

arcutronix

Synchronize the Ethernet

USER GUIDE

EDX100x



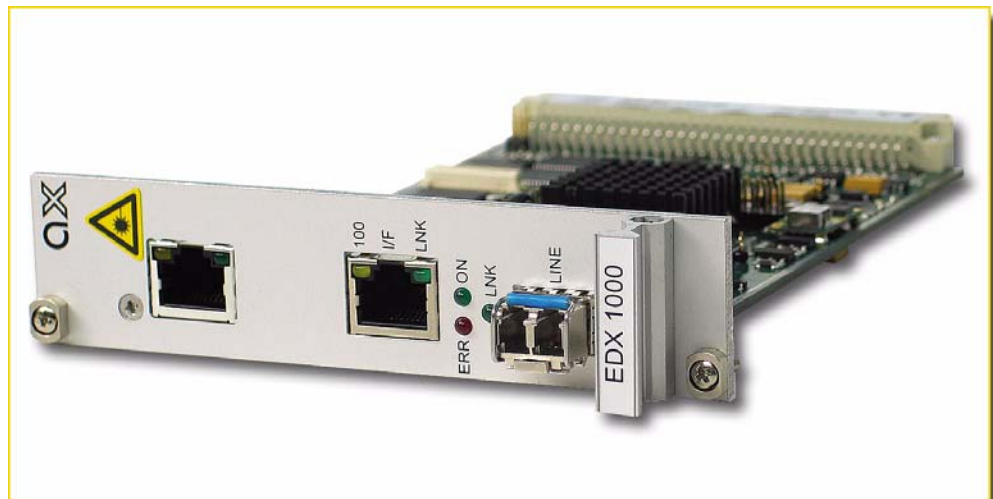
arcutronix GmbH
Deutschland

Installation and
Operation Manual

Version 3.2

EDX - Ethernet Demarcation

USER GUIDE



Covered Variants of EDX100x by this User Guide:

EDX1000:	0716-2001
EDX1002:	0716-2101
EDX1008:	0716-3200
EDX1006e:	0716-4600

Covered Software Versions by this User Guide:

SW-Version (\geq):	V 2_1_43
------------------------	----------

Part-Number (User-Guide):	0716 20 65
Version:	V 3.2
Date of Issue:	2015-05-12

Contacts

arcutronix GmbH
Garbsener Landstraße 10
D-30419 Hannover, Germany
Tel.: +49 (0)511 277- 2700
Fax: +49 (0)511 277- 2709
E-Mail: info@arcutronix.com
<http://www.arcutronix.com>

Copyright Note

© Copyright 2008, arcutronix GmbH. All rights reserved.

Restricted Rights Legend: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software Restricted Rights clause at DFARS 252.227-7013 and/or the Commercial Computer Software Restricted Rights clause at FAR 52.227-19(c) (1) and (2).

Document Contents

This document contains the latest information available at the time of publication. The content of this document is subject to change without prior notice. arcutronix reserves the right to modify the content at any time. arcutronix shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material. To request arcutronix publications or comment on this publication, contact a arcutronix representative or the arcutronix corporate headquarters. arcutronix may, without obligation, use or distribute information contained in comments it receives. Address correspondence to the attention of Manager, Technical Publications.

Trademarks

arcutronix is a registered trademark of arcutronix GmbH. All other products, trade names and services are trademarks, registered trademarks or service marks of their respective owners.

About this Book

Document Organization

This guide describes the hardware and software components of the EDX - Ethernet Demarcation Devices with Gigabit-Ethernet interfaces. It provides information on configuration, system installation and technical data. Also, it provides the procedures to operate or test the components of these devices.

The intended audience of this document is anyone who is responsible for installing, maintaining or operating the EDX - Ethernet Demarcation. This person must be aware of the risks, affected with these actions and must be qualified and trained. **Observe the safety precautions in chapter “Safety, Instructions, Statements”.**

The manual is designed as printable book, therefore chapters start at an odd page (the last even page of the chapter before may be empty). The headlines of the pages contain chapter name, chapter count, and chapter headline. The foot lines of the pages contain chapter page count, the revision date and the document title.

Chapters

Chapter 0, **Safety, Instructions, Statements:** Handling, precautions, warnings.

Chapter 1, **Abstract:** Series description, application area.

Chapter 2, **Getting Started:** Delivered parts, preparing the start-up.

Chapter 3, **Hardware:** List of system components, interface and front panel indicator description.

Chapter 4, **Functionality:** Switching, ring operation, VLAN, and LPT/RFD.

Chapter 5, **EDX100x Control Software & gCLI:** Configuration of the EDX100x.

Chapter 6, **SNMP and MIBs:** Remote monitoring of the EDX100x.

Chapter 7, **axCLI via SCX2e:** Explains the CLI-access to the EDX100x via the agent-card SCX2e.

Appendix A, **Technical Specifications:** Technical data of the EDX100x.

Appendix EC, **EC Declaration of Conformity:** For all EDX - Ethernet Demarcations.

Conventions

This manual uses the following text conventions to convey instructions and information:

Normal text is written in Albany font.

Commands and Arguments are done in `Courier New`.

Notes, cautions, and tips use these conventions and symbols:

NOTE: Means reader take note. Notes contain helpful suggestions or references to materials not contained in this manual.

WARNING:



DANGER

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

Release History

- 2015-05-12 Version 3.2 Editor: mjz
Added and changed the following topics:
- ax-remote management. This functionality enables the remote management access from CO racks to remotely located cards via (proprietary) in-band management link between agent and card.
- 2013-10-02 Version 3.1 Editor: mjz
Added and changed the following topics:
- Correct some typos.
- 2013-06-19 Version 3.0 Editor: mjz
Added and changed the following topics:
- Common template for EDX100x-Family and EDX100xSync-Family to make it easier in handling.
 - New front page: Synchronize the Ethernet.
- 2012-07-19 Version 2.0 Editor: azi
Added and changed the following topics:

- Added document version for better traceability.
 - Improved LPT/RFD explanations.
- 2011-03-18 Added and changed the following topics:
- ssh-support (chapter 7) added.
- 2009-12-23 Changed: More details added to the technical specifications (Appendix A).
- 2009-09-29 New Frontpage, new last page.
- 2009-07-31 LPT/RFD explained in more details.
- 2009-06-20 Added P-VLAN tagging support (“QinQ functionality”).
Changed (R)STP settings. Only Line-Ports support (R)STP.
Added functionality of GigE-SFPs: Copper and Fiber SFPs support auto-detect.
Changed EDX1000 and EDX1002: Additional MGMT-port is available.
Improved DHCP and DNS support available.
Telnet Access is disengageable.
SFP diagnostics show now the RX and TX power in dBm instead of mW.
- 2008-11-03 Added EDX1006e: Full optical active splitter device.
- 2008-06-13 First issue of the EDX100x User Guide.

Referenced and Related Documents

- [axMenuStructEDX] arcutronix GmbH (2013): EDX100x Menu-Structure for Command Line Interface (CLI).
- [axManual_SCX2e] arcutronix GmbH (2010): SCX2e User Manual.
- [IEC 60825-1] IEC 60825-1 - 2007: Safety of laser products - Part 1: Equipment classification and requirements
- [IEEE 802.1D] IEEE Std 802.1D™-2004: Media Access Control (MAC) Bridges.
- [IEEE 802.1Q] IEEE Std 802.1Q™-2011: Media Access Control (MAC) Bridges and Virtual Bridge Local Area Networks.
- [IEEE 802.1ad] IEEE Std 802.1ad™-2005 (Amendment to IEEE Std 802.1Q™-2005): Amendment 4: Provider Bridges.
- [IEEE 802.1w] IEEE Std 802.1w™-2001: Media Access Control (MAC) Bridges; Amendment 2: Rapid Reconfiguration.
- [IEEE 802.3] IEEE Std 802.3™-2008: Part3: Carrier sense multiple access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications.
- [IEEE 802.3ah] IEEE Std 802.3ah™-2004: Part3: Carrier sense multiple access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications. Amendment: Media Access Control Parameters, Physical Layers, and Management Parameters for Subscriber Access Networks.
- [IETF RFC 791] IETF RFC 791 (1981), Internet Protocol (IP).
- [IETF RFC 1065] IETF RFC 1065 (1988), Structure and Identification of Management Information for TCP/IP-based internets.
- [IETF RFC 1066] IETF RFC 1066 (1988), Management Information Base for Network Management of TCP/IP-based internets.
- [IETF RFC 1067] IETF RFC 1067 (1988), A Simple Network Management Protocol.
- [IETF RFC 1305] IETF RFC 1305 (1992), Network Time Protocol (Version 3) Specification, Implementation and Analysis.
- [IETF RFC 1901] IETF RFC 1901 (1996), Introduction to Community-based SNMPv2.
- [IETF RFC 2474] IETF RFC 2474 (1998), Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers.

[IETF RFC 2597]	IETF RFC 2597 (1999), Assured Forwarding PHB Group.
[IETF RFC 3246]	IETF RFC 3246 (2002), An Expedited Forwarding PHB (Per-Hop Behavior).
[IETF RFC 3410]	IETF RFC 3410 (2002), Introduction and Applicability Statements for Internet Standard Management Framework.
[IETF RFC 3619]	IETF RFC 3619 (2003), Extreme Networks' Ethernet Automatic Protection Switching (EAPS).
[INF-8074i]	SFF Committee, INF-8074i Specification for SFP (Small Formfactor Pluggable) Transceiver, Rev 1.0, May 12, 2001
[INF-8077i]	SFF Committee, INF-8077i 10 Gigabit Small Form Factor Pluggable Module, Revision 4.5, August 31, 2005
[ITU-T G.813]	Recommendation ITU-T G.813 (2003), Timing characteristics of SDH equipment slave clocks (SEC).
[ITU-T G.823]	Recommendation ITU-T G.823 (2000), The control of jitter and wander within digital networks which are based on the 2048 kbit/s hierarchy.
[ITU-T G.8032]	Recommendation ITU-T G.8032/Y.1344 (2010), Ethernet ring protection switching.
[ITU-T G.8261]	Recommendation ITU-T G.8261/Y.1361 (2008), Timing and synchronization aspects of packet networks.
[ITU-T G.8262]	Recommendation ITU-T G.8262/Y.1362 (2007), Timing characteristics of synchronous Ethernet equipment slave clock (EEC).
[ITU-T V.11]	Recommendation ITU-T V.11 (1996), Electrical characteristics for balanced double-current interchange circuits operating at data signalling rates up to 10 Mbit/s.
[MEF 6.1]	MEF Technical Specification MEF 6.1 (2008), Ethernet Services Definitions - Phase 2
[MEF 10.2]	MEF Technical Specification MEF 10.2 (2009), Ethernet Services Attributes Phase 2
[MEF 12.1]	MEF Technical Specification MEF 12.1 (2010), Ethernet Services Layer - Base Elements
[MEF 22.1]	MEF Technical Specification MEF 22.1 (2012), Mobile Backhaul Phase 2
[SFP MSA]	Small Form-factor Pluggable (SFP) Transceiver Multi Source Agreement (MSA) (2000)

List of Contents

About this Book 1

Document Organization	about-1
Chapters	about-1
Conventions	about-2
Release History	about-2
Referenced and Related Documents	about-4

Chapter 0 Safety, Instructions, Statements

Safety Precautions	0-1
Power Precautions	0-1
Handling Precautions	0-1
Preventing Damage From Electrostatic Discharge	0-2
Card Protection	0-2
Grounding Procedure	0-2
Fibre Optic Precautions	0-3
Technical Instructions to User	0-4
Inspection	0-4
Commissioning	0-4
Cleaning	0-4
Quality	0-4
Repair	0-5
Disposal and Recycling	0-5
CE Conformity	0-5
Electromagnetic Immunity Statement	0-5
Instructions to User	0-5
Electromagnetic Emissions Statements	0-6

Chapter 1 Abstract

EDX100x Description	1-1
General	1-1
Application Areas for the EDX100x	1-2
Application Media Conversion	1-2
Application PON Network	1-3
Application Synchronous Ethernet	1-4
EDX100x Functions at a Glance	1-4
Error Recovery	1-4
Order Information	1-5
Accessories	1-6
Housings and Cables	1-6

SFPs (Small Form-factor Pluggable)	1-7
--	-----

Chapter 2 Getting Started

Delivered Parts	2-1
Preparing the Start-up	2-1
Operating Conditions	2-1
Ambient Conditions	2-2
EDX100x Mounting	2-2
Start-up of the EDX100x	2-3
Switching on the Device	2-3
Initial Configuration	2-3
Serial Port	2-3
Ethernet/IP-based Management Ports	2-3
Default IP-Address of the Device	2-4
Out-of-band MGMT Port	2-4
In-band Management Port	2-4
Supported Protocols	2-4
Using Agent-Card in Chassis	2-4

Chapter 3 Hardware

List of System Components	3-1
EDX100x Front Panels	3-2
LAN and LINE Interfaces	3-2
10/100BaseT (RJ45)	3-2
100BaseFX (SFP)	3-4
1000BaseX (SFP)	3-4
1000BaseTX (RJ45)	3-4
Common Indicators	3-5
'ON' LED	3-5
'ERR' LED	3-5
Front Views	3-6
EDX1000	3-6
EDX1002	3-7
EDX1008	3-8
EDX100x Rear Connector	3-9
RS-232 Interface	3-9
Power Supply	3-10

Chapter 4 Functionality

Media Conversion	4-1
Switching	4-1
LAN, LINE, and MGMT-Ports	4-2
VLANs	4-4

Introduction to VLAN	4-4
Supported VLAN-Modes of EDX100x	4-5
VLAN Aware	4-6
Example	4-6
Provider VLAN-Tagging	4-8
How it works	4-9
User & Access Administration	4-9
Direct Access to the EDX100x	4-11
Local RS-232 Interface	4-12
Local Ethernet Interface (Copper)	4-13
In-band Access	4-13
SSH connection	4-13
Indirect Access to the EDX100x	4-14
User Administration	4-15
Locally Stored Users	4-15
Rules for Usernames	4-15
Rules for Passwords	4-15
Security Issues	4-16
Auto-Logout	4-17
Time-Based Auto-Logout	4-17
Hardware-Based Auto-Logout	4-17
Management Port Configuration	4-18
IP Configuration	4-18
Management Port(s) "MGMT"	4-18
In-band Management Port	4-18
Default IP Configuration	4-18
DHCP and Manual Address Assignment	4-18
DNS-Support	4-19
Miscellaneous Features	4-19
Firmware-Update	4-19
Fault Propagation with LPT/RFD	4-20
Operation Mode of RFD	4-24
Slow Protocol (Link-Local) vs. UDP/IP	4-25
Status and Log-Messages of the LPT/RFD Stack	4-26
Rapid Spanning Tree Protocol	4-28
EAPS (Ethernet Automatic Protection Switching)	4-29
Line-Protection w/ EAPS	4-31
Auto Negotiation	4-31
Speed and Duplex	4-32

Chapter 5 EDX100x Control Software & gCLI

Menu Structure	5-1
Login Menu	5-3
Navigating	5-4

Select a Menu Entry	5-4
Page Update	5-4
Alarmlog	5-4
Exit	5-4
Overview to Keys	5-5
Main Menu	5-6
General System Information	5-7
Inventory	5-9
Administration	5-10
User & Access Administration	5-12
Users & Passwords	5-12
Add Account	5-14
Change Password	5-15
SSH Access	5-16
Add Key	5-17
SNMP Access Menu	5-18
SNMP Community Configuration Menu	5-19
SNMP Trap Receiver Configuration Menu	5-21
IP Configuration Menu	5-23
Entering VID and Priority	5-25
Date and Time Settings Menu	5-27
Reset System Menu	5-28
Software Download Menu	5-30
Configuration Handling Menu	5-33
Alarm Mgmt Configuration Menu	5-34
Interfaces and Ports Menu	5-37
Ethernet Ports	5-37
Ethernet Ports EDX1000	5-38
Ethernet Ports EDX1002	5-39
Ethernet Ports EDX1006e	5-39
Ethernet Ports EDX1008	5-40
Menu Options	5-40
Edit Port Settings	5-41
Ext. Settings (SFP Port)	5-42
Ext. Settings (Copper Port)	5-44
Priority Settings Menu	5-45
Port-Prio-Mapping	5-47
VLAN-Prio-Mapping	5-48
IP-Prio-Settings	5-50
Global Settings	5-51
SFP Ports	5-52
SFP Diagnostics	5-54
UART Configuration Menu	5-55
Operation Modes Menu	5-56
Ring Settings	5-58

LPT/RFD Settings	5-59
Edit Port Settings	5-62
VLAN Setup	5-63
VLAN Table Settings (Port View)	5-64
VLAN Table Settings (VLAN View)	5-66
Edit VLAN ID	5-67
Bandwidth Limitation Settings	5-68
Ingress Bandwidth Limitation	5-70
Egress Bandwidth Limitation	5-72
Rapid Spanning Tree Settings Menu	5-74
RSTP Global Settings	5-75
RSTP Port Settings	5-76
Edit RSTP Port Settings Menu	5-77
Performance Monitoring	5-78
Ethernet Performance Data	5-78
Read detailed Ethernet Counter	5-80
In Counters Menu	5-81
In Problem Packets Menu	5-83
Out Counters Menu	5-84
Histogram Counter	5-85
Out Problem Packets Menu	5-87
Set Histogram Options	5-88

Chapter 6 SNMP and MIBs

SNMP Access Generally	6-1
SNMPv1	6-2
SNMPv2c	6-2
Traps	6-2
Installation Prerequisites	6-2
Preparing the SNMP Management System	6-3
SNMPv1/v2c Agent	6-3
Management Information Bases (MIBS)	6-4
axg2.mib	6-5
axg2-agent.mib	6-5
axg2-device.mib	6-5
axg2-EDX1000-as.mib	6-5
axg2-EDX1000-ds.mib	6-5

Chapter 7 axCLI via SCX2e

Introduction to axCLI	7-1
CLI Editor Features	7-1
Context Sensitive Help	7-1
Command Syntax Check	7-2
Command Completion	7-2

Hot Keys	7-2
Commands	7-3
Usage of axCLI	7-4
Rackview - Mode	7-5
Example SELECT	7-5
SELECT by rack/slot address	7-5
SELECT by name	7-5
Cardview - Mode	7-5
Example CONFIG	7-6
Quick Usage Guide for CLI-Commands	7-8
Menu-Structure (Directory-Tree) of EDX100x	7-9

Appendix A Technical Specifications

EDX100x Hardware Specification	A-1
EDX100x Software Specification	A-5

Appendix B Exercise Troubleshooting

Is the System Operating Correctly?	B-1
Meaning of Further Indicator Displays	B-2

Appendix EC EC Declaration of Conformity

Declaration of Conformity	EC-1
---------------------------------	------

List of Figures

Figure 1-1	Media Converter	1-2
Figure 1-2	PON Infrastructure	1-3
Figure 1-3	SyncE	1-4
Figure 4-1	Connection LAN - LINE - MGMT	4-3
Figure 4-2	Forwarding Matrix w/ disabled management options	4-4
Figure 4-3	Provider VLAN Tagging Diagram	4-9
Figure 4-4	P-VLAN configuration	4-9
Figure 4-5	Direct and Indirect Access	4-10
Figure 4-6	Management Protocol Stack	4-12
Figure 4-7	Secure Shell to EDX100x	4-14
Figure 4-8	LPT/RFD Application	4-22
Figure 4-9	LPT/RFD Configuration Example	4-24
Figure 4-10	EDX1000 Ring Protection	4-30
Figure 4-11	Ring Protection activated	4-31
Figure 6-1	The SNMP ax-Generation 2 MIB Tree	6-4

List of Tables

Table 0-1	Effects of Cleaning Liquids	0-4
Table 1-1	Order Matrix	1-5
Table 1-2	Accessories Housing & Cables	1-6
Table 1-3	Accessories SFPs	1-8
Table 2-1	Ambient Conditions	2-2
Table 3-1	System Components	3-1
Table 3-2	Electrical Interfaces	3-3
Table 3-3	EDX1000 Front View	3-6
Table 3-4	EDX1002 Front View	3-7
Table 3-5	EDX1008 Front View	3-8
Table 3-6	EDX1006e Front View	3-9
Table 3-7	Transmission Rate of the RS-232 Interface	3-10
Table 4-1	Behaviour for Untagged Packets on LAN-port 1	4-6
Table 4-2	Behaviour for Tagged Packets on LAN-port 1	4-7
Table 4-3	Behaviour for Untagged Packets on LINE-port	4-7
Table 4-4	Behaviour for Tagged Packets on LINE-port	4-8
Table 4-5	LPT/RFD Configuration Example	4-23
Table 4-6	LPT/RFD Status	4-26
Table 4-7	Interface States due to LPT/RFD	4-27
Table 4-8	Settings Auto-Negotiation	4-32
Table 5-1	Overview to key-strokes	5-5
Table 5-2	EDX100x Menu Options	5-6
Table 5-3	General System Information Menu Options	5-8
Table 5-4	Inventory Menu Options	5-9
Table 5-5	Administration Menu Options	5-11
Table 5-6	User Administration Menu Options	5-12
Table 5-7	Users & Passwords Menu Options	5-13
Table 5-8	Add Account Menu Options	5-14
Table 5-9	Change Password Menu Options	5-16
Table 5-10	SSH Access	5-17
Table 5-11	SNMP Access Menu Options	5-18
Table 5-12	SNMP Community Configuration Menu Options	5-19
Table 5-13	Edit SNMP Community Menu Options	5-20
Table 5-14	SNMP Trap Receiver Menu Options	5-21

Table 5-15	Edit SNMP Trap Receiver Menu Options	5-22
Table 5-16	IP-Configuration Menu Options	5-23
Table 5-17	Entry of VID and Priority	5-26
Table 5-18	Date and Time Settings Menu Options	5-27
Table 5-19	Reset System Menu Options	5-29
Table 5-20	Software Download Menu Options	5-30
Table 5-21	Configuration Handling Menu Options	5-34
Table 5-22	Alarm Management Configuration Menu Options	5-36
Table 5-23	Interfaces and Ports Menu Options	5-37
Table 5-24	Ethernet Ports Menu Options	5-40
Table 5-25	Edit Port Settings Menu Options	5-41
Table 5-26	Ext. Settings Menu Options	5-43
Table 5-27	Ext. Settings Menu Options	5-44
Table 5-28	Priority Settings Menu Options	5-46
Table 5-29	Port-Prio-Mapping Menu Options	5-48
Table 5-30	VLAN-Prio-Mapping Menu Options	5-49
Table 5-31	IP-Prio-Settings Menu Options	5-50
Table 5-32	UART Configuration Menu Options	5-55
Table 5-33	Operation Modes Menu Options	5-57
Table 5-34	Ring settings Menu Options	5-58
Table 5-35	LPT/RFD Settings Menu Options	5-60
Table 5-36	LAN Port-States due to LPT/RFD	5-61
Table 5-37	LPT/RFD Edit Port Settings Menu Options	5-62
Table 5-38	VLAN Setup Menu Options	5-64
Table 5-39	Edit Port VLAN Settings Menu Options	5-65
Table 5-40	VLAN View Settings Menu Options	5-66
Table 5-41	VLAN View Settings Menu Options	5-67
Table 5-42	Ingress Bandwidth Limitation Menu Options	5-71
Table 5-43	Egress Bandwidth Limitation Menu Options	5-73
Table 5-44	Rapid Spanning Tree Settings Menu Options	5-74
Table 5-45	RSTP Global Settings Menu Options	5-75
Table 5-46	Rapid Spanning Tree Port Settings Menu Options	5-76
Table 5-47	Edit RSTP Port Settings Menu Options	5-77
Table 5-48	Ethernet Performance Data Menu Options	5-79
Table 5-49	Read Detailed Ethernet Counter Menu Options	5-80
Table 5-50	In Counters Menu Options	5-81
Table 5-51	In Problem Packets Menu Options	5-83

Table 5-52	Out Counters Menu Options	5-84
Table 5-53	Outgoing Packet Shapes Menu Options	5-86
Table 5-54	Out Problem Packets Menu Options	5-87
Table 6-1	SNMP access levels	6-3
Table 7-1	EDX100x CLI Hot Keys	7-2
Table 7-2	EDX100x CLI Commands	7-3
Table 7-3	Menu Indicators and corresponding CONFIG Commands	7-6
Table 7-4	Special CONFIG Commands	7-8
Table 7-5	Quick Reference	7-8
Table A-1	Number of Interfaces	A-1
Table A-2	Power Requirements	A-2
Table A-3	Technical Data of the Interfaces	A-2
Table A-4	Display Functions	A-4
Table A-5	Mechanic and Environment	A-4
Table A-6	µController and Clock	A-5
Table A-7	Technical Data of the EDX100x - Software	A-5
Table B-1	Indicators Displays in Operating State	B-2

Chapter 0

Safety, Instructions, Statements

Safety Precautions

The following sections provide the safety precautions for the supplied device. You must always observe the power precautions for the device. You must follow all warning notes to ensure that the procedures are performed safely. You must follow all caution notes to ensure that the device is operated correctly.

WARNING: Serious injury or loss of life is possible, if instructions are not carried out.

CAUTION: Serious damage or destruction is possible, if instructions are not followed.

NOTE: Before installing the device find out if any local technical rules must be observed. These may be defined by ANSI, ITU-T, IEC, your PTT, or other similar organizations.

Power Precautions



WARNING:

- Disconnect the power cord before opening the device.
- Always plug the power cords into properly grounded receptacles. An improperly wired receptacle could place hazardous voltage on the accessible metal parts of the device.
- Use only approved power cords.
- Use only manufacturer supplied power supplies.
- The power supply must match the power specifications for the device.
- Do not work on the equipment during periods of lightning activity.

Handling Precautions

Note: Precautions for transporting, installing, and operating the device:

- Avoid excessive shocks and vibrations. Install shock absorbers, if you need to use the device for mobile applications.
- Avoid contact with any liquid (e.g. water) or dust or dirt.
- Avoid exposing the device to excessive direct sunlight.

- Ensure sufficient cooling of the device.
- Prevent loose items from falling into the device.
- Avoid damage to components when installing or setting switches or jumpers of the device.
- Always place protective covers on all fibre optic cables and connectors that are not in use to prevent breakage and contamination.
- Inspect all fibre optic connections and clean contaminated surfaces before use.
- Attach a wrist strap and follow ESD procedures, see next paragraph.

Preventing Damage From Electrostatic Discharge



CAUTION: Discharge of static electricity (ESD) can damage or degrade electronic components. The electrostatic potential of a person can be several thousand Volt and a discharge to semiconductor components may have severe consequences. Observe the precautions below when you are handling any hardware with electronic components.

Card Protection

Each card is shipped in a separate, reusable, and anti-static shielding bag. Leave each card in its bag until you are ready to install it into the system. Do not remove the card from its bag unless you are grounded. Do not place a bag on exposed contacts where it can cause short circuits.

Grounding Procedure

Before attempting to install or remove any part of the chassis, ensure that you, the equipment chassis, and the rack mount cards are at ground potential to prevent electrostatic discharge (ESD). Electrostatic discharges can damage the components of the system. To place yourself at ground potential, connect the chassis with a ground wire or via the power cord with a grounded mains socket and clip your wrist strap to the chassis.

The following advice will help you to prevent ESD damage to electrical components:

- Always use an ESD wrist strap with a metal clip for grounding.
- Limit your movement as much as possible. Movement can cause a build-up of static electricity.
- Handle the system and its components carefully. Never touch the circuitry. Place your hands only on the edges, rails, or frame of the unit.
- Touch a spare component - while it is still in the anti-static wrapping - to an unpainted metal portion of the chassis for at least two seconds. This allows the static electricity to discharge harmlessly from your body and the spare.
- Install the device directly into the chassis after removing it from the anti-static wrapping. Do not remove the anti-static wrapping until you are ready to start the installation. If you must set down an unwrapped spare, set it down on an anti-static mat or on its anti-static wrapping.

Caution: Do not place the spare component on the top of the chassis, rack, or on a metal table. Either action could cause severe damage to the spare.

- Set down cards with their component sides face up.
- Be aware of weather conditions. Cold weather increases the likelihood of static electricity build-up.
- Be aware of your own conductivity level. Wear ESD shoes to diminish personal static electricity build-up. Wear e.g. an electrostatic dissipative lab coat.

Fibre Optic Precautions



Caution: An optical fiber may carry (invisible) light from the remote system.

This device may contain Laser Class 1 components, like laser transmitters or light emitting diodes LED (refer to technical data). Operating components emits (invisible) laser radiation. Be careful when you are working with these components. The following safety precautions must be followed when working with fibre optics and Laser Class 1 components:

WARNING: Do not look into the fibre optic output. Looking into the fibre optic output can cause injury to the eye. When observation is necessary eye protection must be worn and precautions must be taken to avoid exceeding the limits recommended in ANSI Z136.1-1981.

WARNING: Use caution when working with the laser components of the device. The device is designed to protect the user against optical powers beyond laser class 1.

WARNING: Ensure that the incoming signal from the remote device does not exceed the power defined for laser class 1 when the cabling is disconnected. The device will also become unsafe, if any unsafe equipment is connected to the system.

WARNING: Do not disconnect the fibre optic cables while power is applied. Disconnecting the fibre optic cables could expose the user to optical powers beyond laser class 1.



Caution: Use Of Controls Or Adjustments Or Performance Of Procedures Other Than Those Specified Herein May Result In Hazardous Laser Light Exposure.

CAUTION Laser Class 1. Complies with FDA radiation standards, 21CFR subcategory J. DANGER (Invisible) laser radiation when open and / or interlock defeated. Avoid direct exposure to beam!

Technical Instructions to User

Do not use this product for other applications than suggested in this manual!

The international standards and the technical rules of your local PTT company must be observed.

All interface cables to this equipment must be shielded and designed in accordance with proper EMI techniques to ensure compliance with EMC requirements. arcutronix will provide cable shielding specifications on request.

Inspection

Before commissioning, check the content of the consignment for completeness and note whether any damage has occurred during transport. If so, do not use the parts and contact your arcutronix representative.

Commissioning

Work may be carried out only by qualified personnel. The relevant precautions must be taken.

Cleaning



To clean the outer surfaces, use a soft damp (not wet) cloth. Do not let moisture go inside. Please consider the properties of the housing and other material used!

Table 0-1 Effects of Cleaning Liquids

Valuation	ABS/ABS+PC/PC/PPE+PS
well resistant	water, aqueous saline solutions, sud, diluted acid and alkali
conditionally resistant	alcohol, aliphatics, oil and fat
not resistant	concentrated mineral acid, aromatic and halogenated hydrocarbon, ester, ether, ketone

Quality



The quality management of arcutronix is certified to DIN ISO 9001:2000.

This product is manufactured to the arcutronix quality standards

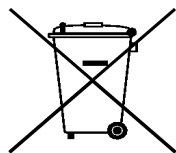
Repair

There are no repairable parts in the device. Defective parts must be sent to arcutronix GmbH for repair. The power supplies of a device may contain fuses. Blown-up mains fuses must be replaced by fuses of the same type and the same ratings. Using repaired fuses or short-circuit the fuse holder are not permitted.

Disposal and Recycling



This symbol on the product or on the packaging indicates that it can be recycled. To save our environment please hand it over to your next recycling point.



This symbol on the product or on its packaging indicates that it shall not be treated as household waste. Instead it shall be handled over to the applicable collection point for the recycling of electronic equipment.



For more detailed information about recycling contact your local city office, your waste disposal service or where you purchased the product.

CE Conformity



arcutronix products complies with the European standard regulation. They are tested to the Council guideline for harmonizing the legal regulations of the member states on electromagnetic compatibility.

Electromagnetic Immunity Statement

This equipment has been tested and found to comply with the limits of EN 55022 and EN 55024 (Electromagnetic Immunity for heavy industry).

Instructions to User

All interface cables to this equipment must be shielded and designed in accordance with proper EMI techniques to ensure compliance with EMC requirements. arcutronix will provide cable shielding specifications on request.

Electromagnetic Emissions Statements

To achieve satisfactory EMC performance, all interface cables to this equipment must be shielded and designed in accordance with proper EMI techniques. Rack mount cards has to be inserted into the designated chassis. Chassis slots that are not used have to be covered with a blanking plate. The chassis must be bonded to earth. This is usually achieved by installing the power cord to the chassis. An extra earth terminal may be provided. If this device is used in a residential setting, resulting interference must be corrected by the user. Any user modification made to the unit voids the user's authority to operate the unit under the FCC rules.



WARNING: This is a Class A product. In a domestic environment, this product may cause interference in which case the user may be required to take adequate measure. 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.

United States Federal Communications Commission (FCC) Electromagnetic Emissions Statement

WARNING: This equipment generates, uses, and can radiate radio frequency energy and if not installed and used in accordance with the instructions in this manual, may cause interference to radio communications. It has been tested and found to comply with the limits for a Class A computing device pursuant to Subpart J of Part 15 of the FCC Rules, which are designed to provide reasonable protection against such interference in which case the user at his own expense will be required to take whatever measures may be required to correct interference.

Canadian Department of Communications (DOC) Statement

WARNING: This equipment generates, uses, and can radiate radio frequency energy and if not installed and used in accordance with the instructions in this manual, may cause interference to radio communications. This digital apparatus has been tested and does not exceed the Class A limits for radio noise for digital apparatus set out in the DOC Radio Interference Regulations. The regulations are designed to provide reasonable protection against radio noise interference in which case the user at his own expense will be required to take whatever measures may be required to correct interference.

European Communities

WARNING: This equipment has been tested and found to comply with the limits of CISPR 22 and EN 55022 Class A for information technology equipment. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications.

Chapter 1

Abstract

EDX100x Description

General

The EDX100x is a full managed next generation high density Ethernet Converter with up to eight switched 10/100BaseTx Ethernet ports and two GbE (up-link) ports. The up-link ports are implemented using SFP (Small Form Pluggable) modules, whereby maximum flexibility is provided regarding the interface type which can be copper or fibre optic. Even single fibre transmission is possible using SFPs with WDM technology.

With the EDX100x flexible universal applications can be created for Layer 2 and Layer 3 Ethernet networks. For example, in point-to-point topologies eight customer applications at 100Mbps each can be switched and converted into one 1000BaseSX/LX optical signal. By cascading the EDX100x via the second GbE port even the number of interfaces can be extended. Also applications requiring 1:1 redundancy can easily be built by using both SFP ports.

In addition, by supporting Ethernet Automatic Protection Switching (EAPS, according to [IETF RFC 3619]) even Ethernet ring topologies can be established. EAPS is similar to the Spanning Tree Protocol (STP), but offers the advantage of recovering link failures in significantly less time (<50ms) than STP (several seconds) or even Rapid Spanning Tree (<1sec).

Its extended management features offer the customer a product that fulfils current standard network requirements. The EDX100x offers extended features such as performance monitoring and in-band management.

Due to VLAN tagging (acc. [IEEE 802.1Q]) the EDX100x is able to transparently interconnect networks of different customers while maintaining complete isolation between their networks. Using the tunnelling feature ([IEEE 802.3ah] = QinQ), service providers can use a single VLAN to support customers who have multiple VLANs. Additionally, priority marking (acc. [IEEE 802.1Q]) and tamper-proof bandwidth limitation allow providers to offer different classes of service and to sell end customers certain Service Level Agreements (SLAs).

Moreover, as part of arcutronix Multi Service System, the EDX100x benefits from the future-proof system architecture and management features. This includes various chassis and housing options with optional redundant power supplies and centralized management via a rack agent (SCX2). Thus, by using the IP forwarding feature the entire management system can easily be maintained and supervised by carriers or ISPs via a single access point.

The device is available as a 3RU rack mount card, which can be modified without the slightest effort to a stand-alone unit by using arcutronix' unique table-top housing SHX3.

Application Areas for the EDX100x

The basic functionality of the EDX100x allows plug-and-play installations for switched networks and/or converting Copper-Ethernet into Fibre-Ethernet and vice versa. Easy configuration via management access of local and remote devices allows quick installation and 24h-supervision of the units. Traps can be send in case of failure and alarm-connectors can be triggered to achieve maximum supervision.

Application Media Conversion

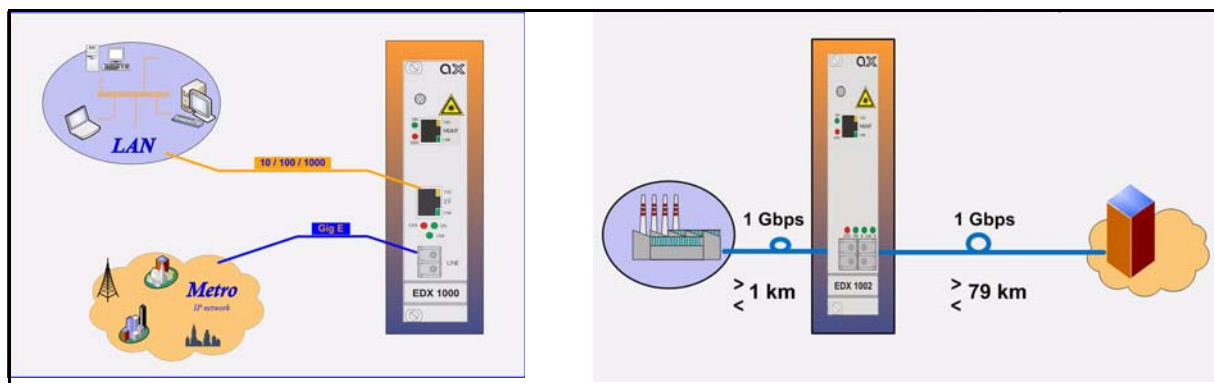


Figure 1-1 Media Converter

Copper-to-Fibre and Fibre-to-Fibre conversion is possible to adopt media, wavelength, type of fibres and distances. All fibre ports are based on SFP, so any type of optical GigE can be supported, including XWDM.

In the figure above, EDX1000 and EDX1002 are used for media conversion.

Application PON Network

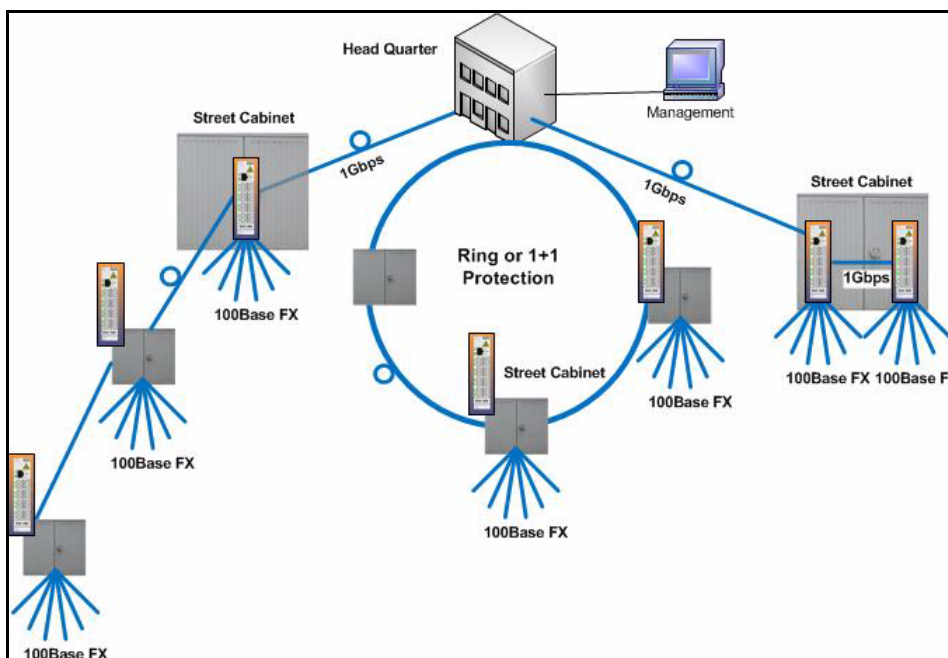


Figure 1-2 PON Infrastructure

In a typical PON network, a tree is spanned to distribute the information from a OLT to the ONUs. With the help of EDX1006 this can be done in a better way by active components. And not only trees can be build up, but also self-protecting rings and location with higher density.

Application Synchronous Ethernet

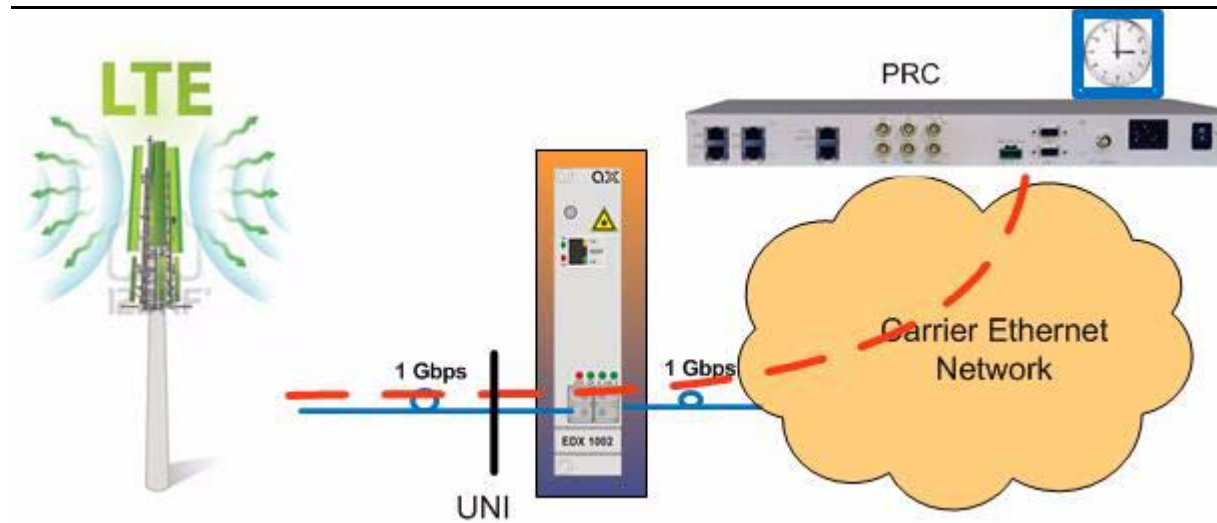


Figure 1-3 SyncE

The EDX100x with SyncE can be synchronized to an external source via one of the GigE-ports. This port is called the “Master-Clock” port. All other ports, GigE as well as FE ports, are using the recovered clock information and can distribute it to the successive units. The synchronisation feature makes it perfectly fitting for mobile back-hauling of the 4G LTE standard.

EDX100x Functions at a Glance

- TX/FX media conversion with LPT/RFD support.
- Fibre and copper Ethernet ports
- 1000Mbps and 100Mbps interface speed.
- Variants with different port numbers available.
- Switching with VLAN and (R)STP support.
- Fast link failure recovery for point-to-point or ring topology.
- Various management access options:
 - Serial RS-232,
 - Telnet via TCP/IP,
 - SSH via TCP/IP,
 - SNMP via TCP/IP.
- In-band and out-of-band management capability.

Error Recovery

If problems occur or if error messages will be displayed, please check whether the system has been installed as described in the installation instructions and whether all con-

figuration rules have been followed. Please also refer to Appendix B, Exercise Troubleshooting.

Order Information

NOTE: All order matrices will be regularly updated. Asked your arcutronix representative for the latest publications.

The order matrix shows the available variants of the EDX - Ethernet Demarcation. Further options are possible on request.

Table 1-1 Order Matrix

Art.- No.	Short Name	Description
0716-2001	EDX1000	Broadband Ethernet Demarcation: <ul style="list-style-type: none">• 1x GbE (1000BaseLX/SX/T), pluggable SFP module (no module included);• 1x GbE (10/100/1000BaseTx) port, RJ45 conn.;• compatible IEC 60870-5-104;• MGMT-port: 1x FE (10/100BaseT), RJ45 conn.;• 3RU rack mount card.
0716-2101	EDX1002	Broadband Ethernet Demarcation: <ul style="list-style-type: none">• 2x GbE (1000BaseLX/SX/T), pluggable SFP modules (no modules included);• compatible IEC 60870-5-104;• MGMT-port: 1x FE (10/100BaseT), RJ45 conn.;• 3RU rack mount card.
0716-3200	EDX1008	Broadband Ethernet Demarcation: <ul style="list-style-type: none">• 2x GbE (1000BaseLX/SX/T), pluggable SFP modules (no modules included);• 8x 10/100BaseTx (RJ45), IEC 60870-5-104;• compatible IEC 60870-5-104;• 3RU rack mount card.
0716-4600	EDX1006e	Broadband Ethernet Demarcation for extended temperature range: <ul style="list-style-type: none">• 2x GbE (1000BaseLX/SX/T), pluggable SFP modules (no modules included);• 6x FE (100BaseFX), pluggable SFP modules (no modules included);• compatible IEC 60870-5-104;• MGMT-port: 1x FE (10/100BaseT), RJ45 conn.;• hardened version: -25...+70°C;• 3RU rack mount card.

Accessories

Housings and Cables

The arcutronix Multi Service System offers a range of accessories for an easy and space saving installation of your device into 19" cabinets or as desktop / wall-mount installation.

Table 1-2 *Accessories Housing & Cables*

Art.- No.	Short Name	Description
0805-9000	SRX10	Rack mount shelf: <ul style="list-style-type: none">• 19" chassis,• Height: 3RU,• 10 slots for line-cards,• 1 slot for management,• 2 slots for modular AC (115/230V) and DC (-48V/-60V) power supplies.
0805-9500 (obsolete!)	SRX24	Rack mount shelf: <ul style="list-style-type: none">• 19" high density chassis,• Height: 6RU,• 24 slots for line-cards,• 1 slot for management,• 2 slots for modular AC (115/230V) and DC (-48V/-60V) power supplies.
0805-9010	SRX3	Rack mount stand-alone housing: <ul style="list-style-type: none">• 19" chassis,• Height: 1RU,• 3 slots for line-cards,• VT100 Management port (D-Sub9),• with alarm contact, ventilation,• mains supply: AC (115/230V).
0805-9110	SRX3plus	Rack mount housing with agent-functionality: <ul style="list-style-type: none">• 19" chassis,• Height: 1RU,• 3 slots for line-cards,• integrated management card• 2x FE management port (SFP + RJ45),• with alarm contact, ventilation,• AC (115/230V) and DC (-48V/-60V) power supplies.
0717-9001 (obsolete!)	SHX3-7W	Stand-alone housing: <ul style="list-style-type: none">• 1 slot for 3RU line-card,• VT100 Management port (D-Sub9),• Alarm contact,• integrated wide range power supply,• mains supply: 48VDC...110/230VAC.

Table 1-2 Accessories Housing & Cables (continued)

Art.- No.	Short Name	Description
0717-9101	SHX3-15W	Stand-alone housing: <ul style="list-style-type: none"> • 1 slot for 3RU line-card, • max. 15W power consumption, • VT100 Management port (D-Sub9), • alarm contact, • with ventilation, • integrated wide range power supply, • mains supply: 48VDC...110/230VAC, • power jack included.
0717-9401	SHX3-10W	Stand-alone housing: <ul style="list-style-type: none"> • 1 slot for 3RU line-card, • max. 10W power consumption, • VT100 Management port (D-Sub9), • alarm contact, • no ventilation, • integrated wide range power supply, • mains supply: 48VDC...110/230VAC, • power jack included.
0500-001	PC-E	Power cord, European plug.
0500-002	PC-B	Power cord, Great Britain plug.

SFPs (Small Form-factor Pluggable)

The EDX100x-series offers a number of SFP-slots (Small Form-factor Pluggable) for usage of a wide range of different optical transceivers. The small form-factor pluggable (SFP) is a compact, "hot-pluggable" optical transceiver used in optical communications for both telecommunication and data communications applications. The SFP transceiver is specified by a multi-source agreement ([SFP MSA]) between competing manufacturers.

Using the right SFP, the EDX100x can be used in different optical environments with different fibre-types (single-mode or multi-mode) and a wide range of distances.

Two speed-rates of SFP-based interfaces are available: 100MBit/s and 1000MBit/s. For both speed-rates, arcutronix offers a bunch of different SFPs. Depending on the present EDX100x, the number of SFP-slots and available speed-rates differ:

Device	# of 100BaseFX-SFP-slots	# of GigE-SFP-slots	Remark
EDX1000	0	1	-
EDX1002	0	2	-
EDX1006e	6	2	-
EDX1008	0	2	-

NOTE: It is not possible to use 100BaseFX SFP in GigE-SFP slots and vice versa!

EDX100x does support all optical modules, which are designed according the [SFP MSA]. For safe operation, arcutronix recommends the SFPs below. Please ask for special types, if required.

Table 1-3 Accessories SFPs

Short Name	Description
Optical Transceiver:	
100Base-FX:	
SFP-155-S13-10	Optical SFP Interface Module: 1310nm SM FO; Fast E, 155 Mbps transceiver; pluggable SFP footprint; LC connector; 10km.
SFP-155-S13-15	Optical SFP Interface Module: 1310nm SM FO; Fast E, 155 Mbps transceiver; pluggable SFP footprint; LC connector; 15km
SFP-155-S13-40	Optical SFP Interface Module: 1310nm SM FO; Fast E, 155 Mbps transceiver; pluggable SFP footprint; LC connector; 40km.
1000Base-SX/LX/LH/ZX	
SFP-1.25-S13-10	Optical SFP Interface Module: 1310nm SM FO; 1xFC, 1.25 Gbps transceiver; pluggable SFP footprint; LC connector; digital diagnostics; 10km.
Copper Transceiver (Triple-Speed SFP):	
SFP-1.25e	Electrical SFP Interface Module: Pluggable SFP module, for data rates of 1.25Gb/s bi-directional data links. - 1000BASE-T Copper port, RJ45 connector - compatible with the Gigabit Ethernet and 1000BASE-T standards as specified in IEEE 802.3 - digital diagnostic supported.

Chapter 2

Getting Started

For the start-up of the EDX100x please follow the directions in this chapter. You must keep the operating conditions specified for the devices. In the following read about the start-up preparation, the start-up itself, and the possibility to automate the start-up.



WARNING: Read the safety notes at the beginning of this manual carefully before you start the device!

Delivered Parts

Please check if all the items listed below are included in your delivery. Your delivery includes:

- One EDX100x system
- optional: Single-Slot Housing SHX3
- optional: Power Cord for AC

Preparing the Start-up

Before you switch on the device you need to check the operating conditions and install the EDX100x into the chassis or the single-slot housing.

Operating Conditions

Read the operating conditions specified in this section carefully to avoid damages to the device or connected systems.

Ambient Conditions

The ambient conditions, which must be maintained for the EDX100x, are shown in Table 2-1.

Table 2-1 Ambient Conditions

Operating Temperature	EDX1000, EDX1002, EDX1008: 5°C to +40°C EDX1006e: -25C to +70C
Max. Relative Humidity (non-condensing)	85% (30°C)
Input Voltage	+5V DC
Power Consumption	< 10 VA ⁱ

i. Depends on the given variant and the SFP plugged. Please check Appendix A, EDX100x Hardware Specification for details.

CAUTION: If operating limits are exceeded, malfunctions and permanent damage to the equipment may result.

NOTE: In order to operate the various interfaces, please ensure that the plugs are firmly engaged in the sockets.

EDX100x Mounting

To mount the EDX100x into the chassis please follow the subsequent step-by-step instructions.

1. Disconnect all cables from the EDX100x before mounting the device.
2. Place the EDX100x right way up on a table with the front panel looking in your direction.
3. Insert the EDX100x that way into the chassis. Mount the EDX100x to the chassis using the provided screws.
4. Connect the interface cables to the EDX100x.

Start-up of the EDX100x

Switching on the Device

The EDX100x does not have the capability to be directly powered by either AC or DC input. A power supply is always required to convert the provided (external) power into the 5VDC, which is required by the EDX100x. The power supply may be a fixed or removable part of the chassis/housing, where the EDX100x is mounted. As soon as the power supply unit is applied with external power, the agent-slot is powered and a plugged EDX100x will start.

After power is connected to either chassis or housing, the device boots its software automatically. No extra switch has to be activated. During the boot-process all internal components are roughly tested and the device is initialized. The last setup is restored; in case the unit starts the first time, it starts with the factory defaults.

The boot-process is indicated by the blinking ON-LED and takes about 2 minutes. At the end of this process the unit is fully operational. If there are any settings, which need special adoption, different to the default, the configuration can start now.

Initial Configuration

The initial configuration can be done like all other configuration settings. There are several ways to get contact to the device, which are explained in more detail later on. Here, only a short overview to the possible options of access are given.

Serial Port

In the single-slot, dual-slot and triple-slot housing a serial port is available, which can be used. A DSUB9 connector (female) is available to connect the chassis to your PC, laptop, etc. The serial port acts as DCE, so a straight serial cable can be used. The data-rate is (by default): 57.6, 8N1.

Username = admin; Password = private

Any terminal program can be used for configuration. A graphical command line interface (gCLI) is presented to the user. See Chapter 5, EDX100x Control Software & gCLI for details.

Ethernet/IP-based Management Ports

A lot of protocols can be used for configuration, which are based on the TCP/IP stack: Telnet, SSH and SNMP. The access to these protocol-stacks are achieved via the available management interfaces. These are either the out-of-band interface (called "MGMT") or the in-band management interface, which is using the LINE port(s) and a dedicated VLAN (4094).

Default IP-Address of the Device

Per default the EDX100x asks for an IP address via DHCP. The DHCP server has to be connected to “MGMT” port or one of the “LINE” ports of the EDX100x. As long as there was no DHCP available, yet, the unit uses the following default IP-address:

Default IP-address: 192.168.1.100/24

NOTE: As long the setting “IP Address Assignment” is kept on “Via DHCP Server”, the units will always use these IP-address after a restart.

If the IP-address shall be assigned manually, then the settings can be changed and a fixed IP-address can be assigned in the configuration menu.

Out-of-band MGMT Port

All Ethernet interface of the EDX100x, which are configured to type “MGMT” are out-of-band management interface. A direct access (without VLAN) is possible. The different variants, do have out-of-band management ports:

- EDX1000, EDX1002, EDX1006e: Dedicated port MGMT, RJ45, 10/100BaseT.
- EDX1008: Port #1, RJ45, 10/100BaseT.

In-band Management Port

All devices support in-band management access via the LINE port(s). By default, the in-band management is enabled and the VLAN-ID 4094 is used to separate the in-band traffic from user’s payload.

In-band management is a direct management connection of the device EDX100x to a NOC. This is different to the “ax remote management”, which is the connection to the superior ax-agent card (SCX2e).

Supported Protocols

When using the in-band or out-of-band management interfaces, three protocol applications can be used:

- SNMP
- Telnet
- SSH (secure shell)

Using Agent-Card in Chassis

In arcutronix multi-service shelf SRX10 and SRX3plus, the EDX100x is managed via an agent-card (SCX2e). The agent-card can be accessed directly by on-board Ethernet interfaces and will grant a single point-of-access to the whole chassis. This spares IP-addresses and cables. The agent-card offers a lot of benefits, like SW-update, several management protocols and a http-based web-GUI for very comfortable operation.

The feature “ax-remote management” offers access not only to the EDX100x-cards in the agent’s chassis, but also to all directly connected “remote” EDX100x-cards. The

ax-remote management is different to the “in-band management”, so it also uses the FO link between “local” and “remote” EDX100x. A different VID is used to separate the traffic. ax-remote management and in-band management can be used in parallel, so it does not make many sense.

A detailed overview on the features and operation of the agent-card is given in the [axManual_SCX2e], which is available on the web-site of arcutronix or via your local representative.

NOTE: The password of the agent-card can vary from the settings of the EDX100x, presented in this document.

Chapter 3

Hardware

In this chapter beside a list of system components you will find a description of the function indicators and external interfaces for the EDX100x.

The EDX100x is a compact unit. All external connection points for data lines and control elements are accessible on the front panel. The indicator elements are also on the front panel.

List of System Components

The EDX100x contains the following system components:

Table 3-1 System Components

Component	Description
Switch	The Ethernet switch 88E6095F from Marvell supports up to 8 Fast and 3 Gigabit Ethernet interfaces and integrates the PHY's. One of the interfaces is directly connected to the LCP to realize management access. The Fast Ethernet interfaces support 10/100BaseTx while the Gigabit interfaces allow the use of SFPs (1000BaseX or copper SFP). Additional functionality includes bandwidth limitation per port and full VLAN support. The data will be transmitted non-blocked. Therefore, full data rate can be provided on all interfaces.
Interfaces	Different numbers of interfaces are available on the various units. All variants do have 2 GigE ports and one (local) management port. A serial interface is available on the rear connector. It is only usable in the single-slot, dual-slot and triple-slot housings.
Processor (Local Control Point, LCP)	The EDX100x is based on a PowerQuick platform with an MPC852T from Freescale. This CPU integrates a 32 bit power PC architecture and is clocked with 100MHz. The CPU is connected to the Ethernet switch via a Fast Ethernet controller.

Table 3-1 System Components (continued)

Component	Description
Flash	The 16Mbyte non-volatile flash memory contains the program code for the operating functionality of the device as well as the system configuration. The software can be updated or added directly through the interfaces of the device. Therefore, it is not necessary to replace memory modules (for example EPROMs).
SDRAM	The 64Mbyte main memory allows an high efficient operation of the CPU. The operating system (an embedded Linux distribution) will first be copied from the Flash memory to the SDRAM and then started from there.
DC/DC Converter	The DC/DC converter generates all required voltages from the 5VDC, coming from backplane. The DC/DC-Converter does include the ax power management, which makes sure a line-card can only start, when sufficient power is available for the unit.

EDX100x Front Panels

The EDX100x series offers on the front side the connectors for user and line interfaces plus a number of LEDs to show status of unit and interfaces.

Depending on the given variant, the front panel looks slightly different. In the following the common parts and the differences of the front panel will be depicted.

LAN and LINE Interfaces

The EDX100x series provides 10/100BaseT, 10/100/1000BaseT, 100BaseFX and 1000BaseX interfaces.

10/100BaseT (RJ45)


The EDX100x can have up to 8 electrical Fast-Ethernet ports. For each interface separate indicators give information on the Link state (LNK) and 10/100BaseTX (100). The device negotiates the operating mode of the corresponding interface automatically with the remote station using Auto Negotiation (if activated). Half-duplex and full-duplex connections are supported. You will find more configuration information in the section "Ethernet Ports" on page 5-37. The data rate is either 10 Mbit/s or 100 Mbit/s. The pro-

ocol is according to [IEEE 802.3] Clause 14 and Clause 25. Auto negotiation and auto crossover are supported.

Table 3-2 Electrical Interfaces

Item	Values
Standards:	[IEEE 802.3], [IEEE 802.1Q]
Ports:	up to 8x 10/100BaseT
Data rate:	10Mbit/s or 100Mbit/s auto negotiation, full- or half-duplex, bandwidth limitation
Range:	Up to 100m over UTP-5 cable
Connector	RJ-45 8-pins:

The connector is a RJ-45 plug with 2 LEDs, which indicate established Link (green LED on the left side) and the data rate (green LED, right). The pin assignment of the RJ45 is as follows:

RJ-45	Pin	Assignment
LED:	1	TD+
green	2	TD-
green	3	RD+
100	4	-
LNK	5	-
	6	RD-
	7	-
	8	-

- The green LED (left, 'LNK') indicates, when the link is established and packets are transferred.
- The green LED (right, '100') indicates a 100BaseT link. If the LED does not light, the link is established with 10BaseT, only.

The device is able to recognize

- a polarity inversion of the receiving signals (RD+ <--> RD-)
- a crossover of transmitting/receiving signals (RD+/RD- <--> TD+/TD-)

and corrects it automatically to ensure that the operation continues smoothly. This allows the usage of 1:1 cables in any case.

CAUTION: For access it is recommended to use twisted-pair cables of the category 5 and an impedance value of 100 Ω. The maximum cable length is 100 metres. Using cables of lower quality or different impedances may result in a restriction of the maximum cable length. In addition the employment of unshielded cables can have a negative effect on the reliability of the data transmission.

100BaseFX (SFP)

The EDX1006 offers 6 optical 100BaseFX interfaces according the SFP industry standard. For each interface separate indicators give information on the Link state (LNK).

- The green LED ('LNK x') indicate(s) that the optical link is established.

No auto negotiation is supported, but only 100Mbit/s transmission.

1000BaseX (SFP)

The EDX100x series provides up two Gigabit Ethernet interfaces according SFP industry standard. For each interface separate indicators give information on the Link state (LNK). The operating mode is fixed to a 1000Mbps full-duplex connection if a fibre SFP is plugged.

For copper SFPs, auto-neg 10/100/1000 is supported. Please ask arcutronix, which vendors are supported for copper SFP.

EDX100x detects automatically, which type of SFP (copper of fibre) is plugged. This makes installation very easy.

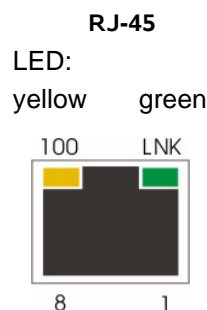
You will find more configuration information in the section "Ethernet Ports" on page 5-37.

- The green LED ('LNK x') indicate(s) that the optical link is established.

1000BaseTX (RJ45)

The EDX1000 provides one copper Gigabit Ethernet interface. Separate indicators give information on the Link state (LNK) and 10/100/1000BaseTX (100). The device negotiates the operating mode of the corresponding interface automatically with the remote station using Auto Negotiation (if activated). Half-duplex and full-duplex connections are supported. You will find more configuration information in the section "Ethernet Ports" on page 5-37. The data rate is either 10 Mbit/s, 100 Mbit/s or 1000 Mbit/s. The protocol is according to [IEEE 802.3]. Auto negotiation and auto crossover are supported.

The connector is a RJ-45 plug with 2 LEDs, which indicate established Link (green LED on the left side) and the data rate (green LED, right). The pin assignment is as follows:



Pin	Assignment
1	BI_DA+
2	BI_DA-
3	BI_DB+
4	BI_DC+
5	BI_DC-
6	BI_DB-
7	BI_DD+
8	BI_DD-

- The yellow LED (left, 'LNK') indicates the speed of the link:
 - 1x blink = 10Mbps
 - 2x blink = 100Mbps
 - 3x blink = 1000Mbps
- The green LED (right, LNK0') indicates, when the link is established and packets are transferred.

The device is able to recognize

- a polarity inversion of the receiving signals (RD+ <--> RD-)
- a crossover of transmitting/receiving signals (RD+/RD- <--> TD+/TD-)

and corrects it automatically to ensure that the operation continues smoothly. This allows the usage of 1:1 cables in any case.

CAUTION: For access it is recommended to use twisted-pair cables of the category 5 and an impedance value of 100 Ω . The maximum cable length is 10 metres. Using cables of lower quality or different impedances may result in a restriction of the maximum cable length. In addition the employment of unshielded cables can have negative effect on the reliability of the data transmission.

Common Indicators

'ON' LED

The green 'ON' LED indicates that the power supply of the EDX100x is available and the DC/DC converter is operating well.

'ERR' LED

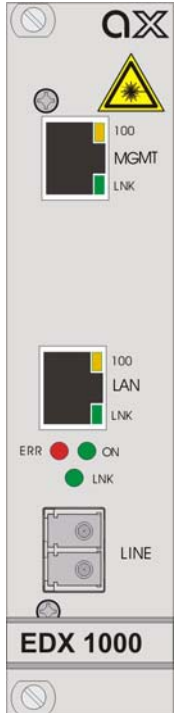
The red 'ALARM' LED indicates that there is problem on the unit.

Front Views

EDX1000

The following table shows the front panel of the EDX1000.

Table 3-3 EDX1000 Front View

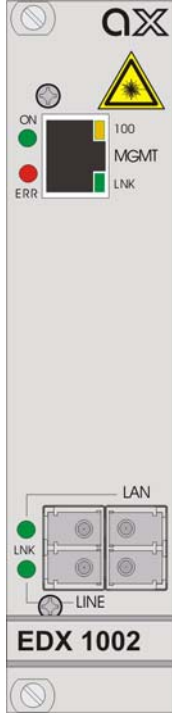
View	Product Number & Details
	0716-2001
	Mounting screw in SRX or SHX.
	1x MGMT-port (10/100BaseT)
	1x 10/100/1000BaseT port.
	3 LEDs for status and error indication.
	1 x SFP slot for 1000BaseFX or 10/100/1000BaseT pluggable devices.
	Handle with Label.
	Mounting screw in SRX or SHX.

- 1 x 10/100BaseT (RJ45), mainly for management purposes,
- 1 x 10/100/1000BaseT (RJ45),
- 1 x 1000Base (SFP) with a LNK LED.

EDX1002

The following table shows the front panel of the EDX1002.

Table 3-4 EDX1002 Front View

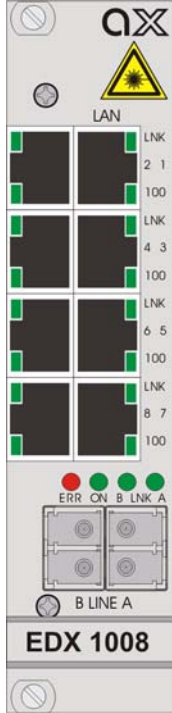
View	Product Number & Details
	0716-2101
	Mounting screw in SRX or SHX.
	1x MGMT-port (10/100BaseT)
	2 LEDs for status and error indication.
	2 x SFP slots for 1000BaseX or 10/100/1000BaseT pluggable devices.
	Handle with Label.
	Mounting screw in SRX or SHX.

- 1 x 10/100BaseT (RJ45), mainly for management purposes,
- 2 x 1000Base (SFP) with a LNK LED, each.

EDX1008

The following table shows the front panel of the EDX1008.

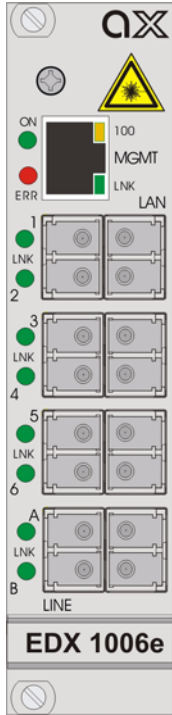
Table 3-5 EDX1008 Front View

View	Product Number & Details
	<p>0716-2102</p> <p>Mounting screw in SRX or SHX.</p> <p>8 x 10/100BaseT LAN ports.</p> <p>4 LEDs for status and error indication.</p> <p>2 x SFP slots for 1000BaseFX or 10/100/1000BaseT pluggable devices.</p> <p>Handle with Label.</p> <p>Mounting screw in SRX or SHX.</p>

- 8 x 10/100BaseT (RJ45) with integrated LEDs (LNK, 100),
- 2 x 1000Base (SFP) with a LNK LED, each.

EDX1006eThe following table shows the front panel of the EDX1006.

Table 3-6 EDX1006e Front View

View	Product Number & Details
	0716-2201
	Mounting screw in SRX or SHX.
	1x 10/100BaseT MGMT port.
	2 LEDs for status and error indication.
	6x SFP slots for 100BaseFX pluggable devices.
	2 x SFP slots for 1000BaseX or 10/100/1000BaseT pluggable devices.
	Handle with Label.
	Mounting screw in SRX or SHX.

- 1 x 10/100BaseT (RJ45), mainly for management purposes,
- 6 x 100BaseFX (SFP) with a LNK LED, each,
- 2 x 1000Base (SFP) with a LNK LED, each.

EDX100x Rear Connector

The EDX100x series has a connector on the rear-side offering the possibility to use the devices either in 19" racks or single-slot housing.

On the connector, the ports for local management (RS-232), power supply and rack-management are placed.

RS-232 Interface

The asynchronous RS-232 interface is used for the serial administration of the device. It is only available if the EDX100x is placed in a single-slot, dual-slot or triple-slot housing.

The standard transmission parameters for the serial interface is shown in Table 3-7. Function Indicators

Table 3-7 Transmission Rate of the RS-232 Interface

Transmission Rate (Baud)	Data Bits	Parity	Stop Bits
57600	8	none	1

Power Supply

For the EDX100x the operating voltage is fed through the backplane connector of the device. 5VDC must be applied to the unit for proper operation.

Chapter 4

Functionality

Media Conversion

The EDX100x-series offers an easy way to do media conversion on Gigabit-Ethernet network between optical and copper infrastructure. Converting copper to fibre seems simple. Using a media converter, you plug a copper cable into one port and a fibre line into the other port, and you have conversion. Media conversion is a cost-effective and simple-to-use tool.

The EDX100x is a carrier-class converter, which gives option to monitor and supervise the point of conversion. This is the qualification for the carrier to supervise its network up to this point and/or to have access to all points in its network.

Two different types of media Converter can be chosen out of the EDX100x-series:

- EDX1000: A copper to Fibre Gigabit Ethernet convertor to be used as providers demarcation point on customer's location (CPE).
- EDX1002: A Fibre to Fibre converter and repeater, which offers multi-option due the usage of SFPs. Either media conversion (multimode <--> singlemode), repeating and refreshing or wavelength transformation (1310 <--> 1550nm) can be done with this universal device.

Switching

The EDX100x is mainly acting as a "managed" switching device in store-and-forward mode. Store-and-forward is a telecommunications technique in which information is sent to intermediate devices where it is kept and sent at a later time to the final destination or to another intermediate station. The intermediate node in the networking context, verifies the integrity of the packet before forwarding it.

A switching device networking node that connects network segments or network devices. The term "switch" refers to a multi-port network bridge that processes and routes data at the data link layer (layer 2) of the OSI model.

Switches have the following properties:

- Switches are used to extend a network beyond the physical boundaries imposed by the number of stations and maximum length in accordance with a defined standard (e.g. Ethernet).
- Switches offer a simple way to limit errors. They drop faulty packets and, therefore, do not reduce the throughput of the entire network.

- Switches dynamically learn MAC addresses and transmit packets only to these ports where the receivers can be found. This increases the throughput of the whole network.

Switching is the default operating mode of the EDX100x. The EDX100x interconnects Networks by transparent protocol communication in accordance with [IEEE 802.1D].

The main functions of a switch are:

- Filtering and forwarding packets
- Gathering information required for filter and forwarding decisions
- Management functions for these tasks

The switch forwards data destined for a different port by protocol transparent communication. Data packets addressed to a learned MAC address are forwarded exclusively to the according port.

Additional functions for controlling data traffic, adjusting data throughput, setting up security mechanisms, and limiting the load on ports are provided through the mechanism of additional filtering (refer to Chapter 5, EDX100x Control Software & gCLI).

LAN, LINE, and MGMT-Ports

The ports on the EDX100x may have three different types of operation:

- LAN-port,
- LINE-port, and
- MGMT-port.

The classification, which port is of which operation-type is mainly fixed, but can be selected by management in some cases. The three types of operation define each a special behaviour of the port, in matter of packet forwarding and the capability of access to the control plane of the unit.

A LAN-port is normally connected to the user's equipment and terminates the service, offered by the operator. In the terminology of the [MEF 6.1], a LAN-port is an UNI. A LINE-port is heading towards the provider's (core) network and is operating like an NNI. A LINE-port carries traffic from (all) LAN-ports plus the optional traffic for the in-band management. Traffic on the LINE-port can be double-VLAN tagged to separate user's traffic from each other.

A MGMT-port is a pure (local) management port and allows only(!) access to the local management point. The traffic from a MGMT-port might be forwarded towards a LINE-port, but this is done by the management plane, neither by direct access.

The next figure shows the (logical) links on board between the three types of operation. In case a port operation-type is changed, this can be done without restarting the device.

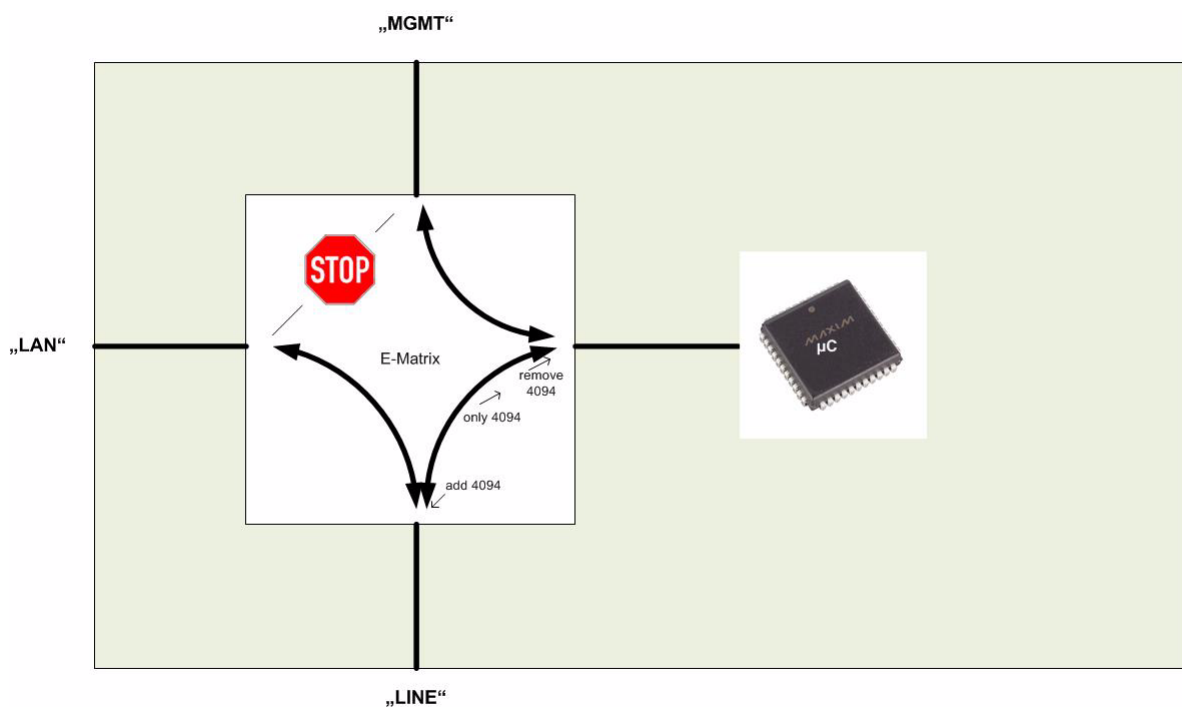


Figure 4-1 Connection LAN - LINE - MGMT

Traffic ingressing at LAN ports can never be seen on MGMT-port nor the customer has access to the control plane of the device. Traffic ingressing at LINE-ports may be forwarded to LAN ports and the management plane. The forwarding is based on MAC-addressing and/or VLAN tagging. As shown in the figure, there is always a VLAN-tag required for in-band management traffic (here 4094). Any traffic, ingressing at a MGMT-port can only be forwarded to the control plane for further handling. Last, the control plane can never communicate to a LAN port, as there is no link. All traffic from control plane to MGMT is un-tagged, while all traffic for in-band management will be tagged before egressing at a LINE-port.

If either in-band management or the MGMT-port are disabled, the following matrixes are applied.

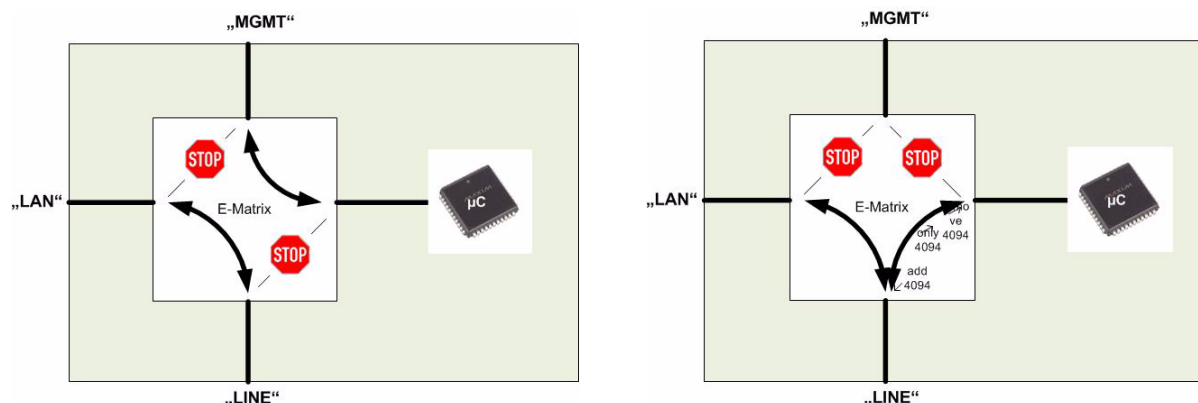


Figure 4-2 Forwarding Matrix w/ disabled management options

On the left side, the links are shown when in-band management is disabled. In this case, nor traffic can be send between control plane and LINE-ports. On the right side, the MGMT-port is disabled, while the in-band is enabled. If both option are disabled, the access to the control plane for all TCP-IP-based protocols is impossible. In this case, the remaining access-options are either serial interface (in SHX and SRX3) or via agent-card (SCX2e), if available.

VLANS

Introduction to VLAN

A Local Area Network (LAN) can generally be defined as a broadcast domain. Hubs, bridges or switches in the same physical segment or segments connect all end node devices. End nodes can communicate with each other without the need for a router. Communications with devices on other LAN segments requires the use of a router.

As networks expand, more routers are needed to separate users into broadcast and collision domains and provide connectivity to other LANs. One drawback to this design is that routers add latency, which essentially delays the transmission of data. This is caused by the process involved in routing data from one LAN to another. A router must use more of the data packet to determine destinations and route the data to the appropriate end node.

Virtual LANs (VLANs) can be viewed as a group of devices on different physical LAN segments which can communicate with each other as if they were all on the same physical LAN segment. Although the network above has some distinct speed and latency advantages over a traditional LAN, it also has some serious drawbacks. The most notable of these for the purposes of this discussion is that all hosts (end nodes) are now in the same broadcast domain. This adds a significant amount of traffic to the network that is seen by all hosts on the network. As this network grows, the broadcast traffic has the potential impact of flooding the network and making it essentially unusable.

Switches using VLANs create the same division of the network into separate broadcast domains but do not have the latency problems of a router. Switches are also a more cost-effective solution.

VLANs allow to create a network that is independent of physical location and group users into logical workgroup. Using VLANs it is possible to confine broadcast traffic for each workgroup to just those devices that need to see it, and reduce traffic to the rest of the network. There is an increased connection speed due to the elimination of latency from router connections. An additional benefit of increased security could be realized if we made the decision to not allow access to the host from foreign networks, i.e., those that originate from another subnet beyond the router.

For instance, if a department has users in three different locations, they can now provide access to servers and printers as if they were all in the same building.

VLAN architecture benefits include:

- Increased performance
- Improved manageability
- Network tuning and simplification of software configurations
- Physical topology independence
- Increased security options

NOTE: The configuration of many VLANs (more than 250) may slow down the start-up of the device after reboot. The device must first configure all ports and all VLANs properly before it allows any packet forwarding. Each 250 VLANs which must be configured, one have to calculate about 2 additional seconds booting-time.

Supported VLAN-Modes of EDX100x

EDX1000 supports three different operation modes for VLAN handling:

- VLAN Unaware (VLAN Mode = Off):

VLAN tags are not investigated and no VLAN-dependant handling is done. This is true for LAN- and LINE-ports, as well as for Ingress and Egress data-transfer.

- VLAN Aware

The EDX100x forwards packets according their VLAN-ID. Each LAN-port can be associated with one or more VLANs which are accepted and forwarded. All other packets are discarded.

- Provider VLAN-Tagging

The EDX100x operates as a Provider Bridge according [IEEE 802.1ad]. All packets coming as ingress data from a LAN-port, will get an additional VLAN-tag. All packets leaving a LAN-port (egress) will lose the most outer VLAN-tag, as this tag is only required inside the provider's network. In this mode, one can decide how to treat the so-called Layer2 Control Protocol (L2CP) frames. They can be either forwarded as normal user-frames, discarded or treated by EDX100x.

VLAN Aware

In “VLAN Aware”-mode the EDX100x acts as a VLAN-switch and forwards all packets according their VLAN-ID. Packets coming from an LAN-port (Ingress) are inspected and the VLAN-ID is used to forward or block the packet.

If an ingress-packet does not carry a VLAN-tag, one can decide what to do with such packets:

- Discard untagged packets,
- Add a VLAN-tag with a port’s defined default VLAN-ID value.

All tagged packets can either be accepted or discard depending on the “Associated VLAN-ID”-list:

- Pass all packets and forward them to the LINE-port(s),
- Pass only packets with VID according the associated VID-list,
- Pass all packets except those packets with VID according the associated VID-list,
- Force all packets to get the Default VID
- Block all packets, regardless of the VID.

Tagged packets coming from a LINE-port can only be forwarded to those LAN-ports, which have the VID in their associated list. If the LAN-port is configured to block all associated VIDs, then all other VIDs are forwarded from LINE to this LAN-port.

Example

LAN-port 1 has the following configuration:

- Associated VID-list = {1, 5-7}, Default VID = 10.

LAN-port 2 has the following configuration:

- Associated VID-list = {7}, Default VID = 14.

The following table shows the behaviour of packet forwarding for different packets and modes, only for LAN-port1:

Table 4-1 Behaviour for Untagged Packets on LAN-port 1

Untagged Packets	
Mode	Behaviour
Discard All Packets	All untagged will be discarded.
Force Default VLAN ID	All untagged packets will be tagged with VLAN ID 10 and forwarded according the rules for VID 10.

Table 4-2 Behaviour for Tagged Packets on LAN-port 1

Tagged Packets	
Mode	Behaviour
Pass all Packets	All packets will be accepted and forwarded according the rules for the VLAN-ID. E.g. packets with VID 7 will be forwarded to LINE-ports and LAN-port 2, as VID 7 is in the associated list of LAN-port 2.
Allow Associated VLANs only	Only packets with VID 1, 5, 6 or 7 are accepted and forwarded according the rules for the VLAN-ID. E.g. packets with VID 7 will be forwarded to LINE-ports and LAN-port 2, as VID 7 is in the associated list of LAN-port 2.
Block Associated VLANs	Packet with VID 1, 5, 6, 7 are blocked. All other packets re accepted and forwarded according the rules for the VLAN-ID. E.g. packets with VID 7 are blocked and will not be forwarded to LINE-ports and LAN-port 2, even when VID 7 is in the associated list of LAN-port 2.
Force Default VLAN ID	All incoming tagged packed will get the VID 10 instead the incoming VID. The associated list of VIDs is non-essential.
Discard All Packets	All tagged packets will be discarded. The associated list of VIDs is non-essential.

Table 4-3 Behaviour for Untagged Packets on LINE-port

Untagged Packets	
Mode (on LAN 1)	Behaviour
Non-Essential!	Incoming untagged packets on a LINE-port will not be forwarded in "VLAN Aware"-mode!

Table 4-4 Behaviour for Tagged Packets on LINE-port

Tagged Packets	
Mode (on LAN 1)	Behaviour
Pass all Packets	\
Allow Associated VLANs only	
Force Default VLAN ID	All incoming packets with VID 1, 5, 6, 7 and 10 may be forwarded to LAN-port 1 (and other LAN-ports). The decision is based on the MAC address table of the EDX100x.
Discard All Packets	
	/
Block Associated VLANs	All incoming packets with VID other than 1, 5, 6, 7 and 10 may be forwarded to LAN-port (and other LAN-ports)1. The decision is based on the MAC address table of the EDX100x.

Provider VLAN-Tagging

An additional feature supported by EDX1000 is VLAN stacking defined in [IEEE 802.1ad], also called “Q-in-Q”. This technology allows additional VLAN tags to be inserted into an existing [IEEE 802.1Q] tagged Ethernet frame. This makes it possible to tunnel LANs and/or VLANs through the provider’s network. The general purpose of Provider VLAN-Tagging is to allow frames from multiple customers to be forwarded (or tunnelled) through another topology (provider network) using provider VLANs or P-VLANs. The provider bridge, which may comprise multiple devices in the service provider domain, looks like a simple bridge port to the customers traffic and maintains the customer’s VLANs.



WARNING: When Provider-Tagging is enabled, the in-band access (In-band MGMT) is also expected to be double-tagged! As soon as the VLAN-mode is configured to Provider-Tagging, you will loose your in-band management connection, if the in-band is not already configured to Double-VLAN-Tagging!

Figure 4-3 shows a sample P-VLAN topology and use model. Customer A has LANs spread across multiple site locations and may want to link them together in a single logical LAN. To do this, the customer could have a cable laid out for the entire distance interconnecting the three sites. A more cost-effective and scalable alternative, however, would be to tunnel frames through the provider’s network to interconnect all the sites subscribing to the service. This solution can be delivered using P-VLAN tagging.

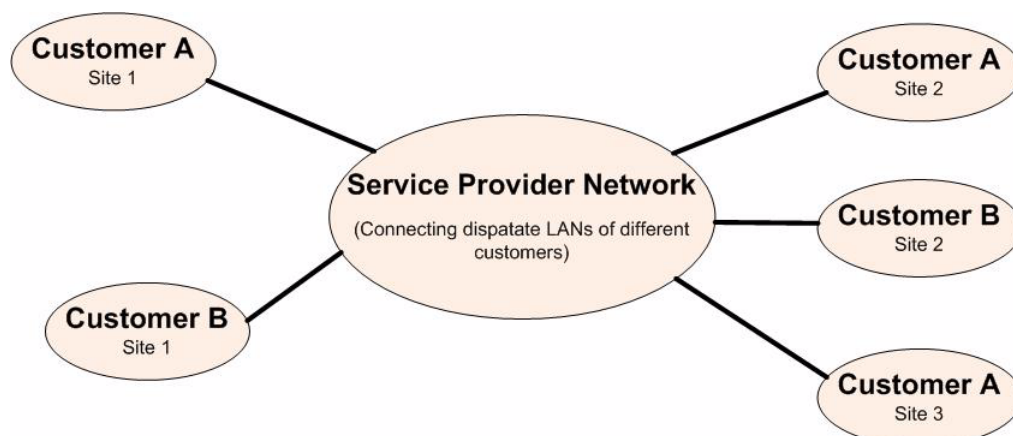


Figure 4-3 Provider VLAN Tagging Diagram

How it works

Under P-VLAN tagging, the provider network operates on a different VLAN space, independent of the VLANs that are used in the customer network as shown in Figure 4-4.

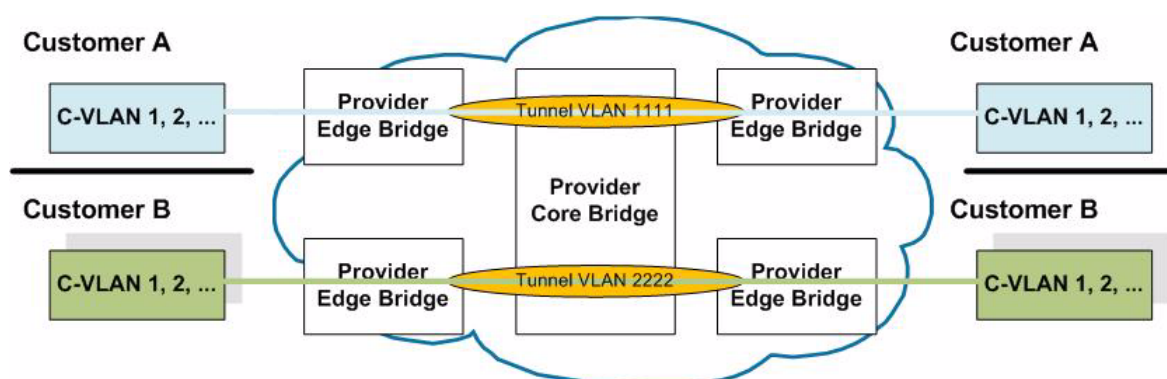


Figure 4-4 P-VLAN configuration

Customer VLANs (referred to as C-VLANs by the [IEEE 802.1ad] specification) are not used to make any forwarding decisions inside the provider network where customer frames get assigned to service VLANs (P-VLANs). Inside the provider cloud, frames are forwarded based on the P-VLAN tag only, while the C-VLAN tag remains shielded during data transmission. The P-VLAN tag is removed when the frame exits the provider network, restoring the original customer frame.

User & Access Administration

The EDX - Ethernet Demarcation device can be configured and maintained in several ways. In principle, one can distinguish two possibilities:

- Direct access to the EDX100x,
- Indirect access to the EDX100x via an agent-card.

The direct access is either serial or TCP/IP communication and uses a direct link to the management application on the unit.

The indirect access is via a relay station, which redirects the information of the device. This relay station is the ax agent-card SCX2e. The agent-card offers more protocol-options than the direct access.

Both ways of access offer the possibility to carry the required information across the LINE-link. Carrying the information for direct access, the transport is called

- in-band management,
- while the transport for indirect access is called
- ax-remote management.

Both communication channels can be used in parallel, so it does not make many sense.

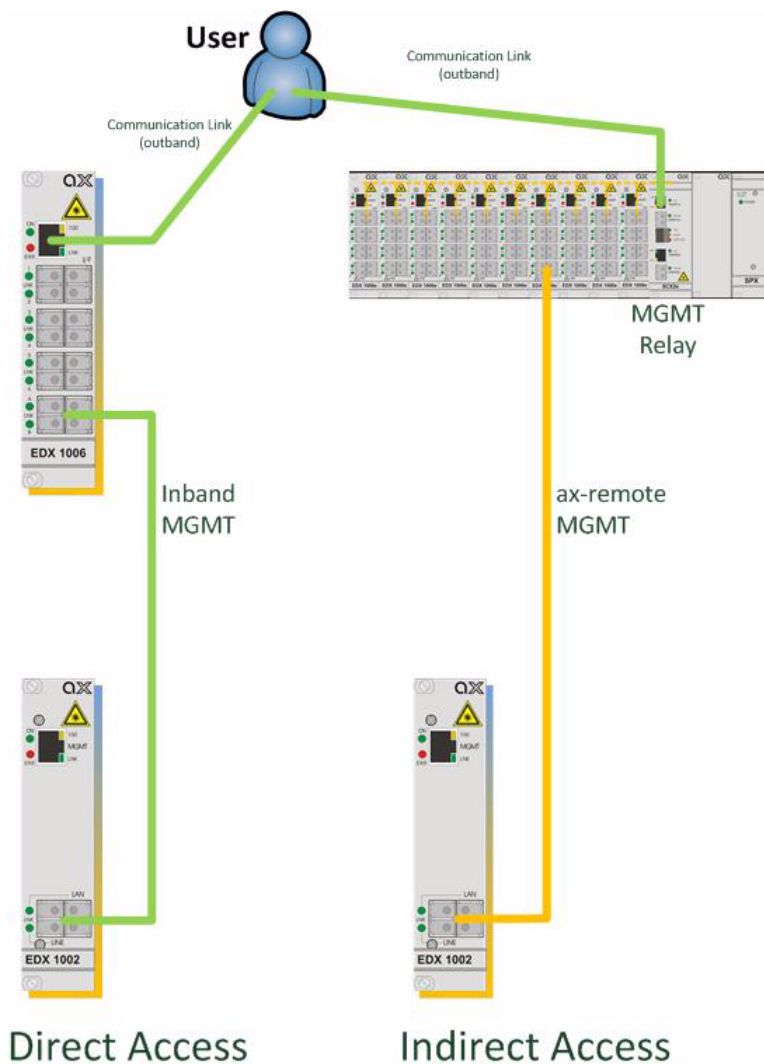


Figure 4-5 Direct and Indirect Access

Direct Access to the EDX100x

The EDX100x offers several physical ways to get access to the device together with different protocol stacks.

Three different protocol stacks to get direct management access to the EDX100x can be differentiated:

- CONSOLE-port (command-line-interface via RS-232)
 - See Chapter 5, EDX100x Control Software & gCLI.
- SNMP (including traps)
 - SNMPv2c and SNMPv3 are supported.
 - See Chapter 6, SNMP and MIBs.
- TELNET

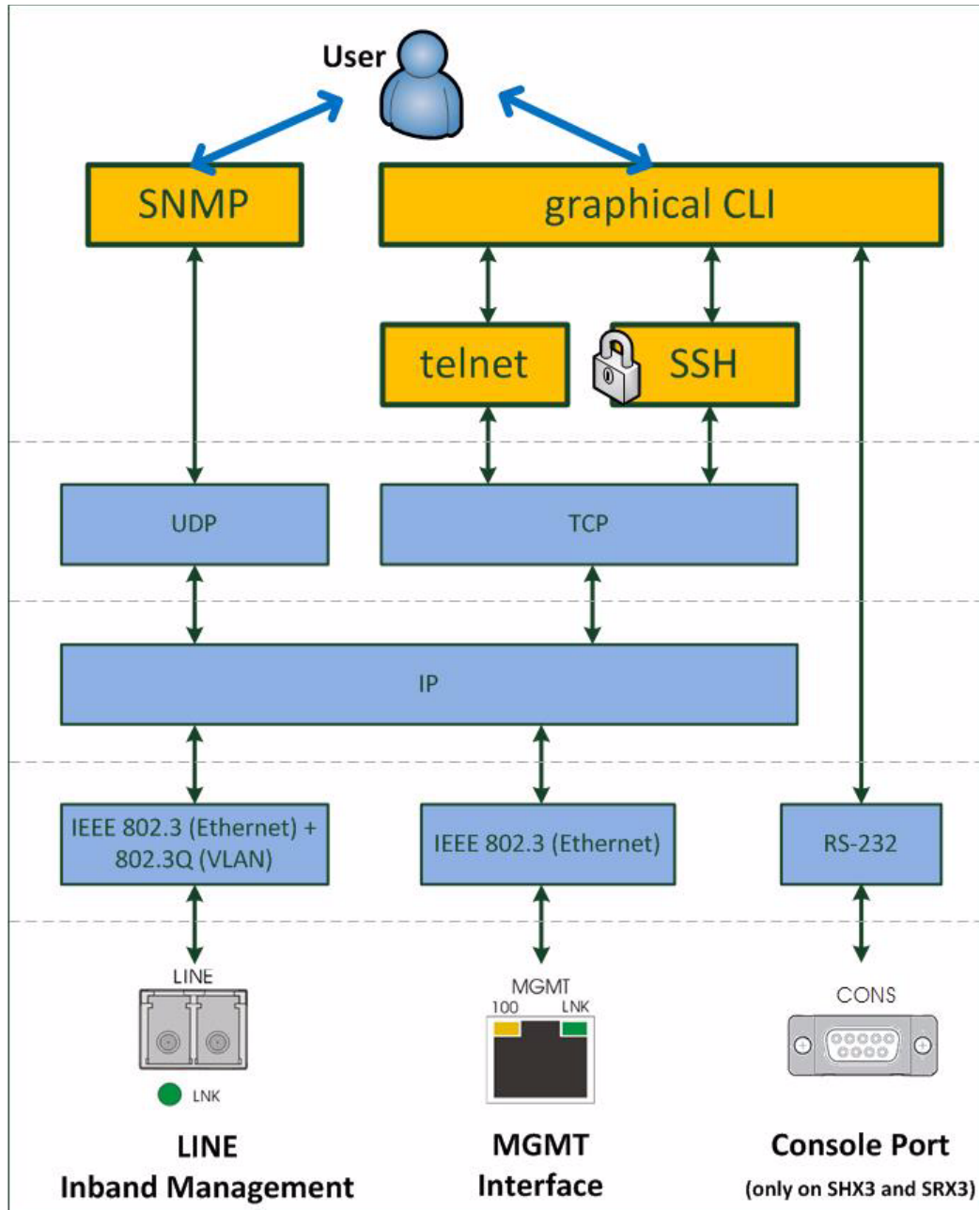


Figure 4-6 Management Protocol Stack

Figure 4-6 shows the protocol stack for the management access to the EDX100x and the adjusting physical interfaces to be used.

Local RS-232 Interface

All variants of the EDX100x are equipped with a backside RS-232 interface, which is accessible in all housing and chassis without separate agent-capability. This is the single-slot housing SHX3, and the triple-slot housing SRX3. The RS-232 interface provides local management access and offers the access to the graphical Command Line

Interface (gCLI) of the EDX100x. The gCLI is accessible via a VT100 terminal (emulation) program.

Local Ethernet Interface (Copper)

The copper ethernet port labelled “MGMT” (RJ-45) is the local management interface. It is dedicated for installation purposes mainly, but can also used for remote out-of-band management access.

All supported protocols, which are based on the TCP/IP stack, can be accessed via the local MGMT port.

The default IP-settings to get connection to the device is listed in chapter “IP Configuration” on page 4-18.

In-band Access

Via the LINE interfaces the user can also get access to the management applications of the EDX100x. To separate the in-band management from user’s traffic, the in-band management is always tagged with a VLAN. The VLAN-ID can be freely configured, the default VLAN-ID for in-band management is 4094.

NOTE: The configured VLAN-ID for the in-band management will be blocked at the LAN-ports in all cases!

All supported protocols, which are based on the TCP/IP stack, can be accessed via the in-band ports.

The default IP-settings to get connection to the device is listed in chapter “IP Configuration” on page 4-18.

SSH connection

The SSH-access offers a secure connection to the device. Keys and passwords might be used to make the communication safe and secure. There are many SSH client-SW on market, which are mainly freeware. We at arcutronix use normally the putty-ssh client and or the TeraTerm. All the following examples are related to puTTY-ssh and or TeraTerm-ssh.

Before the SSH-client on the EDX100x can be used, a public and private SSH-key must be generated. The public key has to be completely(!) stored on the device, while the private key is stored on your PC. The generation of public and private SSH-key can be done with the help of various programs (e.g. puttygen). How to store a public key onto the device is depicted in “Add Key” on page 5-17.

When an SSH link is established to the device, a Secure Shell will be opened and a login-prompt is visible:



Figure 4-7 Secure Shell to EDX100x

NOTE: The user to be logged to the secure shell is “cli”! It is not any other user like admin, guest or other locally-stored users. After login to the secure shell as “cli”, the standard login-menu of the graphical Command Line Interface (gCLI) will be presented. In the standard login-menu (see “Login Menu” on page 5-3) the standard entry of user and password is done. For the secure shell, always use “cli”.

Indirect Access to the EDX100x

The indirect access to the EDX100x is always done via the agent-card SCX2e. The agent-card cards as a relay and offers various north-bound protocols for management.

- See Chapter 7, axCLI via SCX2e.

The indirect access to all cards in the same rack as the agent itself is done via the back-plane and will be depicted here after in detail.

the indirect access can also be achieved to all “remote” EDX100x-cards, which are directly connected to cards in the chassis. A proprietary protocol is used to transport the management and configuration data from the agent-card via the local EDX100x-cards to the remote EDX100x-cards. The protocol is using a special VLAN-channel within the LINE-link, called **ax-remote MGMT**.

The ax-remote MGMT is using VID 4093 as default. ax-remote MGMT must be enabled on both ends (local and remote side) for operation.

User Administration

All the different access-options to the EDX100x are protected by user-name and password. Several users can be configured on the EDX100x and stored locally, or one can use a (central) server, which stores the different users passwords and levels. Each user can have one of three different levels of authority:

- admin,
- user,
- guest.

A new user can be created on the EDX100x locally with access-level, user-name and password.

Locally Stored Users

Locally stored users can be created, modified and deleted by the administrator. The number of locally stored users is limited to 99. If a locally stored user shall be inactive, it must be deleted.

NOTE: After the creation of a new user together with password, only the user itself can change its password. If the password was lost, the user must be deleted and re-created again.

When delivered, the EDX100x does have one locally stored user:

user-name: 'admin'

password: 'private'



WARNING: It is highly recommended to change the password of 'admin' due to security reason!

NOTE: The user 'admin' can never be deleted. Only the password of 'admin' can be changed.

Rules for Usernames

When a new user has to added to the onboard user-list, some simple rules must be considered:

- The (new) user name must consist of at least 3 characters.
- The following characters are allowed: '0-9', 'a-z', 'A-Z', '_', '.', '-'.

Rules for Passwords

The password given to a user or other usage must reach a certain level of "password strength" to protect the system from hackers. The strength of a password is a function of length, complexity, and unpredictability and this is verified by several security rules. If

a new password does not fulfil this rules, it will be not accepted by the EDX1000. The rules are as follows:

- Minimum password length is 3 characters (, maximum password length is 32 characters),
- Character set is 7-Bit ASCII, allowed characters:
 - Capital letters: A...Z,
 - Lower case characters: a...z,
 - Digits: 0...9,
 - additional characters: 0x2D (-), 0x2E (.), 0x5F (_)
- The password may contain any of these characters.

NOTE: It is allowed to have the user-name as part of the password (forwards and backwards, not case sensitive!). BUT the system will remove this string from the password before it is verified.

- E.g. the user-name is “weakuser”. Then a password “12weakUser!” would lead to strength-verification of “12!”. The password would be too weak and not accepted!
- The same user-name in combination with password “12weakuser!_ButStrongPassword” would be ok, as the strength-verification is done on the reduced password “12!_ButStrongPassword” and this fulfils the requirements for a strong password.

Security Issues

The EDX100x is accessible via several different protocols. All these optional ways of access are protected by user-name and password to deny forbidden access against intruders.

Any time you connect or reconnect to the EDX100x the login-window is displayed and a password request turns up.

Be careful with your passwords! If you write them down, keep them in a safe place. Do not choose strings easy to hack. In particular, do not use the default strings which were valid when you received the device.

Do not forget your password. If you forget your password the device will be rendered useless and will have to be sent back to the factory for basic re-configuration.

NOTE: Three different access-level are selectable with different access rights:

1. Guest (only view)
2. User (view and modify)
3. Admin (full access inclusive user administration)

If the device is started-up the very first time, only the user “admin” is defined. See in “User & Access Administration” on page 5-12, how to define the other users and how to change the user password.

Auto-Logout

At the end of a management session it is highly recommended to stop the connection and logout from the unit. This is a safety requirement to make sure nobody else can use the current login without authorization. Nevertheless it can happen that this security demand is not observed, due to:

- Problems of your Computer,
- Problems in the network,
- Laxness of user,
- etc.

To make sure, a forgotten or incomplete logout, or a still open connection is closed there are some features to enforce auto-logout.

Time-Based Auto-Logout

First, there is an auto-logout time, which will terminate each CLI, SSH and Web-GUI session after “No activity”. This auto-logout time can be specified. It defines the time of inactivity, which causes an automatic logout. The specified time-interval is valid for all active logins, and each login does have its “own” timer. A “login” is the combination of user and access (e.g. user “admin” via “ssh” or user “test” via “http”).

Note: If auto-logout-time is defined to zero, the auto-logout is disabled for all logins.

The detection of activity is different for the access options.

CLI:

- For the CLI activity is the <enter> command which sends a new instruction to the device.

Web-Page:

- For the Web-GUI, activity is changing a variable-value, moving to a new page or reload of the existing page.
- A second time-based logout is a java-script for web-GUI. If for 15 seconds the browser does not reply a “hello”-message from the device, it is assumed the browser or browser-tab was terminated and a log-out will happen.

Hardware-Based Auto-Logout

A CLI session via the CONS-port will be terminated, when the RS-232 cable is removed. Important is, that the DTR-signal was properly connected between PC and device. After successful setup of the RS-232 connection, the device checks whether the DTR-signal is established. If not, the auto-logout can not work. If the DTR-signal is present in the device it will terminate the session, as soon as the DTR-signal disappears.

Management Port Configuration

The EDX100x can be managed via different protocols using the TCP/IP stack across the management interface(s) “MGMT” and in-band management port. The in-band management port is only available via the LINE port(s) and can be enabled and disabled. If in-band management is enabled it is always using a special VLAN-ID to separate the management traffic from “normal” user-payload. All management ports use the same IP configuration (host address).

IP Configuration

All management ports (all ports of type “MGMT” plus the in-band management port(s) within the LINE port(s) use the same host-address. Defaults are stored on the device, but these will seldom fit into the given environment. The device supports manual address assignment as well as the dynamic host configuration protocol DHCP.

Management Port(s) “MGMT”

The out-of-band management port(s) use the special port-type “MGMT”. Normally there is a maximum of one “MGMT” port per unit, but there might be customized variants with more. A “MGMT” port has different behaviour than “LAN” and “LINE” ports. A “MGMT” port is directly connected to the local control point of the unit and all packets will be processed there. Special protection is foreseen on a “MGMT” port to protect the system against DoS attacks.

In-band Management Port

The in-band management port carries the management traffic over the same links and in parallel as the payload traffic. To separate the management traffic from the (user’s) payload, it must be VLAN-tagged in all cases.

Default IP Configuration

Per default the EDX100x asks for an IP address via DHCP. The DHCP server has to be connected to “MGMT” port or one of the “LINE” ports of the EDX100x. As long as there was no DHCP available, yet, the unit uses the following default IP-address

- Default IP-Address: 192.168.1.100
- Default Netmask: 255.255.255.0
- Default GW: <empty>

- In-band Management: Enabled
- Default VLAN-ID for In-band Management: 4094

DHCP and Manual Address Assignment

The IP-address of the unit can be assigned by an DHCP-server or manually. If an DHCP-server is used, it must be connected to one of the management interfaces (“MGMT” or in-band). If no DHCP-server is available (or just not reachable), the unit starts with the Default IP-address (see above).

Note: We have sometimes seen problems with DHCP communication over some available USB-to-Ethernet adaptors. This problem is not related to EDX100x, but the implementation of these adaptors. Best results is reached with onboard Ethernet-ports.

After assignment of the management IP-address (via DHCP or manually) the EDX100x is reachable within the existing IP-network. It makes no difference whether the communication uses the out-of-band or in-band interface. Of course, the in-band port uses a VLAN tagged communication method, whilst the MGMT uses an untagged communication method.

DNS-Support

The Domain Name System (DNS) is a hierarchical naming system for computers, services, or any resource participating in the Internet. It associates various information with domain names assigned to such participants. Most importantly, it translates domain names meaningful to humans into the numerical (binary) identifiers associated with networking equipment for the purpose of locating and addressing these devices world-wide. An often used analogy to explain the Domain Name System is that it serves as the “phone book” for the Internet by translating human-friendly computer host-names into IP addresses. For example, *www.example.com* translates to *208.77.188.166*.

EDX100x does support DNS infrastructure to support easy access to the devices after IP address assignment. The EDX100x will inform the DHCP about its name (= serial number) and with this information, the DHCP server will inform the DNS about the logical name and the assigned IP-address.

An example is shown below. The EDX100x with serial number **ax12345678** has been assigned the IP-address **192.10.4.10**. A ping-command will result in the following:

```
C:\> ping ax12345678

Ping ax12345678 [192.10.4.10] with 32 bytes data:

Reply from 192.10.4.10: Bytes=32 Time<1ms TTL=128
Reply from 192.10.4.10: Bytes=32 Time<1ms TTL=128
Reply from 192.10.4.10: Bytes=32 Time<1ms TTL=128
Reply from 192.10.4.10: Bytes=32 Time<1ms TTL=128

Ping-Statistics for 192.10.4.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% Loss),

C:\>
```

Miscellaneous Features

Firmware-Update

It might be necessary to update the software (firmware) on the EDX100x. In this case the new firmware can be uploaded to the device via TFTP.

The master update-file is always called “dimage.spec”. This files carries the list of all files, which have to be installed for proper update.

NOTE: A corrupted file can be uploaded to the EDX100x, but it will not be used for update. The security check can only be done, when the file is on the device.

After successful upload, the update process starts either at once or at a specified time. When update (not upload) is started, the unit will do a reset right after successful installation of the new firmware.

Fault Propagation with LPT/RFD

LPT (Link Fault Pass Through) and RFD (Remote Failure Detection) are troubleshooting features which allow the EDX1000-series to inform the network about detected failures on layer 1.

Link Fault Pass Through is usually used to solve the problem encountered when operating traditional media converters. The problem is when one side of the link fails, the other side still continues to transmit packets, and waits for a response that will never arrive.

Link status on one port is propagated to another port to notify remote nodes. If the TP port is unplugged or the fibre port fails, the remote converter stops transmitting on the TP port.

With link fault pass through, system administrators are able to notice a link failure within a short period of time, minimizing the loss caused by this problem.

Figure 4-8 below shows the behaviour in a simple network (2x EDX1000). Top picture shows the normal state. Two copper ports (called A and C) and a duplex fibre optic link (called B) are connecting two routers.

In case link A fails, the remote link C will be torn down to indicate the router on the right, that there is a problem in the network and the communication does not work any longer. This is called RFD = Remote Failure Detection. Please note, that the optical link is not affected. As soon as the TP port on the left side is up again, the TP on the right will be activated, too.

Last picture in Figure 4-8 shows the failure of the optical link. The LPT (Link fault Pass Through) will tear down the copper ports to indicate the problem towards the routers. As soon as the optical port is operational again, the TPs will be activated, too.

To achieve the communication between the two devices, the IP-address of the peer has to be advertised on both sides. Using IP-layer for this communication, makes the LPT/RFD-implementation independent from the network in between the two peers. If there is any switch or hub in use, the LPT as well as the RFD feature can be used for an end-to-end supervision.

NOTE: When LPT/RFD is configured, it will tear down the client interfaces (LAN) until the communication to the peer is established. As soon as the communication to peer is established, the client interfaces will be configured according to their counterparts on the peer.

In most cases, the two peers will be configured in exactly the same way to have same behaviour on both ends of the network. To achieve this, it is sufficient to configure on site and keep this configuration mirrored to the peer. This can be done, by setting on site to the configuration mode “explicit”, while the peer is configured to “implicit”. This makes it easy to keep configuration synchronized.

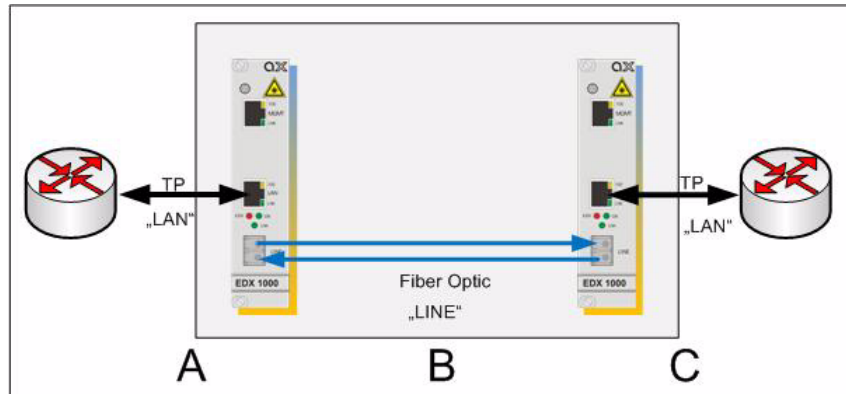
NOTE: At least one of the two peers must be in “explicit” mode, otherwise it will not work!

NOTE: For “implicit” mode, the two peers must be of the same type (e.g. EDX1000 - EDX1000 or EDX1006 - EDX1006). Unsymmetrical types can lead to problems when one side is configured as “implicit” (e.g. EDX1000 - EDX1006).

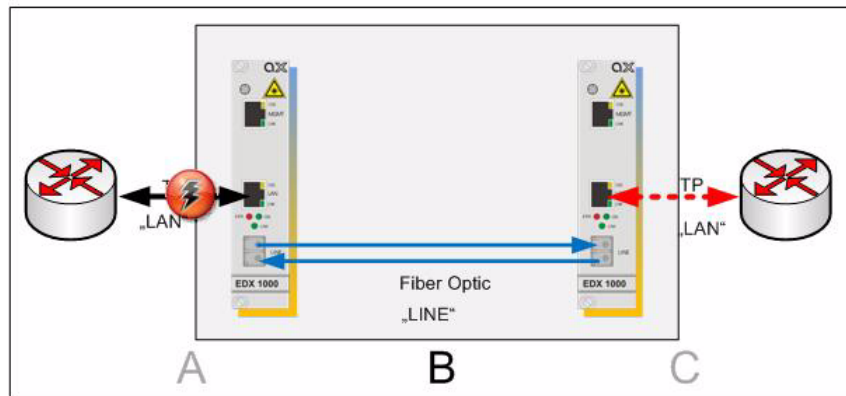
The example below shows a typical LPT/RFD scenario. The two EDX1000 are connected and LPT is configured on both sides. When all links are established, the payload can be send from “LAN” to “LAN” and vice versa.

The RFD (Remote Failure Detection) is active, when on one of the both “LAN” interfaces a link-down is detected. In the example below the defect is on the left side (interface called A). This defect will be notified from the left EDX1000 to the right EDX1000. As a subsequence, interface LAN, called C, is also disabled to “forward” the status from left to right. Any equipment, connected to C, will now detect a link-down and can act on this failure.

LPT (Link Fault Pass Through) is the situation on the bottom of the example. The link between the both EDX1000 has failed and no payload transfer is possible any longer. To announce this to equipment, connected to the LAN link A and C, both EDX1000 will disable their LAN interfaces. Any equipment, connected to the both LAN ports, will now detect a link-down and can act on this failure.



RFD:



LPT:

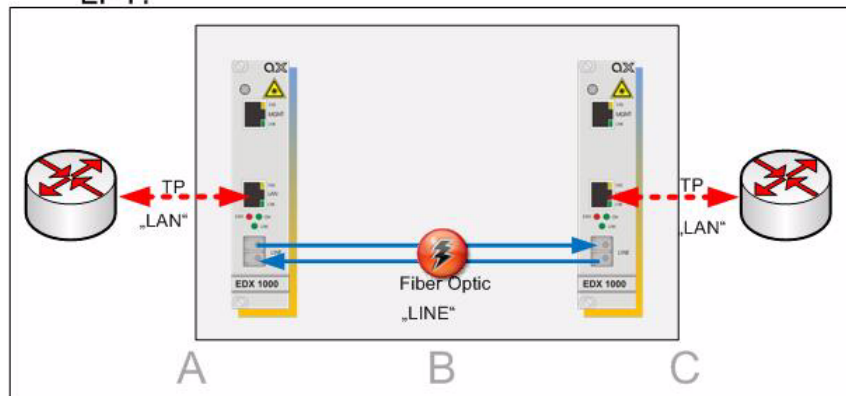


Figure 4-8 LPT/RFD Application

The example above shows a simple 1:1 network. If an EDX1008 or EDX1006 is used, there are more ports, which can be controlled by LPT/RFD. For these devices, an assignment can be done, to define which LAN ports are affected by the failure of remote LAN-ports and/or the failure of a Line-port.

The following example shows the assignment for an EDX1006 scenario: If the line fails on the left side (LPT), LAN2 and 4 shall fail, while a line-failure on the right side will consequently tear down LAN5, only.

For RFD, the examples defines a connection between LAN2 (left) and LAN1 and LAN5 on the right side. More is possible, of course, but the example shall be simple.

Table 4-5 LPT/RFD Configuration Example

EDX1006 (left)				right EDX1006 (right)			
LINE:	LPT	LAN2, 4	(local ports)	LAN5	(local ports)	<- LPT	:LINE
	->						
LAN2:	RFD	LAN1, 5	(remote site)	-	-	-	-
	->						

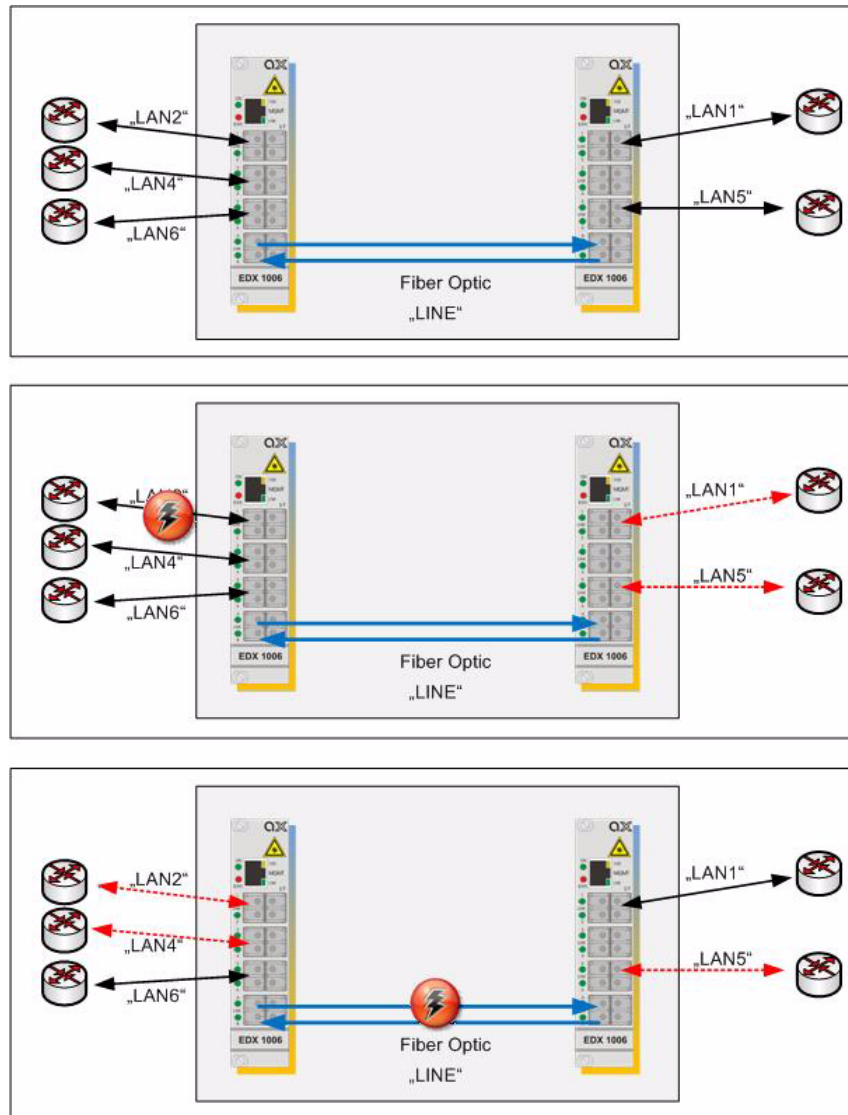


Figure 4-9 LPT/RFD Configuration Example

Operation Mode of RFD

The operation of RFD needs a communication between the both peers. With the communication, the status of local LAN-port(s) is handed over the peer, so it can be replicated on the remote side. The communication between the both peers can be done either via

- Slow Protocol (layer2; "link-local") or
- UDP/IP (layer3).

In the first case, the operation is mainly intended for a point-to-point (back-to-back) application with no other equipment in-between. Slow protocols are used for several application and are located in the MAC-layer (layer 2 of OSI reference model). Slow

protocols need not to be forwarded by switching devices, but are a link-layer protocol. E.g. PAUSE-frames are using slow protocol as Ethertype.

When the communication between the (both) peers shall be across several hops, even across the border of a switched network, the better choice is to use TCP/IP. In this case, the IP-address of the peer must be configured on the unit(s). Make sure, the peer's IP-address is reachable via the given network and the given IP-settings. Especially the missing configuration of an Default-Gateway can lead to communication problems in an IP setup.

Of course both (all) sides need to be configured in the same manner. One side in TCP/IP mode and the other using Slow protocol will not work.

The default configuration for LPT/RFD is the operation with TCP/IP.

Slow Protocol (Link-Local) vs. UDP/IP

When LPT is configured to use Slow Protocol (=MAC; Link-Local) instead of IP, not much happens. The difference is "just" in the way of addressing the packets. While for the IP-way, we need the peer's IP-address to put the right destination address in the packets, which are exchanged for status communication. This is normal IP. First MAC-header, then IP-header, then UDP-header and at last the information:

- MAC-DA | MAC-SA | Ethertype=0x0800 | IP-DA | IP-SA | Port | **information**

When it is configured to use Slow protocol (en.wikipedia.org/wiki/EtherType) the packets are slightly different organized:

- MAC-MC | MAC-SA | Ethertype=0x8809 | **information**

One can see, the packet starts with a special MAC-Multicast-address (01-80-C2-00-00-02) and a different Ethertype is used. BUT, the information is the same. Slow protocol is defined by IEEE802.3 and are only allowed to be forwarded in between the MAC-layer. It will NOT be forwarded across an Ethernet-switch, neither across a router. (But it will be forwarded across an Ethernet-hub!). The good is, that one do not need to know about the peer's address (neither MAC nor IP). The withdraw is, that it cannot be used across a switched or routed network. So if the EDXs are far away from each other (not directly connected) it will NOT work!

Status and Log-Messages of the LPT/RFD Stack

The LPT/RFD software-stack does know several states, which indicates internal and external situations. In the following an overview is given about these states.

Table 4-6 LPT/RFD Status

Status	Description
LPT/RFD disabled	LPT/RFD is disabled by admin. The stack is not initialized and no messages to peer(s) are transmitted.
RFD disabled	RFD is not running. The LPT is activated and operational.
RFD disabled (no peer configured)	RFD is not running, yet. Most common reason for this is, that no peer- IP-) address is configured. The LPT is activated and operational.
Connecting to peer...	RFD Op Mode = IP: The peer-address is first time entered or changed by admin. The stack tries to get (IP-) contact to its peer. The SW-stack is waiting for RFD-packets from the configured IP-peer. The device itself sends out packets to this peer. When the device can not get contact to peer within 30 seconds, it will change to new state "No contact to peer". RFD Op Mode = Link-Local: The SW-stack is waiting for RFD-packets from the (link-local) peer. The device itself sends out packets to this peer. When the device can not get contact to peer within 30 seconds, it will change to new state "No contact to peer".
No contact to peer	The contact to the RFD- peer is not established, yet. The reason can be network problems or wrong settings on local or remote site.
Peer does not accept RFD	Peer is existing, but no RFD support. Check whether the LPT/RFD stack is enabled on peer.
Peer connected	Communication to peer is established, packets are received. RFD-stack is operational.

Table 4-6 LPT/RFD Status (continued)

Status	Description
Communication disturbance	The device has detected missing packets (due to a sequence number) are corrupted packets from the peer. Check the quality of the network, it might be corrupted.
Contact to peer lost	The contact to the peer was established before, but has gone now. The reason can be network problems or changed settings on remote site.
Both peers in IMPLICIT mode - Failure	It is not allowed, that both peers are in IMPLICIT mode. At least one must be EXPLICIT.
Invalid status detected!	Internal failure of the LPT/RFD stack has occurred. You should never see this.

The individual ports can be disabled and enabled by LPT and RFD if the settings allow this. In the following table the states of interfaces and the message in the management application is presented.

Table 4-7 Interface States due to LPT/RFD

Status	Description
Port down	The port has no link detected. This is not due to LPT/RFD!
Port up	The port has detected link and is working fine.
Port disabled	The port is disabled by admin.
Stopping LPT/RFD	The port was disabled by LPT or RFD and will come up again, now. At this moment it is not clear yet, whether the port will enter the "Port up" or "Port down" state.
Disabled by LPT	LPT has disabled the port, due to a Line failure. Note: Note: This will state is called in the port-overview as "Disabled by LPT/RFD".

Table 4-7 Interface States due to LPT/RFD (continued)

Status	Description
Disabled by RFD	RFD has disabled the port, due to a remote port's failure. Note: Note: This will state is called in the port-overview as "Disabled by LPT/RFD".
Disabled, no RFD peer	RFD has disabled the port, due to a missing link to the peer. Note: Note: This will state is called in the port-overview as "Disabled by LPT/RFD".

Rapid Spanning Tree Protocol

The EDX100x supports the Rapid Spanning Tree Protocol (RSTP) according to [IEEE 802.1D] and [IEEE 802.1w]. Hereby, it is possible to prevent ring topologies and consequently circulating packets. Rapid Spanning Tree is an enhancements of the formerly existing Spanning Tree Protocol (STP). RSTP and STP are fully compatible. The only drawback when using both techniques in the same network is that all the "rapid" benefits of RSTP are gone. But inter operability is possible.

RSTP is a refinement of STP and therefore share most of its basic operation characteristics. However there are some notable differences as summarized below:

- Detection of root switch failure is done in 3 hello times or 6 seconds if default hello time have not been changed. This leads to must faster repair and re-operational of Ethernet networks.
- Ports may be configured as Edge ports if they are attached to a LAN which has no other bridges attached. These edge ports transition directly to the forwarding state. RSTP still continues to monitor the port for BPDUs in case a bridge is connected. RSTP can also be configured to automatically detect edge ports.
- Unlike in STP, RSTP will respond to BPDUs sent from the direction of the root bridge. An RSTP bridge will propose to its designated ports its spanning tree information. If another RSTP bridge receives this information, determines this is the superior root information, and sets all its other ports to discarding the bridge may send an agreement to the first bridge confirming its superior spanning tree information. The first bridge, upon receiving this agreement, knows it can rapidly transition that port to the forwarding state bypassing the traditional listening/learning state transition. This essentially creates a cascading effect away from the root bridge where each designated bridge proposes to its neighbours to determine if it can make a rapid transition. This is one of the major elements which allows RSTP to achieve faster convergence times than STP.
- As port roles details above shows, RSTP maintains back up details regarding discarding ports. This avoids time-out if the current forwarding ports were to fail or BPDUs were not received on the root port in a certain interval.

NOTE: RSTP and STP is only supported for LINE-Ports.

NOTE: Rapid Spanning Tree (RSTP) are not supported by the EDX1000 and EDX1002. Both devices have only one LINE-Port and so RSTP does not make any sense.

All devices in the topology must support (R)STP if it shall be used in the network. The devices communicate with each other, to find the “best” route through the network. If a redundant path has been found, one device breaks the connection and a ring free topology is achieved. The devices permanently check the topology and if any changes are detected, the (R)STP process may change the active and passive routes. RSTP realizes very fast reaction of changes. The time to recover is below 1 second. In case STP is used, the detection of changes and the new topology can take up to 30 seconds!

EAPS (Ethernet Automatic Protection Switching)

An alternative/complement mechanism to the (R)STP is the Ethernet Automatic Protection Switching (EAPS) according to [IETF RFC 3619]. This algorithm guarantees switching times of less than 50 ms in typical applications (see Figure 4-10 and Figure 4-11). One EDX100x must be configured as “Master”, the other one(s) as “Transit”. The Master takes the “ring” control and initiates the switch-over, if any link fails. This assures that no packets can circulate or get lost.

EAPS requires an own VLAN to transport special packets in the ring. These packets are used to check whether there is a link failure and to inform “Master”-node about link failure. These special packets allow a very quick detection and report of failures and enable the EAPS to achieve protection switching time of less than 50ms.

The concept of EAPS operation is given in [IETF RFC 3619]:

“An EAPS Domain exists on a single Ethernet ring. Any Ethernet Virtual Local Area Network (VLAN) that is to be protected is configured on all ports in the ring for the given EAPS Domain. Each EAPS Domain has a single designated “master node”. All other nodes on that ring are referred to as “transit nodes”.

Of course, each node on the ring will have 2 ports connected to the ring. One port of the master node is designated as the “primary port” to the ring, while the other port is designated as the “secondary port”.

In normal operation, the master node blocks the secondary port for all non-control Ethernet frames belonging to the given EAPS Domain, thereby avoiding a loop in the ring. Existing Ethernet switching and learning mechanisms operate per existing standards on this ring. This is possible because the master node makes the ring appear as though there is no loop from the perspective of the Ethernet standard algorithms used for switching and learning. If the master node detects a ring fault, it unblocks its secondary port and allows Ethernet data frames to pass through that port. There is a special “Control VLAN” that can always pass through all ports in the EAPS Domain, including the secondary port of the master node.

EAPS uses both a polling mechanism and an alert mechanism, described below, to verify the connectivity of the ring and quickly detect any faults.”

NOTE: Ring mode is not supported by the EDX1000 and EDX1002.

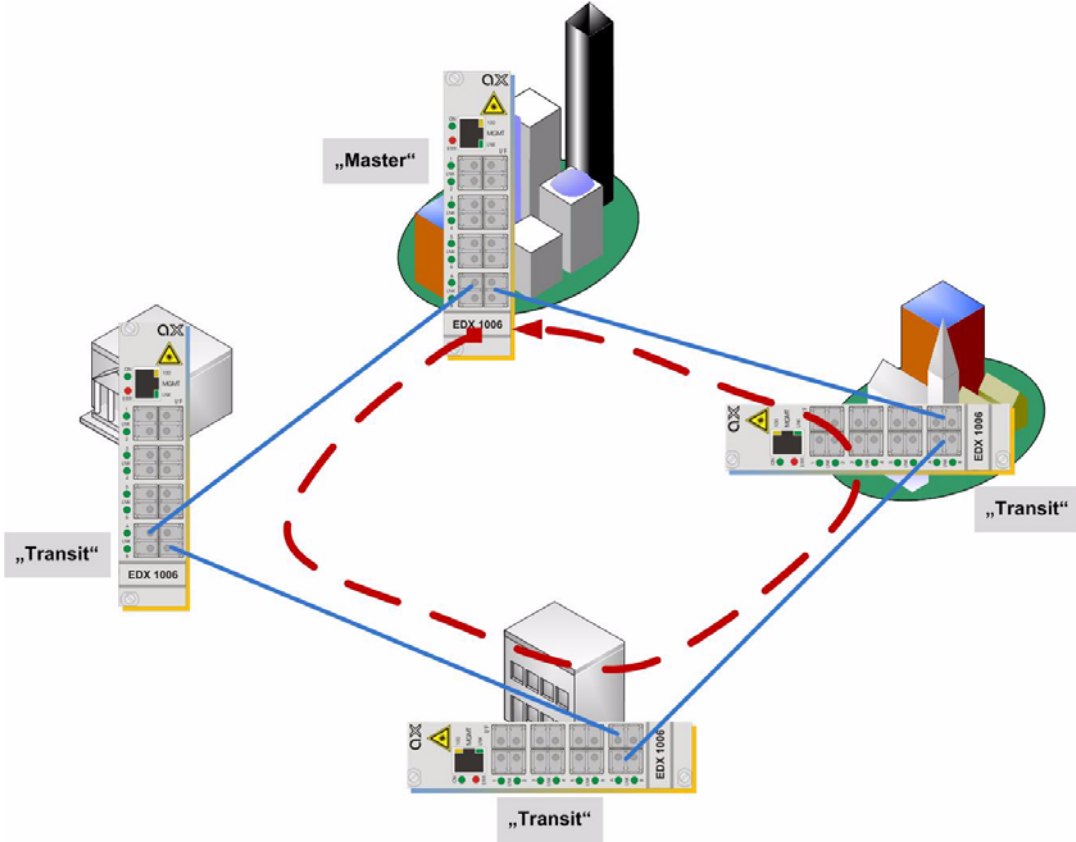


Figure 4-10 EDX1000 Ring Protection

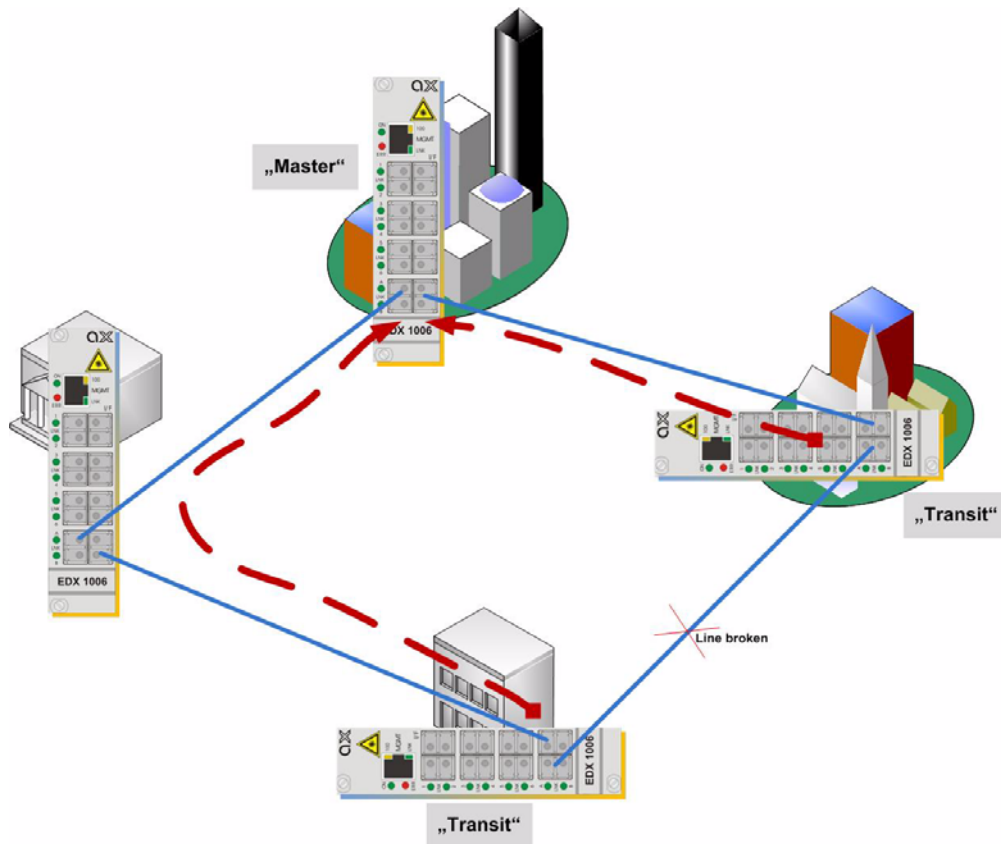


Figure 4-11 Ring Protection activated

Line-Protection w/ EAPS

A very special “ring” is a point-2-point protection of two EDX. In this back-2-back scenario, one EDX has to be configured as Master and the other in Transit-Mode and a very fast line protection can be achieved.

Auto Negotiation

Modern Ethernet interfaces support a mechanism called Auto-negotiation to allow connection of ports with different capabilities. During the auto-negotiation process

- Speed (10, 100 or 1000Mbps),
- Duplex mode (full duplex or half duplex),
- Flow Control capabilities and
- Clock Settings

are defined for the established link.

Speed and Duplex

Auto-negotiation is part of [IEEE 802.3], the Ethernet standard. It was first defined in 1995 as IEEE 802.3u and was an optional implementation. Unfortunately at this time the standard gave partly space for interpretation and so different implementation in older equipment can be found. In 1998 the debatable portions were eliminated and a year later the standard was extended for Gigabit-Ethernet.

In the market, there is still a lot of the older equipment, where auto-negotiation was not clear defined, so there may occur problems when devices try to do auto-negotiation. So some devices do still expect to “talk” auto-neg, even when the port’s speed and duplex mode are strictly defined by the user. For this reason, EDX100x supports to enable and/or disable the auto-neg communication, when the port’s speed or duplex mode is not really matter of negotiation but fixed by the user.

Please see table below for the possible settings and the resulting behaviour.

Table 4-8 Settings Auto-Negotiation

Setting	Result		
	Speed	Duplex	Remark
Auto Speed, Auto Duplex	10, 100 or 1000 Mbps ⁱ	Full or Half Duplex ⁱⁱ	Full Auto-neg takes place; no limitations are given.
Auto Speed, FDx	10, 100 or 1000 Mbps ⁱ	Full Duplex	Auto-neg takes place for speed; Duplex mode is given (FD).
Auto Speed, HDx	10, 100 or 1000 Mbps ⁱ	Half Duplex	Auto-neg takes place for speed; Duplex mode is given (HD).
1000Mbit/s, Auto Duplex	1000 Mbps (GigE)	Full or Half Duplex ⁱⁱ	Auto-neg takes place for duplex mode; speed is given (1000Mbps).
1000Mbit/s, FDx	1000 Mbps (GigE)	Full Duplex	Auto-neg communication is still done, so the possible result is limited to the given values (1000; FD).
1000Mbit/s, HDx	1000 Mbps (GigE)	Half Duplex	Auto-neg communication is still done, so the possible result is limited to the given values (1000; HD).

Table 4-8 Settings Auto-Negotiation (continued)

Setting	Result		
	Speed	Duplex	Remark
1000Mbit/s, FDx fixed	1000 Mbps (GigE)	Full Duplex	No Auto-neg communication is done; Speed and Duplex mode are given (1000; FD).
1000Mbit/s, HDx fixed	1000 Mbps (GigE)	Half Duplex	No Auto-neg communication is done; Speed and Duplex mode are given (1000; HD).
100Mbit/s, Auto Duplex	100 Mbps (FastE)	Full or Half Duplex ⁱⁱ	Auto-neg takes place for duplex mode; speed is given.
100Mbit/s, FDx	100 Mbps (FastE)	Full Duplex	Auto-neg communication is still done, so the possible result is limited to the given values (100; FD).
100Mbit/s, HDx	100 Mbps (FastE)	Half Duplex	Auto-neg communication is still done, so the possible result is limited to the given values (100; HD).
100Mbit/s, FDx fixed	100 Mbps (FastE)	Full Duplex	No Auto-neg communication is done; Speed and Duplex mode are given (100; FD).
100Mbit/s, HDx fixed	100 Mbps (FastE)	Half Duplex	No Auto-neg communication is done; Speed and Duplex mode are given (100; HD).
10Mbit/s, Auto Duplex	10 Mbps	Full or Half Duplex ⁱⁱ	Auto-neg takes place for duplex mode; speed is given.
10Mbit/s, FDx	10 Mbps	Full Duplex	Auto-neg communication is still done, so the possible result is limited to the given values (10; FD).

Table 4-8 Settings Auto-Negotiation (continued)

Setting	Result		
	Speed	Duplex	Remark
10Mbit/s, HDx	10 Mbps	Half Duplex	Auto-neg communication is still done, so the possible result is limited to the given values (10; HD).
10Mbit/s, FDx fixed	10 Mbps	Full Duplex	No Auto-neg communication is done; Speed and Duplex mode are given (10; FD).
10Mbit/s, HDx fixed	10 Mbps	Half Duplex	No Auto-neg communication is done; Speed and Duplex mode are given (10; HD).

i. Depending on ports capability and auto-negotiation result.

ii. Depending on auto-negotiation result. All EDX1000 ports do support full duplex mode.

Chapter 5

EDX100x Control Software & gCLI

The EDX100x has a common management core, which can be accessed via different ways (see “Direct Access to the EDX100x” on page 4-11). All options - besides SNMP - will lead to the graphical Command Line Interface (gCLI), which is a very easy way to configure and monitor the unit. In spite to a classical CLI, one does not have the need to learn cryptic instruction sets and has to move in thousands of sub-directories.

In this chapter the gCLI will be presented and the different options of configurations explained.

Menu Structure

The menu tree structure of the EDX100x is independent of the access (RS-232 serial control port or Telnet/SSH connection via the Ethernet MGMT port at the front panel or remote access). Login and navigating within the menus is described in “Login Menu” on page 5-3. The write- or change- access to many items depends on the Access Level's height,

AL: 1= Guest, 2= User, 3= Administrator.

All items are readable for any access level.

Menu Item	Refer to:
GENERAL SYSTEM INFORMATION	page 5-7
Inventory	page 5-9
ADMINISTRATION	page 5-10
User & Access Administration	page 5-12
Users & Passwords (CLI)	page 5-12
Add Account	page 5-14
Change Password	page 5-15
SSH Access	page 5-16
Add Key	page 5-17
SNMP Access	page 5-18
SNMP Community Configuration	page 5-19
SNMP Trap Receiver Config.	page 5-21
IP Configuration	page 5-23
Date and Time Settings	page 5-27
Reset System	page 5-28

Menu Item (continued)	Refer to:
Software Download	page 5-30
Configuration Handling	page 5-33
Alarm Mgmt Configuration	page 5-34
INTERFACES AND PORTS	page 5-36
Ethernet Ports	page 5-37
Edit Port Settings	page 5-41
Ext. Settings (SFP Port)	page 5-42
Ext. Settings (LAN Port)	page 5-44
Priority Settings	page 5-45
Port-Prio-Mapping	page 5-47
VLAN-Prio-Mapping	page 5-48
IP Prio Settings	page 5-50
Global Settings	page 5-51
SFP Ports	page 5-52
Display SFP Data	page 5-52
SFP Diagnostics	page 5-54
UART Configuration	page 5-55
Operation Modes	page 5-56
Ring Settings ⁱ	page 5-58
LPT/RFD Settings	page 5-59
VLAN Setup	page 5-63
VLAN Settings: Port View	page 5-64
VLAN Settings: VLAN View ⁱ	page 5-66
Edit VLAN ID	page 5-67
BANDWIDTH LIMITATION SETTINGS	page 5-68
Edit Port Settings	page 5-68
Ingress Bandwidth Limitation	page 5-70
Egress Bandwidth Limitation	page 5-72
Rapid Spanning Tree Settings ⁱ	page 5-74
RSTP Global Settings	page 5-75
RSTP Port Settings	page 5-76
Edit RSTP Settings	page 5-77
PERFORMANCE MONITORING	page 5-78
Ethernet Performance Data	page 5-78
Read detailed Ethernet Counter	page 5-80
In Counters	page 5-81
In Problem Packets	page 5-83
Out Counters	page 5-84

Menu Item (continued)

Histogram Counter
Out Problem Packets
Set Histogram Options

Refer to:

page 5-85

page 5-87

page 5-88

i. This menu is not visible on EDX1000 and EDX1002.

Login Menu

After a management connection has been established towards the EDX100x and the Enter key has been pressed, the login menu is displayed. The management software may be accessed by the user with different access levels (see “Security Issues” on page 4-16). An auto logout time may be specified for higher access levels to protect the system against illegal access. After the specified period of inactivity the message ‘Time-out, auto logout performed’ appears on the screen.

NOTE: Autologout = 0 means that the user will never logout automatically.

The Login menu is shown in the figure below. The user selects his login level from the following menu by entering the corresponding user name and password.

```
/Login for serial number: 123456

      Autologout [s]                900

      User

      Passwd

      Login

      Exit
```

A user name and a valid password have to be entered before access to configuration parameters is granted. The default user name and password are as follows:

User: admin
Password: private

“Autologout” is the time constant in seconds on which the login session will be dropped. The default autologout is '900'. To disable this feature select '0'.

CAUTION: It is strongly advised to change these passwords in the USER ADMINISTRATION menu after the first login.

If the device is started-up the very first time, the only user 'admin' is defined with the password 'private', which should be changed immediately after login. The password is not displayed, each character is replaced by an asterisk (*). An error message will be displayed for any unsuccessful login (the application continues with the login menu).

NOTE: Be careful, when typing the password. The CLI does not accept a "backspace" to correct a mistyped character. In this case you have to re-enter the password.

The top line of each menu displays the path of the menu tree. The bottom line of each screen may display text with additional information to the selected line (where the cursor stands). These two lines are highlighted, not selectable, and included in the listed menus within this chapter.

Navigating

The CLI is a graphic oriented user menu. Using the keyboard of your PC you can select menu entries, leave and update the menu-pages and get to some special sites. Please see below the actions and an overview to the keys.

Select a Menu Entry

All menu lines with blue coloured text, depict with italic letters in the screenshots, are accessible by the cursor¹. Black lines display only. Select any coloured menu text of interest by cursor-up/ -down keys and press the Enter key. This will give access to the item of the line.

In some cases, you will find lists to select an entry. Use also the cursor-up/ -down keys to navigate in these list. Press Enter, when the right entry is highlighted to select it.

Page Update

Pressing a 'u' (or 'U') causes the actual shown page to be updated and rebuild. This will be helpfully in case the view is damaged or information has (occasionally) changed.

Alarmlog

Pressing an 'a' (or 'A') forces the CLI to show the Alarmlog. The Alarmlog is a living list of all raised and cleared alarms, starting when a user logs into the CLI. An Autologout (due to inactivity) does not stop the alarm logging. The Alarmlog page can be left by pressing ESC.

Exit

The selection of Exit always returns to the next higher menu, finally to the login menu. Exit has the same effect as the ESC key and/or 'q'. Pressing the ESC key and/or 'q' will

1. The colors depend on the settings of your terminal program.

bring you back one menu level. If you are at the main menu, this will bring you back to the login entry prompt. Pressing ESC and/or 'q' again will log-out and blank the screen. Press the Enter key to redraw the login menu.

Overview to Keys

Table 5-1 provides information on the menu options.

Table 5-1 Overview to key-strokes

Key	ASCII	Action	Remark
Enter (CR)	13	Selects the chosen entry.	Depending on the type of entry, different actions will happen: <ul style="list-style-type: none">• A new menu-page is opened• Open a pull-down menu and select one of the offered entries.• Enter a proper value or a string in a edit-line.
ESC	27	Leaves the current menu-page.	It make take a second after pressing the ESC key before the page is quit. To accelerate this, press 'space' after ESC. Use ESC to leave pull-down menus and/or edit-lines.
a	97	Change to the Alarm-log view.	
q	113	Leaves the current menu-page.	'q' can not be used to leave pull-down menus or edit-lines.
u	117	Update the current view.	
ArrowDown	258	Moves cursor down in the menu.	The cursor moves only from selectable to selectable entry. At the bottom entry of the menu, the cursor will be set to the top entry, after pressing ArrowDown.
ArrowUp	259	Moves cursor up in the menu.	The cursor moves only from selectable to selectable entry. At the top entry of the menu, the cursor will be set to the bottom entry, after pressing ArrowUp.

Main Menu

After the login, the Main menu will be displayed, which provides a general overview of the menu structure.

```
/EDX1000

      General System Information

      Administration

      Interfaces and Ports

      Operation Modes

      VLAN Setup

      Bandwidth Limitation Settings

      Rapid Spanning Tree Settings           RSTP Disabled

      Performance Monitoring

      Logout

                                           (a): Alarmlog
```

Select a menu line with the cursor keys and press the Enter key to open the selected submenu or to logout from the EDX100x's CLI.

Table 5-2 provides information on the menu options.

Table 5-2 EDX100x Menu Options

Parameter	Description	Format	Default
General System Information	Set and get global static information.	Menu	
Administration	Configuration of global parameters.	Menu	
Interfaces and Ports	Configuration of physical interfaces and ports.	Menu	
Operation Modes	Configuration of different modes.	Menu	
VLAN Setup	Configuration of VLANs.	Menu	
Bandwidth Limitation Settings	Configuration of Ingress/Egress bandwidth limitations on the ports.	Menu	

Table 5-2 EDX100x Menu Options (continued)

Parameter	Description	Format	Default
Rapid Spanning Tree Settings ⁱ	Configuration of RSTP.	Menu	
Performance Monitoring	Read and reset performance data.	Menu	
Logout	Leave CLI and terminate the session.	Exit	

i. This line is only visible, when more than one LINE-port is available on the present variant.

General System Information

Select "General System Information" in the Main menu and press the Enter key to access the General System Information menu. The following screen will be displayed:

```
/EDX1000/General System Information

      Device Name                < ... >
      Device location          < ... >
      Contact Person           < ... >

      Inventory

      Time                        09.08.2008 17:21:17
      System Uptime               21d 08:12:50
      Temperature                 30,5 °C

      Exit

(a): Alarmlog
```

This menu contains the general system information of the EDX100x device and system. Table 5-3 provides information on the menu options.

Table 5-3 General System Information Menu Options

Parameter	Description	Format	Default
Device Name	Description/comment of the device/application.	Display/Input (up to 20 characters)	< ... >
Device Location	Present device location.	Display/Input (up to 20 characters)	< ... >
Contact Person	Place holder to input the name of a person for the case of troubleshooting.	Display/Input (up to 20 characters)	< ... >
Inventory	Opens the Inventory menu	Menu	
Time	The current date and time of the device.	Display	no default
System Uptime	The time since the last system re-boot.	Display	no default
Temperature	Present operating temperature of the device.	Display	no default
Exit	Leave the menu page.	Exit	

Inventory

Selecting “Inventory” and pressing the Enter key leads to the Inventory menu, which provides information on the device. These are factory settings which can only be read.

```

/EDX1000/General System Information/Inventory

      Device Type                EDX1000

      Serial Number              123456

      HW Revision                1.1.0.1

      Article Revision           GS1

      Software Version           V 2_1_43

      Date of Production        2015-05-12

      Manufacturer               arcutronix GmbH

      Order Info                 0716-2001

      Exit

(a): Alarmlog
    
```

Table 5-4 provides information on the menu options.

Table 5-4 Inventory Menu Options

Parameter	Description	Format	Default
Device Type	Indicates the device type.	Display	EDX1000
Serial Number	Serial number of the device.	Display	Depends on the factory settings
HW Revision	Revision of the device hardware.	Display	Depends on the factory settings
Article Revision	The release number of the device.	Display	Depends on the factory settings
Software Version	Revision of the loaded system software.	Display	Depends on the loaded software
Date of Production	Date of the device's production.	Display	Depends on the factory settings

Table 5-4 Inventory Menu Options (continued)

Parameter	Description	Format	Default
Manufacturer	Manufacturer of the Device (normally arcutronix GmbH).	Display	arcutronix GmbH
Order Number	Order information for the device.	Display	Depends on the device type. See Order Matrix (Table 1-1 on page 1-5).
Exit	Leave the menu page.	Exit	

Administration

Select "Administration" in the Main menu and press the Enter key. The Administration menu will be displayed. This menu allows to configure the general device settings.

```
/EDX1000/Administration

  User & Access Administration
  IP Configuration                192.168.1.100

  Date and Time Settings         11.30.2006 17:58:45

  Reset System                   No reset scheduled
  Software Download               Idle

  Configuration Handling
  Alarm Mgmt Configuration

  Exit

(a): Alarmlog
```


Table 5-5 provides information on the menu options.

Table 5-5 Administration Menu Options

Parameter	Description	Format	Default
User & Access Administration	Administration of users, access levels and passwords.	Menu	
IP Configuration	Configuration of the IP interfaces.	Menu	
Date and Time Settings	Configure system date and time.	Menu/Display	displays actual time and date
Reset System	Opens the Reset System menu.	Menu/Display	No reset scheduled
Software Download	Update the current SW version.	Menu/Display	Idle
Configuration Handling	Load or store configuration profiles.	Menu	
Alarm Mgmt Configuration	Configuration to store the Alarm List onto a TFTP-file-server.	Menu	
Exit	Leave the menu page.	Exit	

User & Access Administration

Select “Access Administration” in the Administration menu and press the Enter key. The Access Administration menu will be displayed:

```

/EDX1000/Administration/Access Administration

      Users & Passwords

      Telnet Access                               Enabled

      SSH Access

      SNMP Access                               Enabled

      Exit

(a): Alarmlog
    
```

Table 5-7 provides information on the menu options.

Table 5-6 User Administration Menu Options

Parameter	Description	Format	Default
Users & Passwords	Configuration of user- names and passwords.	Menu	
Telnet Access	Configuration of telnet access.	PullDown-Menu • Enabled • Disabled	Enabled
SSH Access	Configuration of SSH access.	Menu	
SNMP Access	Configuration of the SNMP access to the device.	Menu/Display	Enabled
Exit	Leave the menu page.	Exit	

Users & Passwords

This menu gives the administrator the capability to add/remove users and change their passwords if necessary. The maximum number of possible users defined for EDX1000 is 99.

On top of the page is a list with all configured users and their read and write rights.

The list has only one entry after first start-up and/or “Load Default Cfg”. This entry is the user “admin”.

```

/EDX1000/Administration/Access Administration/Users

      User Name      Read Access      Write Access

      admin          adm              adm

      Add Account

      Delete Account

      Change Password

      Exit

(a): Alarmlog
    
```

Table 5-7 provides information on the menu options.

Table 5-7 Users & Passwords Menu Options

Parameter	Description	Format	Default
Add Account	Add an user account.	Menu	
Delete Account	Press Enter and select an user of the (scroll) list. After this confirm the action.	SelectList/Confirm	
Change Password	Press Enter and select an user of the (scroll) list. After this the Change Password menu opens.	SelectList/Menu	
Exit	Leave the menu page.	Exit	

Add Account

Select "Add Account" in the Users menu and press the Enter key. The following screen will be displayed:

```

/EDX1000/Administration/Access Administration/Users/Add Account

      Username                < ... >

      Password

      Retype Password

      Access Level (r)        Unknown

      Access Level (w)        Unknown

      Create Account

      Exit

(a): Alarmlog

```

Table 5-8 provides information on the menu options.

Table 5-8 Add Account Menu Options

Parameter	Description	Format	Default
Username ⁱ	Enter name of new user.	Display/Input	< ... >
Password ⁱⁱ	Definition of a new password.	Input	no default
Retype Password	Retype field for the new chosen password.	Input	no default
Access Level (r)	The read access level is allocated.	PullDown-Menu • adm • usr • guest	Unknown
Access Level (w)	The write access level is allocated.	PullDown-Menu • adm • usr • guest	Unknown

Table 5-8 Add Account Menu Options (continued)

Parameter	Description	Format	Default
Create Account	Press Enter to confirm new user data.	Confirm	
Exit	Leave the menu page.	Exit	

i. The user name must consist of less than 15 characters (≤ 14). The following characters are allowed: '0-9', 'a-z', 'A-Z', '_', '.'.

ii. The password must consist of more than 4 and less than 16 characters ($5 \leq n \leq 15$). The following characters are allowed: '0-9', 'a-z', 'A-Z', '_', '.'.

Note: The maximum number of different users is 99.

Note: You can check, whether the operation succeeded in the “User & Passwords (CLI)” Menu (page 5-12). There you can see all created users and their read- and write-permission.

Change Password

Select “Change Password” in the Users menu and press Enter key to highlight user-name list. Choose the user-name whose password is to be changed and press the Enter key. The following screen will be displayed:

```
/EDX1000/Administration/Access Administration/Users/Change Password

      Changing password for user      admin

      New Password

      Retype Password

      Change

      Exit

(a): Alarmlog
```

Table 5-9 provides information on the menu options.

Table 5-9 Change Password Menu Options

Parameter	Description	Format	Default
New Password	Definition of a new password.	Input	no default
Retype Password	Retype field for the new chosen password.	Input	no default
Change	Press Enter to confirm the changes.	Action	
Exit	Leave the menu page.	Exit	

SSH Access

This menu lists keys and allows to add respectively delete SSH public keys. On top of the page is a list with all configured public keys.

This menu displays a list of all defined SSH keys. Select “Delete Key” and press the Enter key in order to highlight the key list. Then, choose the key to be deleted and press the Enter key again to delete the selected key.

NOTE: The action must be confirmed before it will be executed.

The list is empty after first start-up and/or “Load Default Cfg”.

```

/EDX1000/Administration/Access Administration/SSH Access

SSH Public Keys

ssh-dss AAAAB3NzaC1kc3MAAACBAIWOpttRlM7lTQ+h51otR6J6TFejE2CugZOXQWcQ6

Delete Key

Add Key

Exit

(a): AlarmLog

```

Table 5-10 provides information on the menu options.

Table 5-10 SSH Access

Parameter	Description	Format	Default
Delete Key	Press Enter and select a key of the (scroll) list. After this confirm the action.	SelectList/Confirm	
Add Key	Add a SSH public key.	Menu	
Exit	Leave the menu page.	Exit	

Add Key

Select “Add Key” in the SSH Access menu and press the Enter key. The following screen will be displayed:

```
/EDX1000/Administration/User Administration/SSH Access/Add Key

Key          ssh-dss
State        Key successfully added

Exit

(a): Alarmlog
```

Insert (via cut and paste) your own ssh public key into the field ‘Key’. The ‘State’ line will report, if the key was added successfully or if an error has occurred. After adding the key leave the menu with ‘Exit’. The added public key is listed below ‘SSH Public Key’.

SNMP Access Menu

This menu offers the possibility to configure the SNMP settings, like communities and trap-receivers. If required by the user, the SNMP access can be disabled at all, to avoid illegal access to the device. In factory default, the SNMP access is enabled.

```

/EDX1000/Administration/SNMP Access

      SNMP Access                               Enabled

      SNMP Communities

      SNMP Trap Receiver

      Exit

(a): Alarmlog
    
```

Table 5-11 provides information on the menu options.

Table 5-11 *SNMP Access Menu Options*

Parameter	Description	Format	Default
SNMP Access	Enables or disables the SNMP access.	PullDown-Menu • Disabled • Enabled	Enabled
SNMP Communities	Add, change and delete the communities and the related access levels.	Menu	
SNMP Trap Receiver	Add, change and delete the Trap receivers.	Menu	
Exit	Leave the menu page.	Exit	

NOTE: SNMP is based on IP based data transmission. Make sure the IP configuration is correct and a Default-GW is defined.

SNMP Community Configuration Menu

This menu lists the defined SNMP community strings and allows to add, change and delete the community settings. Each SNMP community can be assigned with an access level, which grants rights for set- and/or get-commands.

```

/EDX1000/Administration/SNMP Access/SNMP Community Configuration

SNMP Community Access Level

public      Monitor
private     Standard
admin       Administrator

          Edit SNMP Community Settings

          Delete SNMP Community

          Add SNMP Community

          Exit

(a): Alarmlog

```

At the head of the page the (pre)defined SNMP communities and the access levels are shown in a list. If there are more than 8 entries, only 8 entries are visible. You can navigate in the list, using the up/down arrow keys.

Table 5-12 provides information on the menu options.

Table 5-12 *SNMP Community Configuration Menu Options*

Parameter	Description	Format	Default
Edit SNMP Community Settings	Press Enter and select an entry in the (scroll) list. After this the Edit SNMP Community menu opens.	SelectList/Menu	
Delete SNMP Community	Press Enter and select an entry in the (scroll) list. After this confirm the action.	SelectList/Confirm	
Add SNMP Community	Add a new SNMP community.	Action	
Exit	Leave the menu page.	Exit	

NOTE: When “Add SNMP Community” is selected, a new entry in the list above is created: “guest”, with access level *Guest*. Please select after this the “Edit SNMP Community Settings” to adapt the settings of the new community.

Edit SNMP Community Settings

```

...SNMP Access/SNMP Community Configuration/Edit SNMP Community Settings

      Community Name                public

      Access Level                 Monitor

                                          (a): Alarmlog

      Exit
    
```

Table 5-13 provides information on the menu options.

Table 5-13 Edit SNMP Community Menu Options

Parameter	Description	Format	Default
Community Name	Enter a (new) name for the community	Input	Guest
Access Level	Select the access level, associated with the community string.	PullDown-Menu <ul style="list-style-type: none"> • Guest • Monitor • Service • Standard • Administrator 	Guest
Exit	Leave the menu page.	Exit	

SNMP Trap Receiver Configuration Menu

This menu lists the defined SNMP trap receivers and allows to add, change and delete the receiver's settings.

```

/EDX1000/Administration/SNMP Access/SNMP Trap Receiver Configuration

SNMP Trap Receiver Version      Community      Comment
192.168.1.10:162    SNMP V2c    public        arcutronix's SNMP

      Edit SNMP Trap Receiver

      Delete SNMP Trap Receiver

      Add SNMP Trap Receiver

      Exit
(a): Alarmlog

```

At the head of the page the defined SNMP trap receivers and the associated information are shown in a list. If there are more than 8 entries, only 8 entries are visible. You can navigate in the list, using the up/down arrow keys.

In Default configuration, no trap receivers are defined.

Table 5-14 provides information on the menu options.

Table 5-14 SNMP Trap Receiver Menu Options

Parameter	Description	Format	Default
Edit SNMP Trap Receiver	Press Enter and select an entry in the (scroll) list. After this the Edit SNMP Trap Receiver menu opens.	SelectList/Menu	
Delete SNMP Trap Receiver	Press Enter and select an entry in the (scroll) list. After this confirm the action.	SelectList/Confirm	
Add SNMP Trap Receiver	Add a new SNMP Trap Receiver.	Action	
Exit	Leave the menu page.	Exit	

NOTE: When “Add SNMP Trap Receiver” is selected, a new entry in the list above is created. Please select after this the “Edit SNMP Trap Receiver” menu to adapt the settings of the new receiver.

Edit SNMP Trap Receiver

```

... Configuration/SNMP Trap Receiver Configuration/Edit SNMP Community Settings

      IP Address                192.168.1.10

      UDP Port                  162

      SNMP Version              V2c

      Community                 public

      Comment                   arcutronix's SNMP

      Exit

(a): Alarmlog
Leave menu page

```

Table 5-15 provides information on the menu options.

Table 5-15 Edit SNMP Trap Receiver Menu Options

Parameter	Description	Format	Default
IP Address	Enter the IP address of the trap receiver.	Input	0.0.0.0
UDP Port	Enter the UDP Port-number, used for traps. Normally Port 162 is ok.	Input	162
SNMP Version	Select the format of the trap, this receiver accepts	PullDown-Menu • V1 • V2c	V2c
Community	Enter a community string, which this receiver will accept for traps.	Input	public
Comment	Enter a short comment about this receiver.	Input	empty
Exit	Leave the menu page.	Exit	

IP Configuration Menu

Use this menu to configure the IP parameters of the IP port and to assign a VLAN ID to the management port. Select "IP Configuration" in the Administration menu and press the Enter key. The following screen will be displayed:

```

/EDX1000/Administration/IP Configuration

      IP Address Assignment           Manual

      IP Address                     192.168.1.100
      Network Mask                   255.255.255.0
      Default Gateway

      DHCP Server Set Default GW     Yes
      DHCP Server
      DHCP State                       Connecting to server ...

      Inband Mgmt                     VID 4094, Prio 6

      ax Remote Mgmt VLAN             Disabled (4093)

      Info: MAC Address                 00:20:F5:80:62:68

### Warning: changing one of these parameters may lead to contact loss! ###

      Exit

(a): Alarmlog

```

Warning: Any changes of the IP parameters may lead to contact loss with the device. Be careful when changing this attributes.
In case you made any changes a reconnection with the new IP address could be necessary.

Table 5-16 provides information on the menu options.

Table 5-16 IP-Configuration Menu Options

Parameter	Description	Format	Default
IP Address Assignment	Defines the IPv4 address assignment.	PullDown-Menu <ul style="list-style-type: none"> • Manual • Via DHCP Server • Via DHCP Server/ Auto IP 	Via DHCP Server
IP Address ⁱ	Configuration of the device's IPv4 address.	Display/Input	192.168. 1.100

Table 5-16 IP-Configuration Menu Options (continued)

Parameter	Description	Format	Default
Network Mask ⁱ	Configuration of the device's IPv4 network mask. When an IPv4 address is entered, a suggested network mask will be displayed.	Display/Input	255.255. 255.0
Default Gateway	Configuration of the device's Default Gateway IP address (IPv4).	Display/Input	no default
DHCP Server Set Default GW ⁱⁱ	Selector to appoint, whether the DHCP server is allowed to set the Default GW, too.	PullDown-Menu • Yes • No	Yes
DHCP Server ⁱⁱ	IP-address of the (discovered) DHCP-server. The IP-Address needs no setting.	Display	no default
DHCP State ⁱⁱ	Displays to state of connection to the DHCP-server.	Display	Connecti ng to Server...
Inband Mgmt	<p>Selector to appoint, whether the unit may send and receive management data via in-band (LINE) connection.</p> <p>If the a value of '0' , 'off' or 'disabled' is entered, the in-band channel is disabled, otherwise enter VID and VLAN Priority.</p> <p>To re-enable the in-band management again, enter 'on' or 'enable' to reactivate it with the latest VID (visible in brackets) or enter a valid VID.</p> <p>See below "Entering VID and Priority" for grammar.</p> <p>Note: When the in-band channel is disabled, the latest used VID is still reserved in side the device. This is noted by displaying "Disabled (old VID)".</p>	Display/Input	VID4094, Prio 6

Table 5-16 IP-Configuration Menu Options (continued)

Parameter	Description	Format	Default
ax-Remote Mgmt VLAN	<p>Selector to appoint, whether the unit may send and receive management data via ax-remote connection.</p> <p>If the a value of '0' , 'off' or 'disabled' is entered, the in-band channel is disabled, otherwise enter VID and VLAN Priority.</p> <p>To re-enable the in-band management again, enter 'on' or 'enable' to reactivate it with the latest VID (visible in brackets) or enter a valid VID.</p> <p>See below "Entering VID and Priority" for grammar.</p> <p>Note: When the in-band channel is disabled, the latest used VID is not allocated any longer.</p>	Display/Input	Disabled
Info: MAC Address	Displays the MAC address of the device.	Display	00:20:F5: aa:bb:cc
Exit	Leave the menu page.	Exit	

- i. This menu item is only selectable, if the manual IP address assignment is enabled. Otherwise it displays the assigned values.
- ii. This menu item is only visible, when DHCP IP address assignment is enabled. Otherwise it is invisible.

If the 'IP Address Assignment' is set to 'Via DHCP Server', configure additionally 'DHCP Server'. The result will be shown in 'DHCP State':

- Connecting to Server...
- Server not available
- Server found, but no answer
- Ok, got address from server.

Entering VID and Priority

Two fields are available to configure the in-band management link and the ax-remote management link. Both entries use the same notation and need only one entry-line. The entry can be done in different ways and will be interpreted by the device. The string presented after entry shows the result of interpretation.

To disable the link, enter either '0' (zero), 'disable' or 'disabled' (upper and lower case is not considered). The result shown is always 'Disabled'.

To enable the link, enter a (valid and not already allocated!) value for VID followed by the priority. If no priority is given the default value of '6' is assumed. The separator between VID and priority may be a space, a comma, text etc.

Note: In case the VID is not freed when entering 'off' etc., the "old" VID is written in brackets after the word 'Disabled': "Disabled (VID4094)". In this case the value can easily be reactivated and the management link enabled, by entering simply 'on' or 'enable' (upper and lower case is not considered).

Some examples are shown below.

Table 5-17 Entry of VID and Priority

Format	Example	Result
values only, separated by space	4094 6	VID 4094, Prio 6
value only, separated by comma	4094, 6	"
values with text	VID4094 Prio6	"
	V4094 P6	"
values with text and comma	VID4094, Prio6	"
	V4094, P6	"
Disable	0	Disabled
	off	"
	disable	"
	Disabled	"
re-activate; only possible when the old VID is still reserved. This is indicated by the displayed text:	on	VID 4094, Prio 6
	enable	"

- e.g. Disabled (4094)

- Valid values for VLAN priority field: 1... 4094 (as long as the VID is not already configured/allocated for other stuff).
- Valid values for VLAN priority field: 0... 7.

Date and Time Settings Menu

Use this menu to set the date, time, and time zone for the device.

```

/EDX1000/Administration/Date & Time Settings

    Current Date                05.12.2012
    Current Time               13:58:55

    Local Time Zone: GMT       0

    Time Server

    Time Server State           Not used

    Exit

(a): Alarmlog

```

Table 5-18 provides information on the menu options.

Table 5-18 Date and Time Settings Menu Options

Parameter	Description	Format	Default
Current Date	Indicates the current device's date (dd.mm.yyyy).	Display/Input	no default
Current Time	Indicates the current device's time (hh:mm:ss).	Display/Input	no default
Local Time Zone: GMT ⁱ	Indicates the relative time deviation to GMT, i.e. '+1' for Berlin.	Display/Input	+1
Time Server	If there is a time server, you may enter its IPv4 address in this field ⁱⁱ .	Display/Input	no default

Table 5-18 Date and Time Settings Menu Options (continued)

Parameter	Description	Format	Default
Time server State	If a time server is used, this field will indicate the result and progress of time synchronization (Not used Not available Connecting Synchronizing Lost sync Synchronized).	Display	Not used
Exit	Leave the menu page.	Exit	

- i. Changes in the Local Time Zone have effect only after Reset
- ii. The EDX100x expects an NTP-server.

Reset System Menu

Use this menu to reset the EDX100x manually immediately or at a scheduled time.

```

/EDX1000/Administration/Reset System

Reset State                               No reset scheduled

Reset Mode                                 At specified Time

Current Time                               05.12.2012 14:22:09
Reset Date
Reset Time

Reset System

Error State                               Reset Date/Time does not exist

Exit

(a): Alarmlog

```

Table 5-19 provides information on the menu options.

Table 5-19 Reset System Menu Options

Parameter	Description	Format	Default
Reset State	Indicates the device's reset state (No reset scheduled System is going down... Reset scheduled).	Display	No reset scheduled
Reset Mode	Defines the device's reset mode.	PullDown-Menu <ul style="list-style-type: none"> • At specified Time • Immediate Reset 	Immediate Reset
Current Time ⁱ	Indicates the current device's date and time (dd.mm.yyyy hh:mm:ss).	Display	no default
Reset Date ⁱ	Enter the date for restart (dd.mm.yyyy).	Display/Input	no default
Reset Time ⁱ	Enter the time for restart (hh:mm:ss).	Display/Input	no default
Reset System	Press Enter to confirm the settings.	Confirm	
Error State	Indicates the result of an system reset (Ok Reset Date/Time is in the past Reset Date/Time does not exist Not allowed (download active)).	Display	no default
Exit	Leave the menu page.	Exit	

i. This menu item is only visible, when the Reset Mode is set to "At specified time".

Note: Before a reset is executed you have to confirm with 'y' the warning line:

Attention! Data transmission will be interrupted. Continue (y/n)?

Software Download Menu

Use this menu to specify the file and the server, where the new software is stored. In addition you can specify when the new software is invoked.

```

/EDX1000/Administration/Software Download

      Server Address                192.168.1.1
      Specfile                    tftp_root/dlimage.spec

      Skip Up-to-date Test         No

      Autorestart Mode             At specified time
      Current Time                   05.12.2012 14:59
      Restart Date                 06.12.2012
      Restart Time                 01:00:00

      Download State                  Idle
      Error State                     Ok
      Reset State                      No reset scheduled

      Start Download

      Exit

(a): Alarmlog

```

Table 5-20 provides information on the menu options.

Table 5-20 Software Download Menu Options

Parameter	Description	Format	Default
Server Address	The IPv4 address of the TFTP server (PC). The server must be reachable via one of the configured IP interfaces (e.g. via the default GW).	Display/Input	no default
Specfile ⁱ	The download file and path, located on the TFTP server. The path has to be written with slash ('/'), e.g. root/EDX1000/dlimage.spec	Display/Input	dlimage.spec
Skip Up-to-date test	Defines, if only the out-dated files ('No') or all software parts ('Yes') will be replaced during download. This effects the overall download time.	PullDown-Menu <ul style="list-style-type: none"> • No • Yes 	No

Table 5-20 Software Download Menu Options (continued)

Parameter	Description	Format	Default
Autorestart Mode	Defines the auto restart mode.	PullDown-Menu <ul style="list-style-type: none"> • Immediately • At specified time • Off 	Immediately
Current Time ⁱⁱ	Displays the actual time of the device. This helps to setup the correct time for restart.	Display	no default
Restart Date ⁱⁱ	Enter the date for restart (dd.mm.yyyy).	Display/Input	no default
Restart Time ⁱⁱ	Enter the time for restart (hh:mm:ss).	Display/Input	no default
Download state	Indicates the download state (Idle Active Sending Restart Command... Sending Reboot Command... Download finished Download failed).	Display	Idle
Error state	Indicates the error state (Ok Critical Error, write failed Error, write failed Error, download data invalid Software up to date Restart Date/Time invalid Restart Date/Time is in the past Download completed).	Display	Ok
Reset State	Indicates the reset state (No reset scheduled System is going down... Reset scheduled).	Display	No reset scheduled
Start Download	Starts the software download.	Action	
Exit	Leave the menu page.	Exit	

i. The specfile is normally called "dlimage.spec".

ii. This menu item is only visible, when the Autorestart Mode is set to "At specified time".



Note: The Specfile's path has to be specified with slash (/), when used on a Windows based TFTP-server. Otherwise the TFTP-server can not locate the correct file.

Format: `root/./EDX1000/dlimage.spec`

Note: When you want to restart the device at a specified time, you first have to configure the device's correct time and date (see "Date and Time Setting Menu" on page 5-27).

You have to do some preparation before starting the software update:

1. Install the TFTP server from the CD-ROM to the PC. Follow the instructions (see the doc file in the same folder).
2. Unzip the archive with the EDX100x software to the TFTP server's download path.
3. Be sure the EDX100x can reach the TFTP server via IP.
 - Connect the TFTP server and the EDX100x via an IPv4 network (in the easiest way this is an Ethernet cable!)EDX100x.
 - Verify that the EDX100x and TFTP server have an IP connection (e.g. execute CMD to open a DOS shell on the server and try a 'ping 192.168.1.100').
4. Set the 'Server IP address' and 'Specfile' in the download menu.
5. Select 'Start Download' to start the download process.

If the update was successfully the EDX100x will reset at the specified time (takes about 1 minute). Log in again as admin and make settings for your application. You will read in the TFTP server's window i.e.:

```
Sent dimage.spec to (192.168.1.100), 366 bytes
Sent kernel-rtai-linux-denx-EDX to (192.168.1.100), 675510 bytes
Sent ramfs-EDX.ubt to (192.168.1.100), 1037974 bytes
Sent flashfs-EDX.tar.gz to (192.168.1.100), 4547767 bytes
```

If an error occurred, you may read in the Software Download menu status lines:

```
Download State      download failed
Error State         Error, download data invalid
Reset State         No reset scheduled
```

The Error State line will display the reason.

Critical Error, write failed	The device may be unusable after power-off.
Error, write failed	Download failed, old software is usable.
Error, download data invalid	The download files cannot be read or are not found (check the path).
Software up to date	Download is not executed.

Configuration Handling Menu

Use this menu to load and store EDX100x's configuration. It is used to store and recall individual configuration settings.

```

/EDX1000/Administration/Configuration Handling

Standard Configurations

Factory default setup

Select Standard Cfg

Overwrite IP Configuration      No

Server Address                  192.168.1.1
Configuration File              edx1002_130211.cfg
Load Configuration File
Store Configuration File

State

Exit

(a): Alarmlog

```

At the head of the page the predefined Standard Configuration is listed. It can be selected by “Select Standard Cfg” on this page. The Standard Configuration is as follows:

NOTE: This Default configuration is stored “onboard” and can be loaded without the usage of a TFTP server.

Name	Description
Factory default setup	Return to factory's default.

NOTE: You can always select, whether you want to keep your actual defined IP configuration or to overwrite it to default. This is done via the “Overwrite IP Configuration” entry.

To keep the IP configuration offers the possibility to load default configuration remotely, without losing contact.

If the IP address shall be overwritten, the following settings are chosen:

- local IP = 192.168.1.100
- line IP = empty
- default GW = empty

NOTE: The values of the “Factory Default Setup”, which are valid when you select it are listed in the tables in the column “Default” within this manual.

Table 5-21 provides information on the menu options.

Table 5-21 Configuration Handling Menu Options

Parameter	Description	Format	Default
Select Standard Cfg ⁱ	Press Enter and select an entry in the (scroll) list. After this the selected configuration is reloaded.	SelectList/Confirm	
Overwrite IP configuration	Select whether you want overwrite or keep the actual IP configuration. This entry is only valid, when a configuration is loaded. To keep the IP configuration offers the possibility to load default configuration remotely, without losing contact.	PullDown-Menu <ul style="list-style-type: none"> • No • Yes 	No
Server Address	The IPv4 address of the TFTP server (PC). The server must be reachable via one of the configured IP interfaces (e.g. via the default GW).	Display/Input	no default
Configuration File	Defines the path and name of the configuration file on the TFTP server.	Display/Input	no default
Load Configuration File ⁱ	Starts to load the specified configuration file from the server.	Confirm	
Store Configuration File	Starts to store the specified configuration file on the server.	Action	
State	Indicates the result of load respectively store the device's configuration file.	Display	no default
Exit	Leave the menu page.	Exit	

i. Loading of a (standard) configuration file may lead to service interrupt.

Alarm Mgmt Configuration Menu

The Alarm Management Menu gives access to the alarm conditions and to the storage-file of the alarm-list.

The Alarm conditions is used to trigger the Alarm LED, the Alarm relay and the SNMP-traps. As source for the Alarm can be either the Line-port(s) and/or the LAN-port(s).

All events/alarms are stored in the alarm-list. If the onboard storage for the alarm-list is full, the oldest alarm will be removed from the list to free buffer space. To avoid deletion of alarms due to lack of memory, the alarm-list can be stored externally on an TFTP-server. Use this menu to define the location and (part of) file name of the uploaded the alarm-list. After configuration of path and file name, the alarm-list is stored, when the internal buffer is going to be full. If no location/file is defined, old alarms will be overwritten.

```
/EDX1000/Administration/Alarm Mgmt Configuration

      Interface Alarms                Line IF(s) only

Alarm Status                          Alarm on

      Server Address                192.168.1.1

      Logfile Path                  ax/alarmists/

      Logfile Prefix                EDX1000_test1_

Exit

(a): Alarmlog
```

The alarm log file is stored on the TFTP server together with a prefix and the date/time when it was stored:

- **LogfilePath/LogfilePrefixalarmlog_year-month-day_hour-minute-second.log**

Table 5-22 provides information on the menu options.

Table 5-22 Alarm Management Configuration Menu Options

Parameter	Description	Format	Default
Interface Alarms	Definition, which types of interfaces are source for alarm-handling.	PullDown-Menu <ul style="list-style-type: none">• Ignore• Line IF(s) only• LAN IF(s) only• All IFs	Ignore
Alarm Status	Display to show the actual alarm status of the device.	Display	Alarm off
Server Address	The IPv4 address of the TFTP server (PC). The server must be reachable via one of the configured IP interfaces (e.g. via the default GW).	Display/Input	no default
Logfile Path	The download path, located on the TFTP server.	Display/Input	no default
Logfile Prefix	A prefix, added to the stored alarm log file, so one can distinguish the origin.	Display/Input	no default
Exit	Leave the menu page.	Exit	

Interfaces and Ports Menu

This Menu offers the configuration of the EDX100x's interfaces and ports.

```
/EDX1000/Interfaces and Ports

    Ethernet Ports

    SFP Ports

    UART Configuration

Exit

(a): Alarmlog
```

Table 5-23 provides information on the Interfaces and Ports menu options.

Table 5-23 Interfaces and Ports Menu Options

Parameter	Description	Format	Default
Ethernet Port	Selecting this option and pressing the Enter key leads to the Ethernet Ports menu.	Menu	
SFP Ports	Display SFP serial EEPROM contents. SFP vendor information.	Menu	
UART Configuration	Selecting this option and pressing the Enter key leads to the UART Configuration menu.	Menu	

Ethernet Ports

This menu allows the user to display and to configure the settings for the Ethernet ports. On top of the menu an overview of all equipped Ethernet ports is shown. Depending on

the EDX100x Hardware version you have a different menu. The usage of the menu is very similar for all variants and will be depicted in “Menu Options” on page 5-40.

Ethernet Ports EDX1000

```
/EDX1000/Interfaces and Ports/Ethernet Ports

Port Name                Status                Type  Port-Type  SyncE
-----                -
      MGMT                disabled-by-admin    MGMT   10/100BaseT  n/a
1  LAN 1                  up                    LAN    10/100/1000Ba n/a
A  LINE A                 up                    LINE   1000Base-X   n/a

      Edit Port Settings
      Priority Settings
      Global Settings

      Exit

(a): Alarmlog
```

Ethernet Ports EDX1002

```

/EDX1002/Interfaces and Ports/Ethernet Ports

Port Name                Status                Type   Port-Type   SyncE
-----
      MGMT                disabled-by-admin    MGMT   10/100BaseT  n/a
1   LAN 1                 up                   LAN    1000Base-X   n/a
A   LINE A                up                   LINE   1000Base-X   n/a

      Edit Port Settings
      Priority Settings
      Global Settings

      Exit

(a): Alarmlog
    
```

Ethernet Ports EDX1006e

```

/EDX1006/Interfaces and Ports/Ethernet Ports

Port Name                Status                Type   Port-Type   SyncE
-----
      MGMT                down                 MGMT   10/100BaseT  n/a
1   LAN 1                 down                 LAN    100FX         n/a
2   LAN 2                 down                 LAN    100FX         n/a
3   LAN 3                 down                 LAN    100FX         n/a
4   LAN 4                 down                 LAN    100FX         n/a
5   LAN 5                 down                 LAN    100FX         n/a
6   LAN 6                 down                 LAN    100FX         n/a
A   LINE A                down                 LINE   1000Base-X   n/a
B   LINE B                down                 LINE   1000Base-X   n/a

      Edit Port Settings
      Priority Settings
      Global Settings

      Exit

(a): Alarmlog
    
```

Ethernet Ports EDX1008

```

/EDX1008/Interfaces and Ports/Ethernet Ports

Port Name                Status      Type      Port-Type      SyncE
-----
1  MGMT                  down       MGMT      10/100BaseT    n/a
2  LAN 2                 down       LAN       10/100BaseT    n/a
3  LAN 3                 down       LAN       10/100BaseT    n/a
4  LAN 4                 down       LAN       10/100BaseT    n/a
5  LAN 5                 down       LAN       10/100BaseT    n/a
6  LAN 6                 down       LAN       10/100BaseT    n/a
7  LAN 7                 down       LAN       10/100BaseT    n/a
8  LAN 8                 down       LAN       10/100BaseT    n/a
A  LINE A                up         LINE      1000Base-X     n/a
B  LINE B                down       LINE      1000Base-X     n/a

    Edit Port Settings
    Priority Settings
    Global Settings

    Exit
    
```

(a): Alarmlog

Menu Options

Table 5-24 provides information on the menu options.

Table 5-24 Ethernet Ports Menu Options

Parameter	Description	Format	Default
Edit Port Settings	Opens the Edit Port Settings menu for one of the ports. Press Enter and select the port from the list above.	SelectList/Menu	
Priority Settings	Opens the Priority Settings menu.	Menu	
Global Settings	Opens the Global Settings menu.	Menu	
Exit	Leave the menu page.	Exit	

Edit Port Settings

This menu option allows to determine the management port. Select “Edit Port Settings” in the Ethernet Ports menu and press the Enter key. Choose the port to be edited and press the Enter key again. The following screen will be displayed:

```

/EDX1000/Interfaces and Ports/Ethernet Ports/Settings Port: 2

      Port Name                LINE A

Current Status                up

Port Type                    SFP-Port (1000Base-X)

Type                          LINE

      Port Mode                Auto Speed, Auto Duplex

      Ext. Settings

      Admin Status            Enabled

      Exit

(a): Alarmlog
    
```

Table 5-25 provides information on the menu options.

Table 5-25 Edit Port Settings Menu Options

Parameter	Description	Format	Default
Port Name	Enter the name of the selected port.	Display/Input	LAN i, LINE x, or MGMT
Current Status	Indicates the current status of the port (down up disabled).	Display	no default
Port Type	Indicates the type of the port. (Copper-Port 10/100/1000BaseT SFP-Port 1000Base-X).	Display	no default
Type	Defines the port’s usage. A “LAN” port is dedicated for user’s equipment, while a “Line” port is connected to the PSN.	Display	depends on type of device

Table 5-25 Edit Port Settings Menu Options (continued)

Parameter	Description	Format	Default
Port Mode	Configures the data transmission mode for the selected Ethernet port. ⁱ	PullDown-Menu ⁱⁱ <ul style="list-style-type: none"> • Auto Speed, Auto Duplex • ... 	Auto Speed, Auto Duplex
Operation Mode ⁱⁱ	Indicates the type of the SFP	Display	Standard-SFP
Ext. Settings	Opens the menu for extended settings.	Menu	
Admin Status	Enables or disables the port.	PullDown-Menu <ul style="list-style-type: none"> • Enabled • Disabled 	Enabled
Exit	Leave the menu page.	Exit	

i. See Table 4-8 for explanation on the settings.

ii. This option is only visible on an SFP Port.

Port 1 of the EDX1000 is an "Triple-Speed-Port" but no SFP Port. So don't be confused of this miscalculation.

Ext. Settings (SFP Port)

Select "Ext. Settings" in the Edit Port Settings menu (SFP Port) and press the Enter key. The following screen will be displayed:

```

/EDX1000/Interfaces and Ports/Ethernet Ports/Settings Port: 2/Ext. Settings

          SFP Shut Down                               Auto. SFP On/Off
          SFP Status                                     SFP On

          Flow Control                                 Disabled

          Operation Mode                                Standard-SFP

          Exit

                                                    (a): Alarmlog
    
```


Table 5-26 provides information on the Ext. Settings menu options.

Table 5-26 Ext. Settings Menu Options

Parameter	Description	Format	Default
SFP Shut Down	The SFP can be enabled or disabled. when "Auto. SFP On/Off" is selected, the SFP will be shut down for security reason, when no link is detected.	PullDown-Menu <ul style="list-style-type: none">• SFP On• SFP Off• Auto SFP On/Off	Auto. SFP On/Off
SFP Status	Shows the SFP status ' SFP is on' or 'SFP is off'.	Display	SFP On
Flow Control	The status of the Flow Control functionality can be set to 'Enabled' or 'Disabled'. Note: Can only be changed if the selected port is disabled (see "Edit Port Settings" on page 5-41).	PullDown-Menu <ul style="list-style-type: none">• Enable• Disable	Disable
SFP Operating Mode	Configure the SFP operation mode. ⁱ	Display <ul style="list-style-type: none">• Standard-SFP• Triple-Speed-SFP• 100Fx-SFP	Standard-SFP
Exit	Leave the menu page.	Exit	

i. The operation-mode is auto-detect and must not be changed by user.

Ext. Settings (Copper Port)

Select “Ext. Settings” in the Edit Port Settings menu (LAN Port) and press the Enter key. The following screen will be displayed:

```

/EDX1000/Interfaces and Ports/Ethernet Ports/Settings Port: 3/Ext. Settings

Auto Crossover                No Crossover

Flow Control                  Disabled

Exit

(a): Alarmlog

```

Table 5-27 provides information on the Ext. Settings menu options.

Table 5-27 *Ext. Settings Menu Options*

Parameter	Description	Format	Default
Auto Crossover	Shows the Auto Crossover status.	Display	No Crossover
Flow Control	The status of the Flow Control functionality can be set to 'Enabled' or 'Disabled'. Note: Can only be changed if the selected port is disabled (see “Edit Port Settings” on page 5-41).	PullDown-Menu • Enable • Disable	Disable
Exit	Leave the menu page.	Exit	Exit

Priority Settings Menu

Select and enter the Priority Settings menu to configure the priority of data transmission for all Ethernet ports and frames.

```
/EDX1000/Interfaces and Ports/Ethernet Ports/Priority Settings

    Priority Mode                Port based Prio

    Port-Prio-Mapping

    VLAN-Prio-Mapping

    IP Prio Settings

    Exit

(a): Alarmlog
```

Table 5-28 provides information on the menu options.

Table 5-28 Priority Settings Menu Options

Parameter	Description	Format	Default
Priority Mode	<p>Defines the basic information on which the priority assignment is based.</p> <p>The possible option depend very much on the selected VLAN Setup (see “VLAN Setup” on page 5-63).</p> <p>VLAN Setup = Unaware:</p> <p>Port based Prio and IP TOS/DSCP based Prio is selectable.</p> <p>VLAN Setup = Aware:</p> <p>VLAN based Prio and IP TOS/DSCP based Prio is selectable.</p> <p>VLAN Setup = Provider Tagging:</p> <p>Port based Prio, VLAN based and IP TOS/DSCP based Prio is selectable.</p>	<p>PullDown-Menu</p> <ul style="list-style-type: none"> • Port based Prio • VLAN based Prio • IP TOS/DSCP based Prio 	Port based Prio
Port-Prio-Mapping	<p>Open this menu and define the priorities for the different ports. All frames entering the EDX100x at this port, will get the assigned priority. ⁱ</p> <p>Note: This menu is only selectable, when Port based Prio is a valid entry for Priority Mode (see above).</p>	Menu	
VLAN-Prio-Mapping	<p>Open this menu and define the priorities for the different VLAN-prio values. All frames entering the EDX100x, will get the assigned priority. ⁱⁱ</p> <p>Note: This menu is only selectable, when VLAN based Prio is a valid entry for Priority Mode (see above).</p>	Menu	

Table 5-28 Priority Settings Menu Options (continued)

Parameter	Description	Format	Default
IP-Prio Settings	Open this menu and define the priorities for the different TOS/DSCP values. All frames entering the EDX100x, will get the assigned priority. ⁱⁱⁱ Note: This menu is only selectable, when IP TOS/DSCP based Prio is a valid entry for Priority Mode (see above).	Menu	
Exit	Leave the menu page.	Exit	

- i. The settings here are only relevant in "Port based Prio" priority mode.
- ii. The settings here are only relevant in "VLAN based Prio" priority mode.
- iii. The settings here are only relevant in "IP TOS/DSCP based Prio" priority mode.

Port-Prio-Mapping

Select and enter the Port-Prio-Mapping menu to configure the priority of the device's port. The settings here are only relevant in "Port based Prio" priority mode.

```

/EDX1008/Interfaces and Ports/Ethernet Ports/Priority
Settings/Port-Prio-Mapping

Port Name                Status      Type      Prio
-----
1 LAN 1                  down       LAN       High Prio
2 LAN 2                  down       LAN       High Prio
3 LAN 3                  down       LAN       High Prio
4 LAN 4                  down       LAN       High Prio
5 LAN 5                  down       LAN       High Prio
6 LAN 6                  down       LAN       High Prio
7 LAN 7                  down       LAN       High Prio
8 LAN 8                  down       LAN       High Prio
A LINE A                 down       LINE      High Prio
B LINE B                 down       LINE      High Prio

      Edit Port Priority

      Exit

(a): Alarmlog
    
```

On top of the menu, you see a list of all (equipped) ports and the assigned port-based priority.

NOTE: Depending on the EDX100x Hardware version you may have less or other ports but the usage is similar. The figure above shows an EDX1008 menu.

Table 5-29 provides information on the menu options.

Table 5-29 *Port-Prio-Mapping Menu Options*

Parameter	Description	Format	Default
Edit Port Priority	Press Enter and select a port from the list above to change the assigned port-based priority.	SelectList/Menu	
Exit	Leave the menu page.	Exit	

VLAN-Prio-Mapping

Select and enter the VLAN-Prio-Mapping menu to configure the priority assignment for VLAN-prio fields. The settings here are only relevant in “VLAN based Prio” priority mode.

```

/EDX1000/Interfaces and Ports/Ethernet Ports/Priority
Settings/VLAN-Prio-Mapping

      VLAN-Prio 0x07          Extra High Prio
      VLAN-Prio 0x06          High Prio
      VLAN-Prio 0x05          High Prio
      VLAN-Prio 0x04          High Prio
      VLAN-Prio 0x03          Low Prio
      VLAN-Prio 0x02          Low Prio
      VLAN-Prio 0x01          Low Prio
      VLAN-Prio 0x00          Low Prio

      Exit

(a): Alarmlog

```

Table 5-30 provides information on the menu options.

Table 5-30 VLAN-Prio-Mapping Menu Options

Parameter	Description	Format	Default
VLAN-Prio 0x07	Define the priority for the mentioned VLAN-Prio value.	PullDown-Menu <ul style="list-style-type: none">• Extra High Prio• High Prio• Low Prio• Extra Low Prio	Extra High Prio
VLAN-Prio 0x06-0x04	Define the priority for the mentioned VLAN-Prio value.	PullDown-Menu <ul style="list-style-type: none">• Extra High Prio• High Prio• Low Prio• Extra Low Prio	High Prio
VLAN-Prio 0x03-0x00	Define the priority for the mentioned VLAN-Prio value.	PullDown-Menu <ul style="list-style-type: none">• Extra High Prio• High Prio• Low Prio• Extra Low Prio	Low Prio
Exit	Leave the menu page.	Exit	

IP-Prio-Settings

Select and enter the IP-Prio-Settings menu to configure the priority assignment for IPv4-TOS field. The settings here are only relevant in “IP TOS/DSCP based Prio” priority mode.

```

/EDX1000/Interfaces and Ports/Ethernet Ports/Priority Settings/IP Prio Settings

    Define DSCP Bit Mask for High Priority Frames:

    DSCP Bit0                '0'
    DSCP Bit1                '0'
    DSCP Bit2                '1'
    DSCP Bit3 (Delay)        '1'
    DSCP Bit4 (Throughput)   '0'
    DSCP Bit5 (Reliability)  '1'

    High Prio DSCP Word (0:5) 001101

    Exit

(a): Alarmlog

```

Table 5-31 provides information on the menu options.

Table 5-31 *IP-Prio-Settings Menu Options*

Parameter	Description	Format	Default
DSCP Bit x	Press Enter and select the bit mask for the bit and define the high prio DSCP word.	PullDown-Menu <ul style="list-style-type: none"> • '0' • '1' • 'x' 	001101
High Prio DSCP Word (0:5)	Result of the above done settings.	Display	001101
Exit	Leave the menu page.	Exit	

Global Settings

Select "Global Settings" in the Ethernet Ports menu and press the Enter key. The following screen will be displayed:

```
/EDX1000/Interfaces & Ports/Ethernet Ports/Global Settings

      MTU Size                               1632

Exit

(a): Alarmlog
```

In this menu the MTU Size of the device can be defined. Possible entries are '1518 (1522)' or '1632'.

SFP Ports

Select “SFP Ports” in the Interfaces and Ports menu and press the Enter. The following screen will be displayed:

```
EDX1006/Interfaces and Ports/SFP Ports

Port Name          Status  Vendor          Serial          Mech.
0  MGMT             down    N/A             N/A             RJ-45
1  LAN 1            down
2  LAN 2            down
3  LAN 3            down
4  LAN 4            down
5  LAN 5            down
6  LAN 6            down
A  LINE A           down
B  LINE B           down

          Display SFP Data

          Exit

(a): Alarmlog
```

NOTE: Depending on the EDX100x Hardware version you may have less or other ports but the usage is similar. The figure above shows an EDX1006 menu.

This menu provides information on the EDX100x SFP-ports. If you want to get further details about the plugged SFP ports, select “Display SFP Data” and choose an SFP port. Pressing the Enter key leads to the following table which provides information on the plugged SFP:

```

/EDX1000/Interfaces and Ports/SFP Ports/SFP Port: 9

      Base Area Checksum           ok
      Ext Area Checksum           ok
      Vendor Name                  Methode Elec.
      Part Number                  DM7041
      Vendor-Rev                   D
      Serial No                    0000000000025731
      Date Code                    08/02/2005
      Transceiver Type             SFP
      Connector Type               Unspecified
      Optical Type                 1000BASE-T
      Line Coding                   8B10B
      Nominal Bit Rate             1300 Mbits/sec
      Link Length                  Not Specified
      Max Margin                   Not Specified
      Min Margin                   Not Specified
      Wave Length                  16652 nm

      Update SFP Info             SFP Diagnostics

      Exit

                                          (a): Alarmlog
    
```

Select "Update SFP Info" and confirm by pressing "y", if you want to update the SFP port information.

NOTE: All displayed values depending on the SFP. arcutronix cannot ensure the correctness of this values.

SFP Diagnostics

This menu provides actual information about the plugged SFP in the selected port.

```
/EDX1000/Interfaces and Ports/SFP Ports/SFP Port: 9/SFP Diagnostics
                                     Press `U` to update counters
SFP Temperature                       33.382 °C
SFP Supply Voltage                     3.2646 V
SFP Tx Bias Current                    020 mA
SFP Tx Power                           -18.816 dBm
SFP Rx Power                            -33.979 dBm

Exit                                     All Values depend on the SFP
                                         (a): Alarmlog
```

NOTE: All displayed values depending on the SFP. arcutronix cannot ensure the correctness of this values.

UART Configuration Menu

This menu will display the settings for the serial RS-232 interface.

```

/EDX1000/Interfaces & Ports/UART Configuration

    Baud Rate                57600

    Data Bits                 8

    Parity                   No Parity

    Stop Bits Length         1

    Commit Changes

Exit

(a): Alarmlog
    
```

Table 5-32 provides information on the menu options.

Table 5-32 UART Configuration Menu Options

Parameter	Description	Format	Default
Baud Rate	Defines the baud rate.	PullDown-Menu <ul style="list-style-type: none"> • 2400 • 9600 • 19200 • 38400 • 57600 • 115200 	38400 (kpbs)
Data Bits	Defines the data bits.	PullDown-Menu <ul style="list-style-type: none"> • 7 • 8 	8
Parity	Defines the usage of parity bits.	PullDown-Menu <ul style="list-style-type: none"> • No Parity • Even Parity • Odd Parity 	No Parity

Table 5-32 UART Configuration Menu Options (continued)

Parameter	Description	Format	Default
Stop Bit Length	Defines the number of stop bits.	PullDown-Menu • 1 • 2	1
Commit Changes	Press Enter to confirm all changes.	Action/Confirm	
Exit	Leave the menu page.	Exit	

NOTE: Do all the changes required and select at last the “Commit Changes” entry. You will loose contact to the board unless your PC is configured the new settings, as well.

Operation Modes Menu

This menu will display the “Operation Modes” menu.

```

/EDX1000/Operation Modes

    Ring Operation Mode           Enabled

    Ring Settings

    LPT/RFD operation mode       Enabled

    LPT/RFD Settings

Exit

(a): Alarmlog
    
```

Table 5-33 provides information on the menu options.

Table 5-33 Operation Modes Menu Options

Parameter	Description	Format	Default
Ring Operation Mode	Select Ring Operation Mode. Note: Not available on variants where only one LINE port is available.	PullDown-Menu <ul style="list-style-type: none">• Disabled• Ring Protection	Disabled
Ring Settings	Open this menu and configure the Ring settings. Note: Only visible, when “Ring Protection Mode” is enabled.	Menu	
LPT/RFD Operation Mode	Select LPT/RFD operation mode.	PullDown-Menu <ul style="list-style-type: none">• Disabled• LPT/RFD	Disabled
LPT/RFD Settings	Open this menu and configure the LPT/RFD settings. Note: Only visible, when “LPT/RFD Operation Mode” is enabled.	Menu	
Exit	Leave the menu page.	Exit	

Ring Settings

This menu will display the “Ring mode settings”, if Ring mode is activated.

```

/EDX1000/Operation Modes/Ring settings

      Node Type                               Transit

      Control VLAN ID                         4092

      RFC3619 Compliance                      Failsafe

      FailsafeRingUp Frame ID                16

      HealthEast Frame ID                    17

      Exit

                                          (a): Alarmlog
  
```

NOTE: Ring Settings menu is not visible on “EDX1000” and “EDX1002” because it is not supported!

Table 5-34 provides information on the menu options.

Table 5-34 Ring settings Menu Options

Parameter	Description	Format	Default
Node Type	Defines if the Node is “Transit” or “Master”	PullDown-Menu <ul style="list-style-type: none"> • Transit • Master 	Transit
Control VLAN ID	Defines the VLAN ID for [IETF RFC 3619] Control Frames	Input (1..4094)	4092
RFC3619 Compliance	Choose “Failsafe” or “Strict”	PullDown-Menu <ul style="list-style-type: none"> • Failsafe • Strict 	Failsafe
FailsafeRingUP ⁱ frame ID	Frame ID for FailsafeRingUp frames	Input (9..255)	16

Table 5-34 Ring settings Menu Options (continued)

Parameter	Description	Format	Default
HealthEastframe ID ⁱⁱ	Frame ID for HealthEast frames	Input (9..255)	17
Exit	Leave the menu page.	Exit	

- i. Only visible if "Failsafe" is chosen.
- ii. Only visible if "Failsafe" is chosen.

LPT/RFD Settings

The menu "LPT/RFD Settings" is only visible, when LPT/RFD is activated.

```

/EDX1006/Operation Modes/LPT/RFD Settings

      RFD Operation Mode                IP
      RFD-Peer IP Address             192.168.1.100
      Status                             contact to RFD peer
      Configuration Mode             explicit

Port Name          Type Status          Local ports      Remote ports
-----
      MGMT          MGMT up
1  LAN 1          LAN up
2  LAN 2          LAN up
3  LAN 3          LAN down
4  LAN 4          LAN down
5  LAN 5          LAN down
6  LAN 6          LAN down
A  LINE A        LINE up          1,2,3,4,5,6
B  LINE B        LINE down

      Edit Port Settings

      Exit

(a): Alarmlog
    
```

NOTE: Depending on the EDX100x Hardware version you may have less or other ports but the usage is similar. This figure shows an EDX1006 menu.

Table 5-35 provides information on the menu options.

Table 5-35 LPT/RFD Settings Menu Options

Parameter	Description	Format	Default
RFD Operation Mode	Configure here the operation mode of the RFD feature. RFD is the forwarding of LAN-status information between local and remote site of a pair of EDX. The communication can be IPv4-based or - in a pure point2point-application - link-local based (slow protocol). If RFD is not used, it can be disabled.	PullDown-Menu <ul style="list-style-type: none"> • IP • Link-Local • Disable RFD 	IP
RFD-Peer IP Address	IP address of the remote device (peering device). Note: This entry is not visible, when the RFD operation mode is "Link-Local".	Input	no default
Status	The "Status" entry of the menu does indicate the LPT/RFD finite state-machine. The possible values and their denotations are given in "LPT/RFD Status" on page 4-26.	Display	No contact to peer
Configuration Mode	Configure LPT/RFD "explicit" or "implicit". Implicit means, the configuration of the remote site is copied to this device.	PullDown-Menu <ul style="list-style-type: none"> • explicit • implicit 	explicit
LPT/RFD overview table	This table gives an overview to all the LPT/RFD settings per port. Select "Edit Port Settings" to get access to the port settings.	Display	-
Edit Port Settings ⁱ	Opens the Edit Port Settings menu for one of the ports. Press Enter and select the port from the list above.	SelectList/Menu	
Exit	Leave the menu page.	Exit	

i. Only visible if "explicit" configuration mode is chosen.

The LPT/RFD overview table is a summary for the LPT/RFD setting. For “LAN”-ports, one can choose, which remote shall be torn down, when this special port is detected a down.

For “LINE”-ports, one can define, which local ports must be tore down, when the LINE-port is down.

“MGMT”-ports can not be edited or configured. LPT/RFD is not valid for MGMT-ports!

In the menu above, the following settings are down for an EDX1006:

- If LAN1 fails, on the remote side, port 1 will be disabled, too.
- If LAN2 fails, on the remote side, port 2 will be disabled, too.
- Same for LAN3...LAN6
- If LINE A fails, the local ports 1-6 will be tore down.
- If LINE B fails, nothing will happen.

The status of the LAN ports are indicated in the status field of the table. It can carry the following information:

Table 5-36 LAN Port-States due to LPT/RFD

Status	Description
Port down	The port has no link detected. This is not due to LPT/RFD!
Port up	The port has detected link and is working fine.
Port disabled	The port is disabled by admin.
Stopping LPT/RFD	The port was disabled by LPT or RFD and will come up again, now. At this moment it is not clear yet, whether the port will enter the “Port up” or “Port down” state.
Disabled by LPT	LPT has disabled the port, due to a Line failure. Note: Note: This state is called in the port-overview as “Disabled by LPT/RFD”.
Disabled by RFD	RFD has disabled the port, due to a remote port’s failure. Note: Note: This state is called in the port-overview as “Disabled by LPT/RFD”.
Disabled, no RFD peer	RFD has disabled the port, due to a missing link to the peer. Note: Note: This state is called in the port-overview as “Disabled by LPT/RFD”.

Edit Port Settings

The menu “Edit Port Settings” is to configure the relationship of ports and peers.

For LAN-ports, one can define which remote ports (on the peer device) shall be disabled, when this LAN-port detects No-Link (port is down). This is called the RFD-feature.

For LINE-ports, one can define which local ports (on this local device) shall be disabled, when this LINE-port detects No-Link (port is down). This is called the LPT-feature.

```

/EDX1006/Operation Modes/LPT/RFD Settings/Port Settings

      Port No. (Front Panel)      A

      Port Name                   LINE A

      Type                       LINE

      Current Status             Port down

      Remote Ports (RFD)        1
      Local Ports (LPT)        1

      Exit

(a): Alarmlog
    
```

Table 5-37 provides information on the menu options.

Table 5-37 LPT/RFD Edit Port Settings Menu Options

Parameter	Description	Format	Default
Port No. (Front Panel)	This is the (selected) port's label on the front plate. Makes is clearly identifiable.	Display	
Port Name	The given name of this port.	Display	
Type	The port's operation type. It can be either LAN or LINE. For LINE ports, only LPT settings are possible. For LAN-ports, only RFD settings are possible.	Display	
Current Status	Displays the ports operation status.	Display	

Table 5-37 LPT/RFD Edit Port Settings Menu Options (continued)

Parameter	Description	Format	Default
Remote Ports (RFD)	This is a list of all ports on the remote (peer) device, which will be disabled, in case this LAN-port is down. Only visible for LAN ports!	List Separate the entries by comma. E.g. 2,4	empty
Local Ports (LPT)	This is a list of all ports on the local device, which will be disabled, in case this LINE-port is down. Only visible for LINE ports!	List Separate the entries by comma. E.g. 1,3	empty
Exit	Leave the menu page.	Exit	

VLAN Setup

This menu allows you to configure the EDX100x's VLAN settings.

```
/EDX1000/VLAN Setup

      Global VLAN Policy           Aware

      Default VLAN ID              1
      Default VLAN Prio            0

      VLAN Table Settings          Port View
                                   VLAN View

      Exit

(a): Alarmlog
```

Table 5-38 provides information on the menu options.

Table 5-38 VLAN Setup Menu Options

Parameter	Description	Format	Default
Global VLAN Policy	The type of VLAN Policy can be set. Possible values are 'Off', 'Aware' and 'Provider Tagging'.	PullDown-Menu <ul style="list-style-type: none"> Aware Unaware Provider Tagging 	Aware
Default VLAN ID ⁱ	The default VLAN ID for incoming packets	Input (1..4094)	1
Default VLAN Prio ⁱ	The default VLAN Prio for incoming packets	Input (0..7)	0
VLAN Table Settings ⁱ	Selecting this option leads to the VLAN Table Settings menu.	PullDown-Menu <ul style="list-style-type: none"> Port View VLAN View 	no default
Exit	Leave the menu page.	Exit	

i. This line will only be displayed, if the Global VLAN Policy is set to 'Aware'.

VLAN Table Settings (Port View)

Select "VLAN Table Settings Port View" in the VLAN Settings menu and press the Enter key. The following screen will be displayed:

```

/EDX1000/VLAN Setup/VLAN Settings: Port View

Port  Name      Egress      Untagged      VLAN IDs
-----
1     LAN 1        Standard    Discard
2     LAN 2        Standard    Discard
3     LAN 3        Standard    Discard
4     LAN 4        Standard    Discard
5     LAN 5        Standard    Discard
6     LAN 6        Standard    Discard
7     LAN 7        Standard    Discard
8     LAN 8        Standard    Discard

      Edit Port VLAN Settings

Set all LAN ports to - discard untagged packets
                    - use global default ID for untagged packets
                    - egress untagged packets
                    - egress standard

      Exit

```

(a): Alarmlog

NOTE: Depending on the EDX100x Hardware version you may have less or other ports but the usage is similar. This figure shows an EDX1008 menu.

This menu lists all VLAN Port Settings. In order to change the port settings select “Edit Port VLAN Settings” and press the Enter key. Then, choose the port to be changed and press the Enter key again. The settings of the chosen port will be displayed.

```

/EDX1000/VLAN Setup/VLAN Settings: Port View/Settings Port: 1

    Associated VLAN IDs

    Untagged frames                Discard Packet

    Egress force mode              Unchanged

    Exit

(a): Alarmlog
    
```

Table 5-39 provides information on the Edit Port VLAN Settings menu options.

Table 5-39 Edit Port VLAN Settings Menu Options

Parameter	Description	Format	Default
Associated VLAN ID's	The VLAN ID's supported by this port can be configured. Possible entries are '1' ... '4094', divided by commas.	Input (1..4094)	no default
Untagged frames	The handling of untagged frames can be configured.	PullDown-Menu <ul style="list-style-type: none"> • Discard Packet • Add global default VLAN ID • Add port VLAN ID 	Discard Packet
Egress force mode	The egress force mode can be configured.	PullDown-Menu <ul style="list-style-type: none"> • Unchanged • Force Untagged Egress • Untag Packets with def. VLAN ID 	Unchanged
Exit	Leave the menu page.	Exit	

VLAN Table Settings (VLAN View)

Select “VLAN Table Settings VLAN View” in the VLAN Settings menu and press the Enter key. The following screen will be displayed.

```
/EDX1000/VLAN Setup/VLAN Settings: VLAN View

      VLAN ID          Port list

      1                1
      4092
      4094 (Mgmt)

Edit VLAN ID      Delete VLAN ID      Add VLAN ID      Delete All VLAN IDs

Exit

(a): Alarmlog
```

NOTE: VLAN Table Settings (VLAN View) menu is not visible on “EDX1000” and “EDX1002” because it is not supported!

Table 5-40 provides information on the VLAN View Settings menu options.

Table 5-40 VLAN View Settings Menu Options

Parameter	Description	Format	Default
Edit VLAN ID	Edit selected VLAN ID	Menu	
Delete VLAN ID	Delete selected VLAN ID	SelectList/confirm	
Add VLAN ID	Add a VLAN ID	SelectList/confirm	
Delete all VLAN IDs	Delete all VLAN IDs	Select/confirm	
Exit	Leave the menu page.	Exit	

Edit VLAN ID

Select “Edit VLAN ID” in the “VLAN View” menu and press Enter key to highlight VLAN ID list. Choose the VLAN ID which is to be changed and press the Enter key. The following screen will be displayed:

```
/EDX1000/VLAN Setup/VLAN Settings: VLAN View/VLAN 0

      VLAN ID                1

      Port List             1

                                Exit

(a): Alarmlog
```

Table 5-40 provides information on the VLAN View Settings menu options.

Table 5-41 VLAN View Settings Menu Options

Parameter	Description	Format	Default
VLAN ID	Shows the selected VLAN ID	display	no default
Port List	Sign in List of Ports comma separated	Input (1,2)	no default
Exit	Leave the menu page.	Exit	

Bandwidth Limitation Settings

Select "Bandwidth Limitation Settings" in the Main menu and press the Enter key. The following screen will be displayed:

```
/EDX1000/Bandwidth Limitation Settings

Port Name          Eg-Limit   Lo-Limit   Status   Type   Port-Type
1   LAN 1          None       None      down    LAN   10/100BaseT
2   LAN 2          None       None      down    LAN   10/100BaseT
3   LAN 3          None       None      down    LAN   10/100BaseT
4   LAN 4          None       None      down    LAN   10/100BaseT
5   LAN 5          None       None      down    LAN   10/100BaseT
6   LAN 6          None       None      down    LAN   10/100BaseT
7   LAN 7          None       None      down    LAN   10/100BaseT
8   LAN 8          None       None      down    LAN   10/100BaseT
A   LINE A         None       None      down    LINE  1000Base-X
B   LINE B         None       None      down    LINE  1000Base-X

          Edit Port Settings

          Exit

(a): Alarmlog
```

NOTE: Depending on the EDX100x Hardware version you may have less or other ports but the usage is similar. This figure shows an EDX1008 menu.

In order to edit the bandwidth limitation settings select “Edit Port Settings” and press the Enter key. Then, choose the port to be changed and press the Enter key again.

```
/EDX1000/Bandwidth Limitation Settings/Settings Port: 1

    Ingress Bandwidth Limitation

    Egress Bandwidth Limitation

Exit

(a): Alarmlog
```

Select “Ingress Bandwidth Limitation” to limit incoming or “Egress Bandwidth Limitation” to limit outgoing packets and press the Enter key to access the Bandwidth Limitation menu of the desired port.

Ingress Bandwidth Limitation

If you selected the “Ingress Bandwidth Limitation” the following screen will be displayed:

```
.../Bandwidth Limitation Settings/Settings Port: 1/Ingress Bandwidth Limitation

    Limit Mode                Limit all types of frames

    Limit Extra Low Prio Frames  250 Mbps

    Limit Low Prio Frames       Same rate as Extra Low Prio

    Limit High Prio Frames      Same rate as Low Prio

    Limit Extra High Prio Frames Same rate as High Prio

Exit

(a): Alarmlog
```

Table 5-42 provides information on the Bandwidth Limitation menu options.

Table 5-42 *Ingress Bandwidth Limitation Menu Options*

Parameter	Description	Format	Default
Limit Mode	The general limitation mode can be configured.	PullDown-Menu <ul style="list-style-type: none"> • Limit all types of frames • Limit BC and MC Frames • Limit BC Frames • No Limitation 	No Limitation
Limit Extra Low Prio Frames	The limitation mode for Extra Low Prio Frames can be configured. Note: The huge number of possible entries is hard to show in the gCLI. please scroll up and/or down to get access to all entries!	PullDown-Menu <ul style="list-style-type: none"> • Unlimited • 128kbps • 256kbps • 512kbps • 1Mbps • 2Mbps • 3Mbps • 4Mbps • 5Mbps • 6Mbps • 7Mbps • 8Mbps • 9Mbps • 10Mbps • 16Mbps • 20Mbps • 30Mbps • 40Mbps • 50Mbps • 60Mbps • 80Mbps • 125Mbps • 250Mbpsⁱ 	250Mbps
Limit Low Prio	The limitation mode for Low Prio Frames can be configured. Possible values are.	PullDown-Menu <ul style="list-style-type: none"> • Same rate as Extra Low Prio • Twice the rate as Extra Low Prio 	Same rate as Extra Low Prio

Table 5-42 Ingress Bandwidth Limitation Menu Options (continued)

Parameter	Description	Format	Default
Limit High Prio	The limitation mode for High Prio Frames can be configured. Possible values are 'Same rate as Low Prio' or 'Twice the rate as Extra Low Prio'.	PullDown-Menu <ul style="list-style-type: none"> • Same rate as Extra Low Prio • Twice the rate as Extra Low Prio 	Same rate as Low Prio
Limit Extra High Prio	The limitation mode for Extra High Prio Frames can be configured. Possible value are 'Same rate as High Prio' or 'Twice the rate as Extra Low Prio'.	PullDown-Menu <ul style="list-style-type: none"> • Same rate as Extra Low Prio • Twice the rate as Extra Low Prio 	Same rate as High Prio
Exit	Leave the menu page.	Exit	

i. 125 Mbps and 250 Mbps are not selectable on an 100Mbit Port.

Egress Bandwidth Limitation

If you selected the “Egress Bandwidth Limitation” the following screen will be displayed:

```

...1/Bandwidth Limitation Settings/Settings Port: 1/Egress Bandwidth Limitation

      Limit Egress Bandwidth           Unlimited

Exit

(a): Alarmlog
  
```

Table 5-43 provides information on the Egress Bandwidth Limitation menu options.

Table 5-43 Egress Bandwidth Limitation Menu Options

Parameter	Description	Format	Default
Limit Egress Bandwidth	The limitation Bandwidth for incoming Frames can be configured.	PullDown-Menu <ul style="list-style-type: none">• Unlimited• 128kbps• 256kbps• 512kbps• 1Mbps• 2Mbps• 3Mbps• 4Mbps• 5Mbps• 6Mbps• 7Mbps• 8Mbps• 9Mbps• 10Mbps• 16Mbps• 20Mbps• 30Mbps• 40Mbps• 50Mbps• 60Mbps• 80Mbps• 125Mbps• 250Mbpsⁱ	Unlimited
Exit	Leave the menu page.	Exit	

i. 80Mbps, 125 Mbps and 250 Mbps are not selectable on an 100Mbit Port.

Rapid Spanning Tree Settings Menu

This menu allows the user to display and to configure the settings for the Rapid Spanning Tree Protocol (RSTP). If no Spanning Tree shall be supported, the protocol can be disabled.

```
/EDX1000/RSTP Settings

      RSTP Mode                RSTP Enabled

      Global Settings

      Port Settings

      Exit

(a): Alarmlog
```

NOTE: Rapid Spanning Tree Settings menu is not visible on “EDX1000” and “EDX1002” because it is not supported!

Table 5-44 provides information on the menu options.

Table 5-44 Rapid Spanning Tree Settings Menu Options

Parameter	Description	Format	Default
RSTP Mode	Select or disable the Rapid Spanning Tree protocol.	PullDown-Menu <ul style="list-style-type: none">RSTP DisabledRSTP Enabled	RSTP Disabled
Global Settings	Global settings for RSTP can be assigned.	Menu	
Port Settings	Opens the RSTP Port Settings menu. Individual settings for each port can be assigned.	Menu	
Exit	Leave the menu page.	Exit	

NOTE: If RSTP is enabled, all LINE-ports are doing RSTP. LAN and/or the management port are not.

RSTP Global Settings

Rapid Spanning Tree Protocol (RSTP) requires some global settings, valid for a switching device.

```

/EDX1000/RSTP Settings/RSTP Global Settings

    Priority                               32768

    Ageing Time [s]                        20

    Interval [s]                           2

    Forward Delay [s]                      15

    Set RSTP Global Defaults

Aging Time must be greater or equal than: 2x(Interval+1)
                                         and
Aging Time must be less or equal than:   2x(Forward Delay-1)

Exit

(a): Alarmlog
    
```

Table 5-45 provides information on the menu options.

Table 5-45 RSTP Global Settings Menu Options

Parameter	Description	Format	Default
Priority	Enter the RSTP bridge priority in steps of 4096 (0-61440).	Display/Input	32768
Ageing Time [s]	Enter the SRTP bridge aging time (6...40).	Display/Input	20
Interval [s]	Enter the RSTP bridge Hello interval (1...10).	Display/Input	2
Forward Delay [s]	Enter the RSTP bridge forward delay (4...30).	Display/Input	15
Set RSTP Global Defaults	Press Enter to (re)set the global RSTP settings to defaults.	Action/Confirm	
Exit	Leave the menu page.	Exit	

NOTE: RSTP does have some dependencies for “Aging Time” (AT), “Hello Interval” (HI) and “Forward Delay” (FD):

- AT >= 2 * (HI + 1)
- AT <= 2 * (FD - 1)

RSTP Port Settings

On top of the menu an overview for all the equipped Ethernet ports and their actual RSTP settings is listed.

```

/EDX1000/RSTP Settings/RSTP Port Settings

P# Name      Status  Type  Cost      Prio State   Role      Desig. Bridge
1 LAN 1 down    disabled 100 200000 128 no RSTP 00:00:00:00:00:00
2 LAN 2 down    disabled 100 200000 128 no RSTP 00:00:00:00:00:00
3 LAN 3 down    disabled 100 200000 128 no RSTP 00:00:00:00:00:00
4 LAN 4 down    disabled 100 200000 128 no RSTP 00:00:00:00:00:00
5 LAN 5 down    disabled 100 200000 128 no RSTP 00:00:00:00:00:00
6 LAN 6 down    disabled 100 200000 128 no RSTP 00:00:00:00:00:00
7 LAN 7 down    disabled 100 200000 128 no RSTP 00:00:00:00:00:00
8 LAN 8 down    disabled 100 200000 128 no RSTP 00:00:00:00:00:00
A LINE A down  enabled 1000 200000 128 listening 00:20:F5:00:17:21
B LINE B down  enabled 1000 200000 128 listening 00:20:F5:00:17:21

      Edit RSTP Port Settings

      This Device                               00:20:F5:00:17:21

      Exit

(a): Alarmlog

```

NOTE: Depending on the EDX100x Hardware version you may have less or other ports but the usage is similar. This figure shows an EDX1008 menu.

Table 5-46 provides information on the menu options.

Table 5-46 Rapid Spanning Tree Port Settings Menu Options

Parameter	Description	Format	Default
Edit RSTP Port Settings	Opens the Edit RSTP Port Settings menu for one of the ports. Press Enter and select the port from the list above. ⁱ	SelectList/Menu	
This Device	Displays the MAC address of this device.	Display	no default
Exit	Leave the menu page.	Exit	

i. Only 'Line' ports are selectable in the list.

Edit RSTP Port Settings Menu

Select and enter the Edit RSTP Port Settings menu, and choose a port from the port list to edit one's parameters.

Note: Only ports, configured as 'LINE' are selectable.

```

/EDX1000/RSTP Settings/RSTP Port Settings/RSTP Settings Port: 2

    Port Priority                128

    Port Path Cost              0

    Port RSTP State            disabled

    Port Link Type             Edge

    Set RSTP Port Defaults

Exit

(a): Alarmlog
    
```

Table 5-47 provides information on the menu options.

Table 5-47 Edit RSTP Port Settings Menu Options

Parameter	Description	Format	Default
Port Priority	Enter the port's RSTP priority in steps of 16 (0...240).	Display/Input	128
Port Path Cost	Enter the port's RSTP path cost (0...200000000), 0 = auto.	Display/Input	0
Port RSTP State	Set current port state.	PullDown-Menu • Enabled • Disabled	Enabled

Table 5-47 Edit RSTP Port Settings Menu Options (continued)

Parameter	Description	Format	Default
Port Link Type	Select current port link type	PullDown-Menu <ul style="list-style-type: none">• None• Edge• P2P• Auto	Edge
Set RSTP Port Defaults	Press Enter to (re)set the port's RSTP settings to defaults.	Action/Confirm	
Exit	Leave the menu page.	Exit	

Performance Monitoring

Select "Performance Monitoring" in the Main menu and press the Enter key. The following screen will be displayed:

```
/EDX1000/Performance Monitoring

      Ethernet Performance Data

Exit

(a): Alarmlog
```

Ethernet Performance Data

This menu displays the values/results for the Ethernet performance data. In the top of the menu a list with all available ethernet ports is shown. A rough overview about

received and sent packets (“simple counters”) is presented together with the actual status of the port.

```

/EDX1008/Performance Monitoring/Ethernet
                                         Press `U` to update counters

      Port   Name           Rx-Packets   Tx-Packets   Status
      ---   ---           -
      1     LAN 1           0            0            down
      2     LAN 2           0            0            down
      3     LAN 3           0            0            down
      4     LAN 4           0            0            down
      5     LAN 5           0            0            down
      6     LAN 6           0            0            down
      7     LAN 7           0            0            down
      8     LAN 8           0            0            down
      A     LINE A          0            0            down
      B     LINE B          0            0            down

      Read detailed Ethernet Counter
      Clr all detailed counter
      Set Histogram Options

      Exit
  
```

(a): Alarmlog

NOTE: Depending on the EDX100x Hardware version you may have less or other ports but the usage is similar. This figure shows an EDX1008 menu.

Table 5-48 provides information on the menu options.

Table 5-48 Ethernet Performance Data Menu Options

Parameter	Description	Format	Default
Read detailed Ethernet Counter ⁱ	Press Enter and select one of the ports in the list above to see the detailed counters.	Menu	
Clr all detailed counter ⁱ	Enables to reset all detailed counters to zero. Confirm 'Do you really want to clr all counter values (Y/N)' with 'Y' to reset all detailed counters.	Action/Confirm	
Set Histogram Options	Opens the Histogram Options Menu	Menu	
Exit	Leave menu page.	Exit	

i. The “detailed counters” are the counters, visible in the sub menus. This helps to synchronize the counters for all ethernet ports.

Read detailed Ethernet Counter

Select and enter the Read detailed Ethernet Counter menu, and choose a row from the list to read one's performance values.

```

/EDX1000/Performance Monitoring/Ethernet/Counter Port: 2

    In Counters

    In Problem Packets

    Out Counters

    Histogram Counter

    Out Problem Packets

    Clr Detailed Counters

    Exit
    
```

(a): Alarmlog

Table 5-49 provides information on the menu options.

Table 5-49 Read Detailed Ethernet Counter Menu Options

Parameter	Description	Format	Default
In Counters	Opens the In Counters menu.	Menu	
In Problem Packets	Opens the In Problem Packets menu.	Menu	
Out Counters	Opens the Out Counters menu.	Menu	
Histogram Counter	Opens the Histogram Counter menu.	Menu	
Out Problem Packets	Opens the Out Problem Packets menu.	Menu	
Clr Detailed Counters	Enables to reset all detailed counters to zero. Confirm 'Do you really want to clr all counter values (Y/N)' with 'Y' to reset all detailed counters.	Action/Confirm	
Exit	Leave menu page.	Exit	

In Counters Menu

All counters valid for incoming data are shown. Press 'u' to update the menu.

```

/EDX1000/Performance Monitoring/Ethernet/Counter Port: 2/In Counters
                                     Press `U` to update counters

      inUnicasts                       0
      inMulticast                       0
      inBroadcast                       0

      inPause                           0

      inFCSError                        0
      inAlignError                      0

      inGoodOctets                      0
      inBadOctets                       0

      inDiscards                        0
      inFiltered                        0

      Exit

(a): Alarmlog
    
```

Table 5-50 provides information on the menu options.

Table 5-50 *In Counters Menu Options*

Parameter	Description	Format	Default
inUnicasts	Total valid ⁱ frames received with an unicast destination address.	Display	no default
inMulticast	Total valid frames received with a multicast destination address that are not counted in 'inBroadcast' or 'inPause'.	Display	no default
inBroadcast	Total valid frames received with a destination address equal to FF:FF:FF:FF:FF:FF.	Display	no default
inPause	Total valid pause frames received.	Display	no default
inFCSError	Total frames received with a valid length that have an invalid FCS and an integral number of octets.	Display	no default

Table 5-50 In Counters Menu Options (continued)

Parameter	Description	Format	Default
inAlignError	Total frames received with a valid length that have an invalid FCS and a non-integral number of octets.	Display	no default
inGoodOctets	Total data octets received in frames with a valid FCS. Undersize or oversize frames are included. The count includes the FCS but not the preamble.	Display	no default
inBadOctets	Total data octets received in frames with an invalid FCS. Fragments and Jabbers are included. The count includes the FCS but not the preamble.	Display	no default
inDiscards	Total valid frames received that are discarded due to a lack of buffer space. This includes frames discarded at ingress as well as those dropped due to priority and congestion considerations at the output queues. Frames dropped at egress due to excessive collisions are not included but are counted in the 'outExcessive' counter.	Display	no default
inFiltered	Total valid frames received that are not forwarded to a destination port. These are frames which are not forwarded due to the port state. Valid frames discarded due to a lack of buffer space are not included.	Display	no default
Exit	Leave menu page.	Exit	

i. A valid frame is one with a good FCS and whose size is 64 octets to MTUSize octets inclusive.

In Problem Packets Menu

This menu provides several counters for packet shapes of incoming data.

```

/EDX1000/Performance Monitoring/Ethernet/Counter Port: 2/In Problem Packets
                                     Press `U` to update counters

      inUndersize                      0
      inFragments                      0

      inJabber                         0
      inOversize                       0

      Exit

(a): Alarmlog
    
```

Table 5-51 provides information on the menu options.

Table 5-51 *In Problem Packets Menu Options*

Parameter	Description	Format	Default
inUndersize	Total frames received with a length of less than 64 octets but with a valid FCS.	Display	no default
inFragments	Total frames received with a length of less than 64 octets but with an invalid FCS.	Display	no default
inJabber	Total frames received with a length of more than MTUSize octets but with an invalid FCS.	Display	no default
inOversize	Total frames received with a length of more than MTUSize octets but with a valid FCS.	Display	no default
Exit	Leave menu page.	Exit	

Out Counters Menu

All counters valid for outgoing data are shown.

```

/EDX1000/Performance Monitoring/Ethernet/Counter Port: 2/Out Counters
                                     Press `U` to update counters

    outUnicasts                       0
    outMulticast                       0
    outBroadcast                       0

    outPause                           0

    outFCSError                        0

    outOctets                          0

    Exit

(a): Alarmlog

```

Table 5-52 provides information on the menu options.

Table 5-52 *Out Counters Menu Options*

Parameter	Description	Format	Default
outUnicasts	Total frames transmitted with an unicast destination address.	Display	no default
outMulticast	Total frames transmitted with a multicast destination address that are not counted in 'outBroadcast' or 'outPause'.	Display	no default
outBroadcast	Total frames transmitted with a destination address equal to FF:FF:FF:FF:FF:FF.	Display	no default
outPause	Total pause frames transmitted.	Display	no default
outFCSError	Total frames transmitted with an invalid FCS. ⁱ	Display	no default

Table 5-52 Out Counters Menu Options (continued)

Parameter	Description	Format	Default
outOctets	Total data octets transmitted from frames counted above. The count includes the FCS but not the preamble.	Display	no default
Exit	Leave menu page.	Exit	

i. Whenever a frame is modified and a new FCS is computed for the frame. Before the new FCS is added into the frame the old FCS is inspected to insure the original unmodified frame was still good. If an error is detected the new FCS is added with a bad FCS and the 'outFCSError' counter is incremented.

Histogram Counter

This menu provides several counters for packet shapes of history data.

```
/EDX1000/Performance Monitoring/Ethernet/Counter Port: 2/Histogram Counter
                                     Press `U` to update counters

his64Octets           0
his127Octets          0
his255Octets          0
his511Octets          0
his1023Octets         0
hisMaxOctets          0

Exit

(a): Alarmlog
```

Table 5-53 provides information on the menu options.

Table 5-53 *Outgoing Packet Shapes Menu Options*

Parameter	Description	Format	Default
his64Octets	Total frames transmitted with a length of exactly 64 octets, including those with errors.	Display	no default
his127Octets	Total frames transmitted with a length of between 65 and 127 octets inclusive, including those with errors.	Display	no default
his255Octets	Total frames transmitted with a length of between 128 and 255 octets inclusive, including those with errors.	Display	no default
his511Octets	Total frames transmitted with a length of between 256 and 511 octets inclusive, including those with errors.	Display	no default
his1023Octets	Total frames transmitted with a length of between 512 and 1023 octets inclusive, including those with errors.	Display	no default
hisMaxOctets	Total frames transmitted with a length of between 1024 and MTUSize octets inclusive, including those with errors.	Display	no default
Exit	Leave menu page.	Exit	

Out Problem Packets Menu

This menu provides several counters regarding faulty outgoing data packets.

```

/EDX1000/Performance Monitoring/Ethernet/Counter Port: 2/Out Problem Packets
                                Press `U` to update counters

    outCollisions                0
    outLate                      0
    outExcessive                 0
    outMultiple                  0
    outSingle                    0
    outDeferred                  0
    outDiscards                  0

                                Exit
                                (a): Alarmlog
    
```

Table 5-54 provides information on the menu options.

Table 5-54 *Out Problem Packets Menu Options*

Parameter	Description	Format	Default
outCollisions	Total number of collisions during frame transmission.	Display	no default
outLate	Total number of times a collision is detected later than 512 bit-times into the transmission of a frame.	Display	no default
outExcessive	Total number of frames not transmitted because the frame experienced 16 transmission attempts and it was discarded.	Display	no default
outMultiple	Total number of successfully transmitted frames that experienced more than one collision.	Display	no default

Table 5-54 Out Problem Packets Menu Options (continued)

Parameter	Description	Format	Default
outSingle	Total number of successfully transmitted frames that experienced exactly one collision.	Display	no default
outDeferred	Total number of successfully transmitted frames that are delayed because the medium is busy during the first attempt.	Display	no default
outDiscards	Total number of frames discarded that were not transmitted due to a lack of buffer space. Always 0 in this device since all discards occur at Ingress and are counted in 'inDiscards'.	Display	no default
Exit	Leave menu page.	Exit	

Set Histogram Options

Select "Set Histogram Options" in the Ethernet menu and press the Enter key. The following screen will be displayed:

```

/EDX1000/Performance Monitoring/Ethernet/Set Histogram Options

      Histogram Mode          count RX only

Exit

(a): Alarmlog
  
```

In this menu the Histogram Mode can be selected. Possible Values are 'count RX only', 'count TX only' and 'count RX + TX'.

The events will be displayed in the same menu.

Any changes which are made will be highlighted/indicated by an asterisk (*) in front of the line. All highlighted changes are NOT activated, yet. the activation will take place for ALL changes only when “Apply Changes and Restart (if required)” is pressed. So all changes will be activated at the same time. IP-address etc. can be changed without losing contact to the device at once.

NOTE: If “Exit” is selected instead of “Apply Changes and Restart (if required)”, nothing(!) will be stored or activated. All changes are refused!

After the changes are applied, the device might restart. Not all changes will cause a restart, but some. For example, the assignment of a new profile, will always lead to a re-boot of the device!

After leaving the menu and re-enter it, the actual values of the variables are shown. So if there were any changes, the new values are presented after leaving and re-entering the menu.

NOTE: The different profiles do set the IP address and the LPT/RFD setting. So it might be, that after loading a new profile, these settings are according to the defaults stored in the profile. If there is need for different settings, these have to be changed after loading the profile. this can not be done in parallel (new profile plus changes!).

Chapter 6

SNMP and MIBs

This chapter provides information on the SNMP and the management information bases (MIBs) used by the EDX1000.

SNMP Access Generally

The growing global network 'Internet' was the home of plans to simplify network maintenance by defining a maintenance protocol, which would allow network managers to control network equipment via the network itself. This protocol was given the name SNMP (Simple Network Management Protocol). As the name implies, SNMP was originally planned as an intern solution. However, SNMP became widely used and is now a universal standard.

What is the difference between equipment with and without SNMP? Generally, SNMP featured equipment has:

- Added intelligence to talk SNMP and to get and set unit parameters
- An own unique network address
- Some kind of local management port

Network management by SNMP requires at least two partners:

- Network equipment with SNMP software, called 'agent'
- A network station, running some kind of network management software

The two partners communicate via the net using SNMP. The network management station sends configuration commands and data requests to the network equipment. The network equipment responds to requests by sending the requested data. Additionally, traps are triggered by certain events in the network equipment. Traps are data packets containing information about these events. Their destination is a (or multiple) network management station, where the information is collected. SNMP traps enable an agent to notify the management station(s) of significant events by way of an unsolicited SNMP message.

Network configuration information, in particular configuration commands, is sensitive data and must therefore be protected against prying eyes. SNMP deals with this problem by implementing something called a 'community'. A community is comparable to a password and gets attached to each SNMP message. The attached community allows the receiving SNMP partner to decide if the transmitting partner is allowed to force the execution of the command.

The EDX100x supports two versions of SNMP: SNMPv1 (version 1) and SNMPv2c (version2, community-based).

SNMPv1

SNMPv1 first appeared in 1988 and is defined in [IETF RFC 1065], [IETF RFC 1066] and [IETF RFC 1067]. It supports a basic set of commands (get, set and the possibility to send traps). Authentication of clients is performed only by a “community string”, in effect a type of password, which is transmitted in clear text.

SNMPv2c

Community-Based Simple Network Management Protocol version 2, or SNMP v2c, is defined in [IETF RFC 1901]. SNMP v2c revises version 1 and includes improvements in the areas of performance, confidentiality, and manager-to-manager communications. It introduced GETBULK, an alternative to iterative GETNEXTs for retrieving large amounts of management data in a single request. SNMPv2c uses the same simple community-based security scheme as SNMP v1. While officially only a “Draft Standard”, this is widely considered the de facto SNMP v2 standard.

Traps

SNMPv1 and SNPv2c encourage trap-directed notification. The idea behind trap-directed notification is as follows: if a manager is responsible for a large number of devices, and each device has a large number of objects, it is impractical for him to poll or request information from every object on every device. The solution is for each agent on the managed device to notify the manager without solicitation. It does this by sending a message known as a trap of the event or NOTIFICATION.

After receiving the event, the manager displays it and may choose to take an action. For instance, the manager can poll the agent directly, or poll other associated device agents to get a better understanding of the event.

Trap-directed notification can result in substantial savings of network and agent resources by eliminating the need for frivolous SNMP requests. However, it is not possible to totally eliminate SNMP polling. SNMP requests are required for discovery and topology changes. In addition, a managed device agent can not send a trap, if the device has had a catastrophic outage.

Installation Prerequisites

This section provides the installation prerequisites for SNMP.

Prerequisites for SNMP management:

- A management station with an Ethernet 10/100BaseT respectively RS232 interface.
- Management software for SNMP management (e.g. SNMPc, HP Openview).
- A VT100 compatible terminal or PC with terminal software (only used for initial installation).

Preparing the SNMP Management System

Before managing the EDX100x by SNMP, one has to prepare the SNMP management system. First install the MIBs for the EDX100x and second configure the correct access parameters.

You can download the MIB from the ax extranet (www.arcutronix.com/customer):

Login: **User = p49170644-0**
 Password = 1qayxsw2

A MIB (Management Information Base) is a kind of database, which tells the network management station about specific capabilities of the new equipment. Add the contained MIBs to the MIBs already known to your management system. Generally, you have to re-compile the MIB database to include the new information.

Configure your management station to use SNMPv2c for read and write access mode and enter the community strings for read/write and read-only access.

SNMPv1/v2c Agent

The EDX100x has the functionality of an SNMPv1 and SNMPv2c agent. It can retrieve and send SNMP messages, generate traps and may be configured via an SNMP manager.

Five access levels are supported by the EDX100x to enable read and read/write operations. Depending on these levels different rights for reading (get-command) and writing (set-command) of MIB-OIDs (see also below “Management Information Bases (MIBS)”) are granted. This opens the possibility to give dedicated privileges to different SNMP managers. Table 6-1 shows the five levels and their corresponding access rights.

Table 6-1 *SNMP access levels*

Name	OIDs allowed to Get (Read)	OIDs allowed to Set (Write)
Administrator	<ul style="list-style-type: none"> • All, but – snmpTargetMIB (.1.3.6.1.6.3.12) – snmpVacmMIB (.1.3.6.1.6.3.16) – snmpCommunityMIB (.1.3.6.1.6.3.18) 	<ul style="list-style-type: none"> • All, but – snmpTargetMIB (.1.3.6.1.6.3.12) – snmpVacmMIB (.1.3.6.1.6.3.16) – snmpCommunityMIB (.1.3.6.1.6.3.18)
Standard	<ul style="list-style-type: none"> • Like <i>Administrator</i>, but – agentSecurityTable (.1.3.6.1.4.1.760.2.10.3) – agentTrapReceiverTable (.1.3.6.1.4.1.760.2.10.4) 	<ul style="list-style-type: none"> • Like <i>Administrator</i>, but – snmpSystemMIB (.1.3.6.1.2.1.1) – agentSecurityTable (.1.3.6.1.4.1.760.2.10.3) – agentTrapReceiverTable (.1.3.6.1.4.1.760.2.10.4)
Service	<ul style="list-style-type: none"> • Like <i>Standard</i> 	<ul style="list-style-type: none"> • Nothing
Monitor	<ul style="list-style-type: none"> • Like <i>Standard</i> 	<ul style="list-style-type: none"> • Nothing
Guest	<ul style="list-style-type: none"> • Only snmpSystemMIB (.1.3.6.1.2.1.1) 	<ul style="list-style-type: none"> • Nothing

SNMP and MIBs

Management Information Bases (MIBS)

These access levels may be combined with a community string, which is a “low-level” password. Thus a SNMP-manager, using a defined community, gets the assigned privileges.

For normal operation, the two predefined community strings “public” (access level = *Guest*) and “private” (access level = *Standard*) should be used.

You may use the CLI to add, change or delete the community strings (see Chapter 5, IP Configuration Menu on page 5-23).

Management Information Bases (MIBS)

The MIBs (Management Information Bases) define the variables which are used to control an SNMP device or to retrieve operational data from the device. The MIB hierarchy can be depicted as a tree with a nameless root, the levels of which are assigned by different organizations. This model permits management across all layers of the OSI reference model.

The new MIBs for arcutronix’s SNMP management Generation 2 are based on the arcutronix naming convention. The root-OID tree structure is accessible via

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).arcutronix(30507).g2Management(2)

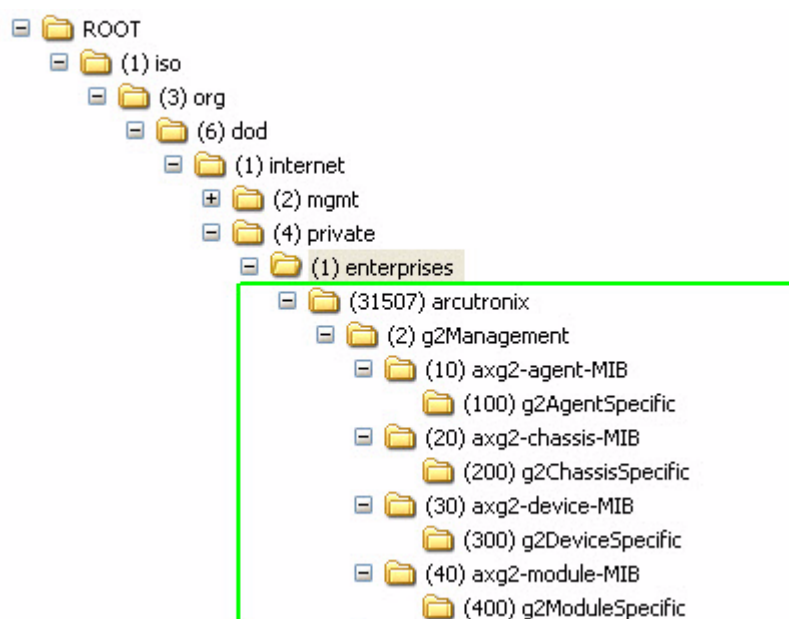


Figure 6-1 The SNMP ax-Generation 2 MIB Tree

The format of the MIBs as well as global sections are defined in the SNMP standard. MIBs are written in a special language (ASN.1 = Abstract Syntax Notation One) and are plain ASCII text. Thus they can be read using any available editor.

The following arcutronix MIBs are on the web and are supported by the EDX100x:

- axg2 MIB
- axg2-agent MIB
- axg2-device MIB
- axg2-EDX1000-agent-specific MIB
- axg2-EDX1000-device-specific MIB

As the EDX100x's SNMP agent always work in a stand-alone environment, the "axg2 chassis MIB" is not supported. The same is true for the "axg2 module MIB" as there is no (generic) module to be plugged onto the EDX100x platform.

In the next chapters only a short and rough overview about the mentioned MIBs are presented. All detailed information concerning the MIBs and how to use them for managing the EDX100x can be found in an extra document.

axg2.mib

The axg2 MIB specifies the general OIDs for arcutronix's g2Management. It is something like the root to all other MIBs.

axg2-agent.mib

The agent-MIB provides tables from the agent and access to variables of the SNMP agent (IP-Address, Subnet Mask, Trap Receiver, Communities, e.t.c.).

axg2-device.mib

The device-MIB provides tables from the EDX100x and access to variables of this device. This MIB {g2Management 30} describes and gives general information about all DEVICES from arcutronix designed for the g2Management and is mandatory for those. For specific features of devices see g2DeviceSpecific-MIB {300}.

axg2-EDX1000-as.mib

The axg2-EDX1000-as.mib describes all AGENT SPECIFIC {g2AgentSpecific 4} entities of EDX100x devices from arcutronix designed as a stand-alone unit and is mandatory for those devices. Hint: As the EDX100x is part of the g2management there are other MIBs to manage this type of unit. This MIB module may be extended without notice, when needed. Also refer to general information in the axg2-agent-MIB {g2Management 10}, for agent specific information for the EDX100x see the g2AgentSpecific {axg2-agent 100}.axg2-EDX1000-ds MIB

axg2-EDX1000-ds.mib

The axg2-EDX1000-ds.mib is device specific {g2DeviceSpecific 21} MIB (content of MIB-TREE g2management) and describes the specific features of EDX100x devices. This mob module may be extended without notice, when needed. Also refer to general information in the axg2-device-MIB {g2Management 30}, for specific information of the

SNMP and MIBs

Management Information Bases (MIBS)

EDX100x see the Device Table {axg2-devices 1} and the g2DeviceSpecific {axg2-device-MIB 300}.

Chapter 7

axCLI via SCX2e

When the EDX100x is mounted in an arcutronix sub-rack (e.g. SRX10) with an arcutronix System Controller Card (SCX2e) it can be configured via a text-based Command Line Interface (CLI). The arcutronix-CLI can be reached over a Secure Shell (SSH) connection, which has to be established between the host (SCX2e) and your PC. Only an SSH-client and an IP-connection to the SCX2e are needed.

The SCX2e-Manual (axManual_SCX2e.pdf) explains in detail how to connect the agent via ssh and how to use the CLI. Within this chapter a short introduction to the CLI is given and the menu-tree of the EDX100x is shown.

NOTE: The EDX100x-CLI menu-tree is very similar to the information shown in Table 5-2 in chapter “EDX100x Menu Options”. The details of the menu and usage of variables are given there, too.

The axCLI is organized just in the same way as the “EDX100x Control Software & gCLI”. It has the same menu-structure and options. The “navigation” within the CLI-menus and the access to the management-variables will be depicted in the next chapter.

Introduction to axCLI

CLI Editor Features

Context Sensitive Help

arcutronix-CLI offers context sensitive help. This is a useful tool for a new user because at any time during an ssh-session, a user can type a question mark (?) to get help. Two types of context sensitive help are available - word help and command syntax help.

Word help can be used to obtain a list of commands that begin with a particular character sequence. To use word help, type in the characters in question followed immediately by the question mark (?). Do not include a space before the question mark. The router will then display a list of commands that start with the characters that were entered.

Command syntax help can be used to obtain a list of command, keyword, or argument options that are available based on the syntax the user has already entered. To use command syntax help, enter a question mark (?) in the place of a keyword or argument. Include a space before the question mark. The router will then display a list of available command options with <cr> standing for carriage return.

Command Syntax Check

If a command is entered improperly (e.g. typo or invalid command option), the CLI will inform the user and indicate where the error has occurred.

Command Completion

Commands can not be abbreviated but a commands and keywords can always be completed with <TAB>. For example, you can abbreviate the “config” command to “c<TAB>” because “config” is the only command that begins with “c” and the <TAB> will complete it. If there are more than one possible completion, the CLI will show them to give you help. For example, “s<tab>” can be “show” and/or “select”. Both commands will be shown.

Hot Keys

For many editing functions, the arcutronix-CLI editor provides hot keys. Table 7-2 lists some editing short-cuts that are available.

Table 7-1 EDX100x CLI Hot Keys

Hot Key	Description
Delete	Removes one character to the right of the cursor.
Backspace	Removes one character to the left of the cursor.
TAB	Completes a partial command.
Ctrl-A	Moves the cursor to the beginning of the current line.
Ctrl-B	Moves the cursor one word to the left.
Ctrl-D	Removes one character to the right of the cursor.
Ctrl-I	Finishes a partial command.
Ctrl-J	Repeats the last command.
Ctrl-H	Removes one character to the left of the cursor.
Ctrl-N	Erases a line.
Ctrl-M	<CR>.
Up Arrow	Allows user to scroll forward through former commands.
Down Arrow	Allows user to scroll backward through former commands.

NOTE: The most helpful Hot-Key is the TAB. It allows inexperienced users to complete commands, gives correct syntax and shows possible entries at all stages!

Commands

Once an ssh-session is established, one can navigate within EDX100x-CLI like in a hierarchically structured tree. The EDX100x-CLI menu-tree is shown in “Menu-Structure (Directory-Tree) of EDX100x” on page 7-9. The tree is just the same as depicted in Table 5-2. Handling and meaning of the variables are the same and here it will not be presented in detail again.

To assist users in navigation through arcutronix-CLI, the command prompt will change to reflect the position of a user within the command hierarchy. This allows users to easily identify where within the command structure they are at any given moment. Also a <Tab> shows all possible options at the given position. This gives easy possibility to identify “Tab-by-Tab” the correct command.

NOTE: A <blanc> inside a string must be preceded by a back-slash (\) or the string must be wrapped by quotes. E.g.

```
$> mode "Rack View"           or
$> mode Rack\ View
```

The “Tab-by-Tab”-feature helps here a lot to build always the correct syntax.

Table 7-2 is a summary of commands and the corresponding syntax.

Table 7-2 EDX100x CLI Commands

Command	Syntax / Explanation
help	help [COMMAND] HELP is in any context available and lists the possible commands in the given context. If HELP is used with an command, it shows the syntax of the command together with a short help-text. • ARG COMMAND - any available command.
log	log LOG shows the last entries of agent's log file.
config	config [go up root SUBPAGE set OPTION VALUE do COMMAND [OPTION]]

Table 7-2 EDX100x CLI Commands (continued)

Command	Syntax / Explanation
	<p>CONFIG shows and changes configuration settings. Configurations are grouped and this command can also be used to display/change configuration group. Without an argument CONFIG shows the current configuration group and its settings/subgroups.</p> <ul style="list-style-type: none">• ARG go up root SUBPAGE - Go to another config page. Choose a SUBPAGE from the current config page, go UP to the parent page or go to the ROOT page. Type config to see available submenus (marked with '>').• ARG set OPTION VALUE - Set a new VALUE for a writable OPTION• ARG do COMMAND - Execute a config command (displayed with config as [Command])• ARG OPTION - Show config OPTION
select	<p>select [agent [rack RACK] slot SLOT serial SERIAL DEVICENAME]</p> <p>SELECT a device which should be configured in Cardview-mode.</p> <ul style="list-style-type: none">• ARG agent - Select the agent card.• ARG rack RACK - Select device from RACK (integer).• ARG slot SLOT - Select device in slot SLOT (integer).• ARG serial SERIAL - Select device with serial number SERIAL.• ARG DEVICENAME - Select device DEVICENAME.
show	<p>show</p> <p>SHOW presents the information about all available racks.</p>
mode	<p>mode [MODE]</p> <p>With MODE one can easily switch between RACKVIEW and CARDVIEW.</p> <ul style="list-style-type: none">• ARG MODE - Select mode MODE; available modes are:<ul style="list-style-type: none">- MODE Card View- MODE Rack View
quit	<p>quit</p> <p>Quit the current CLI session.</p>

Usage of axCLI

Two modes are defined for the axCLI when used via the agent-card SCX2e:

- Rackview-Mode and
- Cardview-Mode

Rackview-mode is to get mainly information about the rack, the plugged cards, power supply etc. In Cardview-mode one can select one single card and gets direct access to

it. One can configure, supervise and control cards only in Cardview-mode. To switch between the two modes, one has to use the `mode` command.

Rackview - Mode

In the Rackview-mode, one can get information about (all) the discovered racks and plugged cards.

NOTE: Rackview-mode is the Default after first login.

The Rackview-mode can be reached from any point within the CLI using the command `MODE`:

```
cardview $> mode Rack\ View
rackview $>
```

In Rackview-mode no settings or changes are possible. One can see all racks and cards and has the option to navigate to one of the discovered cards via “select”-command or to change to CardView-mode via “mode”-command.

Example SELECT

The command `SELECT` gives you the chance to change into the Cardview-mode of a single card. If you want to select a EDX1000, which is plugged in slot 7, the following ways are possible.

SELECT by rack/slot address

```
rackview $> select rack Rack1 slot 7
Rack1:7 EDX1000 "Test Device7" $>
```

SELECT by name

```
rackview $> select "Test Device7"
Rack1:7 EDX1000 "Test Device7" $>
```

SELECT by serial number:

```
rackview $> select serial 2010002229
Rack1:7 EDX1000 "Test Device7" $>
```

The 3 ways are identical by result. The mode is changed to Cardview-mode and the EDX1000-device in slot 7 is selected.

Cardview - Mode

The Cardview-mode can be reached from any point within the CLI using the command `MODE`:

```
rackview $> mode Card\ View
```

```
Agent SCX2e "Main Agent" $>
```

or by using the SELECT command (see examples above):

```
rackview $> select rack Rack1 slot 7  
Rack1:7 EDX1000 "Test Device7" $>
```

NOTE: The default card, which is selected, when no other card is explicitly selected is the agent card.

Example CONFIG

The command CONFIG is the most mighty tool in the EDX100x CLI. It is only available in Cardview-mode and gives access to the menu-structure of the selected card. Within this document, the following examples will mostly depend on the EDX1000 itself. The menu-structure of the EDX1000 is shown in "Menu-Structure (Directory-Tree) of EDX100x" on page 7-9.

When entering the command CONFIG apart in any context (of the Cardview-mode), the available menu-entries are shown:

```
Rack1:7 EDX1000 "Test Device7" $> config  
--Login  
> Local
```

The first 1-2 signs in the resulting overview are type-indicators which shows can be done with this entry and which config-command can be used.

Table 7-3 Menu Indicators and corresponding CONFIG Commands

Typ	Explanations / Examples
--	<p>Headline:</p> <p>This is the name of the shown menu. Nothing can be done with CONFIG; it is only a text.</p> <p>Example:</p> <pre>\$> config --LOGIN . . \$></pre>
>	<p>Sub-Menu:</p> <p>">" indicates a sub-menu, which can be accessed via CONFIG GO <sub-menu-name></p> <p>Example:</p>

Table 7-3 Menu Indicators and corresponding CONFIG Commands (continued)

```
$> config
--Login
> General System Information
> Administration
> Alarm Management
> Firmware Update
$> config go Administration
/Administration $>
```

***** Changeable Management Variable

“**“ indicates a menu-entry which can be changed via
CONFIG SET <variable-name> <value>

Example:

```
/General System Information $> config
--General System Information
* Device Name: "Main Agent"
.
.
.
/General System Information $> config set Device\ Name "New Name"
/General System Information $> config
--General System Information
* Device Name: "New Name"
.
.
.
/General System Information $>
```

+ Command

“+“ indicates a command-entry which can be invoked via
CONFIG DO <command-name>

Example:

```
/Administration/Reset System $> config
--Reset System
Reset State: No reset scheduled
* Reset Mode: Immediate reset
+ [Start Reset]
/Administration/Reset System $> config do Start\ Reset
```

Table 7-3 Menu Indicators and corresponding CONFIG Commands (continued)

blan	Read-Only Variable
^C	No sign (or blanc character “ ”) indicates a read-only variable which can be read via
	CONFIG <variable-name>
	Example:
	<pre>/General System Information \$> config --General System Information . . . Device Temperature: "35.5" . /General System Information \$> config Device\ Temperature "35.5" /General System Information \$></pre>

There are some special CONFIG commands, which help to navigate:

Table 7-4 Special CONFIG Commands

Typ	Explanations / Examples
e	<p>Go back one directory in the directory-tree of the selected device in Cardview-mode.</p> <p>Example:</p> <pre>/Administration/Reset System \$> config go up /Administration \$> config go up \$></pre>
	<p>Goto root directory of the selected device in Cardview-mode.</p> <p>Example:</p> <pre>/Administration/Reset System \$> config go root \$></pre>

Quick Usage Guide for CLI-Commands

Table 7-5 Quick Reference

Select Agent:
<pre>\$> select agent</pre>
Select Card in Slot 1:
<pre>\$> select slot 1</pre>

Table 7-5 Quick Reference (continued)

Select Local/Remote Instance of Connectivity Products:

```
$> config go Local
$> config go Remote
```

Show options in actual menu:

```
$> config
```

Change (User-) Name (e.g. FCX10G): [Local -> Maintenance -> General Information -> User Name]

```
$> config go root
$> config go Local
$> config go Maintenance
$> config go General\ Information
$> config set User\ Name "new Name"
```

Reboot Device (e.g. FCX10G): [Local -> Maintenance -> Update]

```
$> config go root
$> config go Local
$> config go Maintenance
$> config go Update
$> config set Reboot\ flash\ 1\ software
```

View Alarms (e.g. FCX10G): [Local -> System Monitor]

```
$> config go root
$> config go Local
$> config go system\ Monitor
$> config
```

Clear Alarms (e.g. FCX10G): [Local -> System Monitor -> Clear Current Alarms]

```
$> config go root
$> config go Local
$> config go system\ Monitor
$> config set Clear\ Current\ Alarms clear_now
```

Go back 1 Step in Menu:

```
$> config go up
```

Go back to Top-Level Menu (/):

```
$> config go root
```

Menu-Structure (Directory-Tree) of EDX100x

The menu structure of the EDX100x variants is stored in an extra document:

MenuStructureEDX100x.pdf [axMenuStructEDX].

Appendix A

Technical Specifications

EDX100x Hardware Specification

Table A-1 to Table A-6 provide the general technical data of the EDX - Ethernet Demarcation.

Table A-1 Number of Interfaces

Type		
EDX100x-Family		
Number of Interfaces		
EDX1000	1x Fast Ethernet 10/100BaseT (RJ45),	MGMT, only
	1x Gigabit Ethernet 10/100/1000BaseT (RJ45),	General Purpose
	1x Gigabit Ethernet 1000BaseX (SFP),	General Purpose
	1x V.24 (only accessible in SHX and SRX3)	local MGMT
EDX1002	1x Fast Ethernet 10/100BaseT (RJ45),	MGMT, only
	2x Gigabit Ethernet 1000BaseX (SFP),	General Purpose
	1x V.24 (only accessible in SHX and SRX3)	local MGMT
EDX1006e	1x Fast Ethernet 10/100BaseT (RJ45),	MGMT, only
	6x Fast Ethernet 100BaseFX (SFP),	General Purpose
	2x Gigabit Ethernet 1000BaseX (SFP),	General Purpose
	1x V.24 (only accessible in SHX and SRX3)	local MGMT

Technical Specifications
EDX100x Hardware Specification

Table A-1 Number of Interfaces (continued)

Type		
EDX1008	8x Fast Ethernet 10/100BaseT (RJ45),	General Purpose
	2x Gigabit Ethernet 1000BaseFX/T (SFP),	General Purpose
	1x V.24 (only accessible in SHX and SRX3)	local MGMT

Table A-2 Power Requirements

Type			
Power Supply			
Type:	DC		
Input voltage:	+5VDC	+/- 5%	
Connector:	Via backplane		
Power Requirements ⁱ			
Device	w/o SFP	With Standard SFP(s) (700mW)	Max. power to be used by SFP(s)
EDX1000	3.4 VA	4.1 VA (1x SFP)	1.8 VA
EDX1002	3.4 VA	4.8 VA (2x SFP)	1.8 VA, each
EDX1006	3.4 VA	9.0 VA (2x GE-SFP + 6x FE-SFP)	1.8 VA, each
EDX1008 (1xFE connected)	3.5 VA	4.9 VA (2x SFP)	1.8 VA, each
(8xFE connected)	5.8 VA	7.2 VA (2x SFP)	1.8 VA, each

i. The total power need depends on the used SFP(s).

Table A-3 Technical Data ⁱ of the Interfaces

Type
Interfaces
Fast Ethernet Interfaces (Copper)

Table A-3 Technical Dataⁱ of the Interfaces (continued)

Type	
Type:	[IEEE 802.3] (full- and half-duplex, Autonegotiation)
Data rate	10 or 100Mbps
Connection type:	Twisted-Pair interface (TP)
Function, electrical values, pin assignment:	according to [IEEE 802.3] Clause 14 (10BaseT), [IEEE 802.3] Clause 25 (100BaseTX)
Impedance:	100 Ohm (balanced)
Connector:	8 pin RJ-45 connector according to ISO 8877
Fast Ethernet Interfaces (SFP)	
Type:	[IEEE 802.3] (full- and half-duplex, Autonegotiation)
Connection type:	Fibre Optics (FO), SFP
Function, electrical values:	[IEEE 802.3] Clause 25 (100BaseFX, 100BaseSX, 100Base-BX, 100Base-LX10)
Connector:	LC
SFP:	According to [SFP MSA], Rev 4.5, Aug. 31, 2006 All vendors supported. Max. 100 insertion / extraction.
Gigabit Ethernet Interface (Copper)	
Type:	[IEEE 802.3] (full- and half-duplex, Autonegotiation)
Connection type:	Twisted-Pair interface (TP)
Function, electrical values:	according to [IEEE 802.3] Clause 14 (10BaseT), [IEEE 802.3] Clause 25 (100BaseTX) [IEEE 802.3] Clause 34 (1000BaseT)
Impedance:	100 Ohm (balanced)
Connector:	8 pin RJ-45 connector according to ISO 8877
Gigabit Ethernet Interface (SFP)	
Type:	[IEEE 802.3] (full-duplex)
Connection type:	Fibre Optics (FO), SFP
Function, electrical values:	according to [IEEE 802.3] Clause 14 (10BaseT), [IEEE 802.3] Clause 25 (100BaseTX)
Connector:	LC or RJ45

Table A-3 Technical Dataⁱ of the Interfaces (continued)

Type	
SFP:	According to [SFP MSA], Rev 4.5, Aug. 31, 2006 All vendors supported. Max. 100 insertion / extraction.
Serial Interface (V.24)	
Purpose:	Management port
Function, electrical values:	According to V.24, standard rate 57.600 Baud, 8N1

i. Technical specifications are subject to change.

Table A-4 Display Functions

Type	
Display Functions	
System:	LEDs for operating and error status
Fast Ethernet interfaces:	LEDs for Link Status and 10/100Mbps recognition (only TP ports)
Gigabit Ethernet interfaces:	LEDs for Link Status and 10/100/1000Mbps recognition (only TP ports)

Table A-5 Mechanic and Environment

Type	
Mechanics	
Design:	LineCard for Rack mount chassis or single-slot housing
Dimensions:	190 x 130 x 30mm
Weight:	250g
Cooling:	Convection cooling through ventilation slots in the housing environment
Operation:	ETS 300 019: class 3.1
Transport:	ETS 300 019: class 2.1
Storage (in packing):	ETS 300 019: class 1.1

Table A-5 Mechanic and Environment (continued)

Type	
EMC	
	EN 55022:1998 + A1:2000 class B
	EN 61000-3-2:2000
	EN 61000-3-3:1995 + A1:2001
Product Security	
Electrical security:	EN 60950
Sound emission:	None (no build-in fan)
Conformity:	CE

Table A-6 μ Controller and Clock

Type	
Electronics	
Main processor:	32 Bit power PC, Freescale MPC852T
Non-volatile memory:	16 MB
Main memory:	64 MB SDRAM
Real Time Clock	
Accuracy	10ppm (<1sec/day)
Hold Time (without ext. power)	min. 11 days

EDX100x Software Specification

Table A-7 provides the general technical data of the EDX - Ethernet Demarcation.

Table A-7 Technical Data ⁱ of the EDX100x - Software

Type
EDX100x
General Information
Valid SW-Version for this manual: V 2_1_43

Table A-7 Technical Data ⁱ of the EDX100x - Software (continued)

Type	
IP address assignment:	The IP address dynamically (e.g. by ISP) allocated through DHCP is accepted
Switching, VLAN	
Interfaces:	LAN: 10/100BaseTX, Line: 1000BaseX or 10/100/1000BaseTX
RS-232:	Serial management (if single-slot housing or terminal access card is used)
Switching Options	
	Traffic classification/priority based on TOS/DSCP [IEEE 802.1Q]
	4 priority queues for traffic management
	Low latency handling of VoIP/video services
	[IEEE 802.1Q] VLAN: forwarding, stacking (802.1Q-in-Q)
	16 port based VLANs with tagging acc. [IEEE 802.1Q]
	8k MAC addresses supported
Jumbo-Frames supported:	MTU (Maximum Transmission Unit): 1632 Bytes

i. Technical specifications are subject to change.



Appendix B

Exercise Troubleshooting

In case of a malfunction of the system, please refer to this section for information about possible causes. Consider the following points to find out why the system is not operating properly:

1. Data traffic from and to the system must be possible (refer to the section “Is the System Operating Correctly?”).
2. If the current indicator display does not match the display that you have expected and the system is not working properly, you should be able to carry out a detailed error diagnosis using the tables of these sections (refer to the section “Meaning of Further Indicator Displays”).

Is the System Operating Correctly?

Check the LED indicators on the front panel of the device.

- The LNK indicator of the LAN interfaces are permanently lightened when a link signal from the TP line is recognized.
- The ALARM, RFD and LPT indicators remain off.

If the current display does not match the display that you have expected and the system is not working properly, you should be able to carry out a detailed error diagnosis by using the tables of the next sections.

Meaning of Further Indicator Displays

Please refer to the following table for the interpretation of the LED to determine if an error is present.

Table B-1 Indicators Displays in Operating State

LED	Display	Meaning/Possible Cause
LNK	Remains off	Link signal from TP line not recognized TP plug is not engaged Remote station is not operational TP line is interrupted TP cable attenuation is too high or TP line is too long TP interface is defective
ERR	Enlightened	Indicates alarm condition on configured interface
LPT	Enlightened	Link Pass Through functionality activated due to loss of link
RFD	Enlightened	Remote Fault Detection functionality activated due to loss of link
ON	Remains off	No operating voltage Check that the power supply cable is well connected

Appendix EC

EC Declaration of Conformity



Declaration of EC-Conformity

We arcutronix GmbH
Garbsener Landstr. 10
D – 30419 Hannover
Germany

declare under our sole responsibility that the product group

Name: EDX1000 – Gigabit Ethernet Demarcation Devices
Members: EDX1000, EDX1002, EDX1008, EDX1006
Number: 0716-2001, -2101, -3200, - 4600

to which this declaration relates conforms to the following standards, which have been described in the CE-guideline:

93/68/EEC	CE marking
2004/108/EC	Electromagnetic compatibility (EMC)
2006/95/EC	Safety of low voltage equipment (LVD)
1999/5/EC	Radio & Telecommunications Terminal Equipment (R&TTE)
2002/95/EC	Restriction of the use of certain Hazardous Substances (RoHS)
2002/96/EC	Waste Electrical and Electronic Equipment (WEEE)

The above listed products satisfy all technical regulations, applicable to the products based on following standards:

EN 55022	Electromagnetic compatibility (EMC) for Information technology equipment
EN 55024	Electromagnetic compatibility (EMC) for Information technology equipment
EN 61000-4-1	Electromagnetic compatibility (EMC) for Information technology equipment
EN 61000-4-2	Electrostatic discharge immunity test
EN 61000-4-3	Radiated, radio-frequency, electromagnetic field immunity test
EN 61000-4-4	Electrical fast transient/burst immunity test
EN 61000-4-5	Surge immunity test
EN 61000-4-6	Immunity to conducted disturbances, induced by radio-frequency fields
EN 61000-4-11	Voltage dips, short interruptions and voltage variations immunity tests
EN 61000-6-1	Generic immunity standard – Residential, commercial and light industry
EN 61000-6-2	Generic immunity standard – Industrial environment
EN 60950	Safety of Information technology equipment

Hannover, 16.8.2009

Andreas Zimmermann
TD arcutronix GmbH

arcutronix GmbH ☺ Garbsener Landstr. 10 ☺ D-30419 Hannover ☺ Germany
+49 511 277 2700 ☺ sales@arcutronix.com ☺ www.arcutronix.com

Headquarter

arcutronix GmbH
Garbsener Landstrasse 10
30419 Hannover
Germany

Phone: **+49 (511) 277 2700**

Fax: **+49 (511) 277 2709**

Email: **info@arcutronix.com**

Web: **www.arcutronix.com**