>
<thead>
<tr>
<th>Device</th>
<th>Host IP</th>
<th>IP mask</th>
<th>Default Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>ETX-203A (A)</td>
<td>192.168.10.10</td>
<td>255.255.255.0</td>
<td>192.168.10.1</td>
</tr>
<tr>
<td>ETX-203A (B)</td>
<td>192.168.10.20</td>
<td>255.255.255.0</td>
<td>192.168.10.1</td>
</tr>
</tbody>
</table>
Table 8-2. Flow Configuration Summary, ETX-203A (A) and (B)

<table>
<thead>
<tr>
<th>Flow ID</th>
<th>Ingress Port</th>
<th>Egress Port</th>
<th>Classification Criteria</th>
<th>Outer VLAN Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>data20_out</td>
<td>User port 1</td>
<td>Network port 1</td>
<td>VLAN 20</td>
<td>Change to VLAN 220</td>
</tr>
<tr>
<td>data220_in</td>
<td>Network port 1</td>
<td>User port 1</td>
<td>VLAN 220</td>
<td>Change to VLAN 20</td>
</tr>
<tr>
<td>data30_out</td>
<td>User port 2</td>
<td>Network port 1</td>
<td>VLAN 30</td>
<td>Change to VLAN 230</td>
</tr>
<tr>
<td>data230_in</td>
<td>Network port 1</td>
<td>User port 2</td>
<td>VLAN 230</td>
<td>Change to VLAN 30</td>
</tr>
</tbody>
</table>

Configuring Classifier Profiles

In both units, you have to create classifier profiles for VLANs 20, 30, 220, and 230. The same scripts can be used in both units, therefore they are presented here only once.

➤ To create the classifier profile for VLAN 20:
   - Execute the following script to create the classifier profile for VLAN 20.

```
configure flows
classifier-profile vlan20 match-any
  match vlan 20
exit all
```

➤ To create the classifier profile for VLAN 30:
   - Execute the following script to create the classifier profile for VLAN 30.

```
configure flows
classifier-profile vlan30 match-any
  match vlan 30
exit all
```

➤ To create the classifier profile for VLAN 220:
   - Execute the following script to create the classifier profile for VLAN 220.

```
configure flows
classifier-profile vlan220 match-any
  match vlan 220
exit all
```

➤ To create the classifier profile for VLAN 230:
   - Execute the following script to create the classifier profile for VLAN 230.

```
configure flows
classifier-profile vlan230 match-any
  match vlan 230
exit all
```

Configuring Flows

In both units, you have to create four flows, as flows are unidirectional (see Table 8-2)
• Flow data20_out from user port 1 (ethernet 3) to network port 1 (ethernet 1), changing VLAN 20 to VLAN 220
• Flow data220_in from network port 1 (ethernet 1) to user port 1 (ethernet 3), changing VLAN 220 to VLAN 20
• Flow data30_out from user port 2 (ethernet 4) to network port 1 (ethernet 1), changing VLAN 30 to VLAN 230
• Flow data230_in from network port 1 (ethernet 1) to user port 2 (ethernet 4), changing VLAN 230 to VLAN 30

The same scripts can be used in both units, therefore they are presented here only once.

➤ To create flow data20_out:
  • Execute the following script to create flow data20_out as shown in Table 8-2.

```plaintext
configure flows flow data20_out
  classifier vlan20
  policer profile Policer1
  ingress-port ethernet 3
  egress-port ethernet 1 queue-map CosProfile1 block 0/1
  mark all
  vlan 220
  no shutdown
exit all
```

➤ To create flow data220_in:
  • Execute the following script to create flow data220_in as shown in Table 8-2.

```plaintext
configure flows flow data220_in
  classifier vlan220
  policer profile Policer1
  ingress-port ethernet 1
  egress-port ethernet 3 queue-map CosProfile1 block 0/1
  mark all
  vlan 20
  no shutdown
exit all
```

➤ To create flow data30_out:
  • Execute the following script to create flow data30_out as shown in Table 8-2.

```plaintext
configure flows flow data30_out
  classifier vlan30
  policer profile Policer1
  ingress-port ethernet 4
  egress-port ethernet 1 queue-map CosProfile1 block 0/1
  mark all
  vlan 230
  no shutdown
exit all
```
To create flow data230_in:

- Execute the following script to create flow data230_in as shown in Table 8-2.

```bash
configure flows flow data230_in
    classifier vlan230
    policer profile Policer1
    ingress-port ethernet 1
    egress-port ethernet 4 queue-map CosProfile1 block 0/1
    mark all
    vlan 30
    no shutdown
exit all
```
Appendix A

Connection Data

A.1 Ethernet Connector

The Ethernet electrical interface terminates in 8-pin RJ-45 connectors, of type 10/100BaseT or 10/100/1000BaseT, wired in accordance with Table A-1. The connector supports both MDI and MDIX modes.

<table>
<thead>
<tr>
<th>Pin</th>
<th>MDI</th>
<th>MDIX</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>A+</td>
<td>B+</td>
</tr>
<tr>
<td>2</td>
<td>A-</td>
<td>B-</td>
</tr>
<tr>
<td>3</td>
<td>B+</td>
<td>A+</td>
</tr>
<tr>
<td>4</td>
<td>C+</td>
<td>D+</td>
</tr>
<tr>
<td>5</td>
<td>C-</td>
<td>D-</td>
</tr>
<tr>
<td>6</td>
<td>B-</td>
<td>A-</td>
</tr>
<tr>
<td>7</td>
<td>D+</td>
<td>C+</td>
</tr>
<tr>
<td>8</td>
<td>D-</td>
<td>C-</td>
</tr>
</tbody>
</table>

A.2 MNG Connector

The ETX-203A Ethernet management port uses an electrical interface that terminates in an RJ-45, 8-pin connector. The port supports MDI and MDIX modes. Table A-2 lists the pin assignments.

<table>
<thead>
<tr>
<th>Pin</th>
<th>Designation</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>RxD+</td>
<td>Receive Data output, + wire</td>
</tr>
<tr>
<td>2</td>
<td>RxD-</td>
<td>Receive Data output, – wire</td>
</tr>
<tr>
<td>3</td>
<td>TxD+</td>
<td>Transmit Data input, + wire</td>
</tr>
<tr>
<td>4, 5</td>
<td></td>
<td>Not connected</td>
</tr>
</tbody>
</table>
### Appendix A  Connection Data

**A-2 CONTROL Connector ETX-203A Ver. 3.0**

#### A.3 CONTROL Connector

The control terminal interface terminates in an 8-pin RJ-45 connector. *Table A-3* lists the CONTROL connector pin assignments.

<table>
<thead>
<tr>
<th>Pin</th>
<th>Designation</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>TxD-</td>
<td>Transmit Data input, – wire</td>
</tr>
<tr>
<td>7,8</td>
<td>–</td>
<td>Not connected</td>
</tr>
</tbody>
</table>

*Table A-3. CONTROL Connector Pinout*

If you are using a cable with a DB-9 connector on the other end, the following table shows the pinout for the DB-9 connector.

<table>
<thead>
<tr>
<th>Pin</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>1, 2, 3, 4</td>
<td>–</td>
</tr>
<tr>
<td>5</td>
<td>Transmit Data (output)</td>
</tr>
<tr>
<td>6</td>
<td>Receive Data (input)</td>
</tr>
<tr>
<td>7, 8</td>
<td>–</td>
</tr>
</tbody>
</table>

*Table A-4. DB-9 Pinout*
Appendix B
Operation, Administration, and Maintenance (OAM)

B.1 Introduction

ETX-203A supports standard implementation of Ethernet OAM based on ITU-T Y.1731 and IEEE 802.1ag-D8. Pre-standard implementation based on Y.1731 is supported for backward compatibility, for instance when working opposite a device with an older version of Ethernet OAM software. This appendix describes the pre-standard implementation. The standard implementation can be found in the ITU-T Y.1731 and IEEE 802.1ag-D8 documentation.

The pre-standard OAM implementation provides the following:

- Continuity check
- Non-intrusive loopback which used to detect loss of bidirectional continuity
- Performance measurements (per service).

*Table B-1* lists the Ethernet OAM-related terms used in the appendix.

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UNI</td>
<td>User Network Interface. The physical demarcation point between the responsibility of the Service Provider and the responsibility of the Subscriber</td>
</tr>
<tr>
<td>UNI_C</td>
<td>Customer side of a UNI link</td>
</tr>
<tr>
<td>UNI_N</td>
<td>Network side of a UNI link</td>
</tr>
<tr>
<td>Service frame</td>
<td>An Ethernet frame transmitted across the UNI toward the Service Provider or an Ethernet frame transmitted across the UNI toward the Subscriber.</td>
</tr>
<tr>
<td>Flow</td>
<td>Ethernet Virtual Connection : An association of two or more UNIs that limits the exchange of Service Frames to UNIs in the Ethernet Virtual Connection</td>
</tr>
<tr>
<td>Point-to-point Flow</td>
<td>Flow connecting exactly two UNIs</td>
</tr>
</tbody>
</table>
### Term Description

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multipoint-to-Multipoint Flow</td>
<td>Flow connecting two or more UNIs</td>
</tr>
<tr>
<td>Service Instance / Class of service (CoS)</td>
<td>A set of Service Frames that have a commitment from the Service Provider to receive a particular level of performance</td>
</tr>
<tr>
<td>Service Instance Identifier (CoS ID)</td>
<td>Service Frame delivery performance is specified for all Service Frames transported within a flow with a particular Class of Service instance. The Class of Service instance is identified by a Class of Service Identifier associated with each Service Frame (Class of service can be identified by more than one parameter/frame attribute)</td>
</tr>
<tr>
<td>MEP</td>
<td>Proactive OAM reference point which is capable to initiate and terminate proactive OAM frames. MEP is also capable to initiate and react to diagnostics OAM frames.</td>
</tr>
<tr>
<td>MIP</td>
<td>A provisioned OAM reference point which is capable to respond to diagnostics OAM frames initiated by the MEP.</td>
</tr>
<tr>
<td>MEP Service Instance Source</td>
<td>The receiver of OAM frames in each Service Instance</td>
</tr>
<tr>
<td>MEP Service Instance Destination</td>
<td>The transmitter of OAM frames in each Service Instance</td>
</tr>
</tbody>
</table>

### B.2 Reference Architecture

*Figure B-1* illustrates two OAM flows:

- **OAM flow originating from the CPE**
  
  The CPE-to-CPE OAM flow is transferred transparently by ETX-203A and treated as data.

- **OAM flow originating from the ETX-203A devices.**
  
  The ETX-203A OAM flow runs on a data flow on the same VLAN. The ETX-203A units terminate the OAM flow and can be referred as a Maintenance Entity (ME). Each device supports up to 8 such MEs. In this case, the ETX-203A units act as MEPs (Maintenance End-Points) and not as a MIP (Maintenance Intermediate Points) and all measurements are performed on the UNI_N to UNI_N segment.
Handling of OAM Levels

**UNI_C to UNI_N Direction**

In the UNI_C to UNI_N direction ETX-203A blocks all OAM messages with OAM level greater than 2. Messages with other OAM levels are passed transparently.

**Network Ingress to UNI_N Direction**

All OAM messages coming from the network ingress with the device MAC address or with the special OAM multicast address are sent to the CPU. All other OAM messages are passed transparently to the user ports as per the respective flow definition.

### B.3 OAM Entities

This section describes the OAM entities hierarchy. *Figure B-2* illustrates the relationship between UNI, flow and Service Instance (COS ID), when one or more service instances belong to one flow and one or more flow belong to a UNI. From the OAM perspective, the continuity messages and defects are activated per flow, and the PM is activated per service instance.

**Note**  
A flow can belong only to one UNI in the same ETX-203A.
Figure B-3, Figure B-4 and Figure B-5 illustrate different combinations of UNIs, flows and service instances. Each UNI contains at least one flow, which contain at least one service instance.

- In the one flow per UNI case (Figure B-3), the PM and CC are transmitted once.

![Figure B-3. One Flow per UNI](image)

- In case of multiple flows per UNI (Figure B-4), PM and CC are transmitted three times.

![Figure B-4. Multiple Flows per UNI](image)

- In case of one flow and multiple CoS (Service Instances) per UNI (Figure B-5), the PM is transmitted three times and the CC – once.

![Figure B-5. One Flow and Multiple CoS (Service Instances) per UNI](image)

### B.4 OAM Flows

Figure B-6 illustrates a typical OAM traffic flow. The OAM message is transmitted from the source MEP 1 to the destination MEP 2 and the reply is transmitted back. The source is also a destination for messages from the other direction.

The OAM interval is one second, so each NTU transmits one request and one reply and receive one request and one reply. Total of four messages are transmitted per second per service instance.

![Figure B-6. OAM Flow](image)
OAM Message Addressing

The OAM defines two modes of addressing, unicast and multicast. Unicast addressing is used for point-to-point connections, while multicast addressing is used in cases where the MAC address of the destination MEP is not known. Currently ETX-203A supports point-to-point flows in proprietary mode.

OAM Message Association

On the receiver side the OAM frame is associated with a flow and a service.

Flow Association

When an OAM frame is associated with a flow, the following steps are performed:

- **Request message reception**
  
  When a request message is received, the VLAN is extracted to find the Flow ID. The Flow ID found at the receiver is compared against the Flow ID in the frame. If the IDs are equal, further service association is made. If it is not found, the “Flow ID no match” notification is returned in the reply message.

- **Reply message reception**
  
  When a reply message is received, the VLAN is extracted to find the Flow ID. The Flow ID found at the receiver is compared against the Flow ID in the frame. If the IDs are equal, further service association is made. If it is not found, the frame is discarded and connectivity alarm is issued.

Service Association

When an OAM frame is associated with a service, the following steps are performed:

- **Request message reception**
  
  The class of service characteristics are extracted from the frame and must be matched to an entry in the flows <-> services table at the receiver. If they are matched, the frame is processed. If not, the service ID is returned with the “Not Found” notification.

- **Reply message reception**
  
  The class of service characteristics are extracted from the frame and must be matched to an entry in the flow <-> services table at the receiver. If they are matched, the frame is processed. If not, the frame is discarded.

Ethernet Loopback (ETH-LB)

The ETH-LB can be used to verify connectivity. The ETH-LB is performed by sending a request ETH-LB message to the remote unit and expecting an ETH-LB reply message back to verify connectivity. When the insertion rate of ETH-LB messages is much slower compared to data rate between the flow points.

Unicast ETH-LB request message is sent from a MEP to a specific MEP (remote device). The DA of the request message is a unicast MAC address of destination device. Upon receipt of the request message, the MEP responds with unicast ETH-
LB reply message. The DA of the reply message is a unicast MAC address of requesting device, learned from request message.

**Continuity Check (ETH-CC)**

Ethernet Continuity Check (ETH-CC) can be used to detect continuity failures across flows between a given pair of edge service point on a flow. Continuity failures are caused by:

- Major failures (link failure, device failure, network path failure etc)
- Minor failures (software failure, memory corruption, incorrect configuration etc).

The ETH-CC signal is generated by one MEP. Upon receipt of the first ETH-CC signal from a sending MEP, the receiving MEP detects continuity with sending MEP and expects to receive further periodic ETH-CC signals. Once the receiving MEP stops receiving periodic ETH-CC signals from sending MEP, it declares continuity failure.

**OAM Procedures**

This section discusses the continuity check (CC) and the performance measurement (PM) procedures.

**Continuity Check Procedure**

The loopback message and the ETH-CC messages are used for continuity check. In case the services are defined and PM collection is enabled, they are also used to carry PM messages. If PM collection is disabled, the messages are used for continuity check only.

If the RX CC mode of the receiver is configured to CC-based, the continuity detection is based on ETH-CC. If the mode is set to LB-based, the continuity detection is based on ETH-LB. If the mode is disabled, the continuity detection is not performed.

**ETH-LB Method**

The ETH-LB method includes the following elements:

- Unicast ETH-LB transmission

  Unicast ETH-LB request message is transmitted by a MEP (ETX-203A) every 1 second. The transmitted Transaction Identifier is retained for at least 5 seconds after the unicast ETH-LB signal is transmitted. The Transaction Identifier must be changed for every unicast ETH-LB message, and no Transaction Identifier from the same MEP is allowed to be repeated within 1 minute.

- Unicast ETH-LB reception and reply transmission

  Whenever a valid unicast ETH-LB request message is received by MEP (ETX-203A), a unicast ETH-LB reply message is generated and transmitted to the requesting MEP. Every field in the unicast ETH-LB request message is copied to the unicast ETH-LB reply message with the following exceptions:
- The source and destination MAC addresses are swapped.
- The OpCode field is vendor-specific 0xFE.
- The Flow and MEP ID are processed as follows: if the Flow/MEP ID do not exist in the device, it changes them to “No Match” otherwise they are left intact.

**Unicast ETH-LB reply receipt**

When a unicast ETH-LB reply message is received by a MEP (ETX-203A) diagnostic flow termination function, it examines the TLVs returned in the unicast ETH-LB reply message. The signal is declared invalid if the TLVs do not match those sent in the corresponding unicast ETH-LB request signal, including MEP ID and Flow ID.

**Continuity declarations**

Loss of Continuity and Connectivity Mismatch states are declared by the ETH-LB mechanism.

- **Loss of continuity declaration**

  After the source device sends an ETH-LB message a timer is set with a 3.52 second timeout. If the destination device does send reply within the timeout, the source enters the loss of continuity state. Upon reply from the destination, the source resets the timer to 3.52 seconds. Regarding the continuity check message, the source checks only the Flow ID with the MEP ID. When the source enters the loss of continuity state, it adds 24 to Unavailable Seconds counter. The 3.52 second period is calculated as a sliding window.

  Loss of continuity state is cleared after 3.52 seconds with at least 21 reply messages from the destination. In this case the Unavailable Seconds counter decreased by 24.

- **Connectivity mismatch declaration**

  If the source Flow ID is not equal to the destination Flow ID as recorded in the reply message for 10 consecutive times, the source enters in to misconnection state.

  Misconnection state is cleared after 10 consecutive reply messages with the correct flow name from the destination.

  The Unavailable counter is maintained by the service according to the number of PM messages that did not receive replies. If a mismatch notification is received to the LB request, the frame is dropped and reply message is not sent. This is why the service becomes unavailable (no reply) in case of mismatch and the unavailable counter is raised.

**ETH-CC Method**

The ETH-CC method includes the following elements:

- **ETH-CC transmission**

  Unicast ETH-CC request message is transmitted by a MEP (ETX-203A) every 1 second. The transmitted Transaction Identifier is retained for at least 5 seconds after the unicast ETH-CC signal is transmitted. The Transaction Identifier must be changed for every Unicast ETH-CC message, and no
Transaction Identifier from the same MEP is allowed to be repeated within 1 minute.

- **Unicast ETH-CC reply receipt**

  When a unicast ETH-CC message is received by a MEP (ETX-203A) diagnostic flow termination function, it examines the TLVs returned in the unicast ETH-CC message, and declares the signal invalid if the TLVs do not match those sent in the corresponding exiting MEP ID and Flow ID.

- **Continuity declarations**

  Loss of Continuity and Connectivity Mismatch states are declared by the ETH-CC mechanism.

  - **Loss of continuity declaration**
    
    When the MEP receives the ETH-CC message a timer is set with a 3.5 seconds timeout. If the source does send another message during this period, the destination enters the loss of continuity state. Upon receipt of the ETH-CC message, the destination resets the timer to 3.5 seconds. Regarding the continuity check message, the destination check the Flow ID and the MEP ID. When the destination enters the loss of continuity state, it adds 4 to the Unavailable Seconds counter. The 3.5 second period is calculated as a sliding window.

    Loss of continuity state is cleared after 3.5 seconds with at least 2 messages from the source. In this case the Unavailable Seconds counter is decreased by 4.

  - **Connectivity mismatch declaration**

    If the source Flow ID is not equal to the destination Flow ID for 10 consecutive times, the destination enters into misconnection state. Misconnection state is cleared after 10 consecutive reply messages with the correct flow name from the source.

    The Unavailable counter is maintained by the service according to the number of PM messages that did not receive replies. If a mismatch notification is received to the LB request, the frame is dropped and reply message is not sent. This is why the service becomes unavailable (no reply) in case of mismatch and the unavailable counter is raised.

**Performance Measurement**

For details on OAM statistic counters, refer to *Chapter 5.*
To drill the holes for a wall installation, tear this page out of the manual or print it on letter-size paper (8.5x11.0") and hold it against the wall.

- LEDs facing up - drill at 1.
- LEDs facing down - drill at 2.
- LEDs facing left - drill at 3.

This panel is drawn to scale.

1. LED 176 mm (6.92 in)
2. 101.6 mm (4 in)
3. 176 mm (6.92 in)
Note

Ignore this supplement if the unit is AC-powered.

Certain DC-powered units are equipped with a plastic 3-pin VDC-IN power input connector, located on the unit rear panel. Different variations of the connector are shown in Figure 1. All are functionally identical.

Supplied with such units is a kit including a mating Terminal Block (TB) type connector plug for attaching to your power supply cable.

Connect the wires of your power supply cable to the TB plug, according to the voltage polarity and assembly instructions provided on the following pages.

Caution

Prepare all connections to the TB plug before inserting it into the unit’s VDC-IN connector.
To prepare and connect the power supply cable with the TB Plug:

**Note:** Refer to Figure 2 for assistance.

1. Strip the insulation of your power supply wires according to the dimensions shown.
2. Place each wire lead into the appropriate TB plug terminal according to the voltage polarity mapping shown in Figure 3. (If a terminal is not already open, loosen its screw.) Afterwards, tighten the three terminal screws to close them.
3. Pull a nylon cable tie (supplied) around the power supply cable to secure it firmly to the TB plug grip, passing the tie through the holes on the grip.
4. Isolate the exposed terminal screws/wire leads using a plastic sleeve or insulating tape to avoid a short-circuit.
5. Connect the assembled power supply cable to the unit by inserting the TB plug into the unit's VDC-IN connector until it snaps into place.

---

**Warning**

- Reversing the wire voltage polarity can cause damage to the unit!
- Always connect a ground wire to the TB plug’s chassis (frame) ground terminal. Connecting the unit without a protective ground, or interruption of the grounding (for example, by using an extension power cord without a grounding conductor) can cause harm to the unit or to the equipment connected to it!
**Note:** Certain TB plugs are equipped with captive screws for securing the assembled cable’s TB plug to the unit’s VDC-IN connector (C and E types only). To secure the plug, tighten the two screws on the plug into the corresponding holes on the sides of the input connector as shown in Figure 4.

![Figure 4. TB Plug with Captive Screws (optional)](image)

To disconnect the TB plug:

1. If the TB plug is equipped with captive screws, loosen the captive screws (see Figure 4).
2. If the unit’s VDC-IN connector is type B, lift the locking latch (see Figure 1).
3. Pull out the TB plug carefully.

---

**Caution** Always lift the locking latch of type B connectors before disconnecting the TB plug, to avoid damaging the TB plug.
# Customer Response Form

RAD Data Communications would like your help in improving its product documentation. Please complete and return this form by mail or by fax or send us an e-mail with your comments.

Thank you for your assistance!

**Manual Name:** ETX-203A Ver. 3.0  
**Publication Number:** 530-200-07/11

Please grade the manual according to the following factors:

<table>
<thead>
<tr>
<th></th>
<th>Excellent</th>
<th>Good</th>
<th>Fair</th>
<th>Poor</th>
<th>Very Poor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation instructions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operating instructions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manual organization</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Illustrations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The manual as a whole</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

What did you like about the manual?

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________
Error Report

Type of error(s) or problem(s):
- Incompatibility with product
- Difficulty in understanding text
- Regulatory information (Safety, Compliance, Warnings, etc.)
- Difficulty in finding needed information
- Missing information
- Illogical flow of information
- Style (spelling, grammar, references, etc.)
- Appearance
- Other

Please list the exact page numbers with the error(s), detail the errors you found (information missing, unclear or inadequately explained, etc.) and attach the page to your fax, if necessary.

________________________________________
________________________________________
________________________________________

Please add any comments or suggestions you may have.

________________________________________
________________________________________
________________________________________

You are:
- Distributor
- End user
- VAR
- Other

Who is your distributor?

Your name and company:

Job title:

Address:

Direct telephone number and extension:

Fax number:

E-mail: