

arcutronix

Synchronize the Ethernet

USER GUIDE

ENX
GS1



arcutronix GmbH
Deutschland

**Installation and
Operation Manual**

Version 1.3

ENX - Synchronous Ethernet Network Termination

USER GUIDE



Covered Variants of ENX by this User Guide:

ENX-F: 1102 - 1000

Covered Software Versions of ENX by this User Guide:

SW-Version: V 1_1_00

Boot-Loader: V 1_3

Part-Number (User-Guide): 1102 00 65.man

Version: V 1.3

Date of Issue: 2013-07-18

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
Web: <http://www.arcutronix.com>

Copyright Note

© Copyright 2011, 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 modifying 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 ENX - Synchronous Ethernet Network Termination. It provides information on configuration, system installation and technical data.

The intended audience of this document is anyone who is responsible for installing, maintaining or operating the ENX - Synchronous Ethernet Network Termination. 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:** General description of the ENX devices and applications for use.

Chapter 2, **Getting Started:** Short form about installation, mounting and configuration of ENX-family.

Chapter 3, **Hardware & Interfaces:** Description of hardware and front panel elements.

Chapter 4, **Functionality:** Switching, routing, agent.

Chapter 5, **ENX Web-GUI:** Control and configuration of the ENX.

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

Chapter 7, **SSH and CLI:** Explains the SSH access to the ENX and the usage of the Command Line Interface (CLI).

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

Appendix EC, **EC Declaration of Conformity:** Valid for the ENX product family.

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

- 2013-01-10 Version 1.3 Editor: mjz
Added and changed the following topics:
- As this manual become much to huge it was not longer possible to send it via e-mail. Main reason for this was the great number of screen-shots in chapter 5 (Web-GUI). For this reason, chapter 5 was almost completely extracted from this manual and a new document “[axRefGuideWebGUI_ENX]”was created.
- 2012-07-01 Version 1.2 Editor: mjz
Added and changed the following topics:
- Order of Release History changed from bottom-up to top-down.
 - Expansion of chapter Related and Referenced Documents.
 - An additional picture to illustrate the behaviour around the SSM clock quality level.
 - SSH-connection details depicted in more detail.
 - PTP Alarm Group added.
 - Size of MAC address table added (8k).
- 2012-05-14 Version 1.1 Editor: mjz
Added and changed the following topics:
- Added document version for better traceability.
 - Added missing VLAN-section in chapter 5.
 - Extended LACP-section in chapter 5.
 - Front page updated to “Synchronize the Ethernet”
- 2012-04-18 Added and changed the following topics:
- Adoptions for new SW release V1_0_5.
- 2012-03-13 Added and changed the following topics:
- Adoption for customer’s variant.
- 2011-10-21 First issue of the ENX User Guide.

Referenced and Related Documents

- [axRefGuideWebGUI_ENX] arcutronix GmbH (2013): ENX Web-GUI, Reference Guide.
- [axRefGuideCLI_ENX] arcutronix GmbH (2012): ENX Command Line Interface, Reference Guide.
- [IEC 60825-1] IEC 60825-1 - 2007: Safety of laser products - Part 1: Equipment classification and requirements
- [IEEE 802.1AS] IEEE Std 802.1AS™-2011: Timing and Synchronization for Time-Sensitive Applications in Bridged Local Area Networks.
- [IEEE 802.1AX] IEEE Std 802.1AX™-2008: Link Aggregation.
- [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 802.3] IEEE Std 802.3™-2008: Part3: Carrier sense multiple access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications.
- [IEEE 802.11] IEEE Std 802.11™-2012: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.
- [IEEE 1588] IEEE Std 1588™-2008: IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems.
- [IEEE 1901] IEEE Std 1901™-2010: Broadband Over Power Lines PHY/MAC Working Group (COM/SC/BPLPHMAC).
- [IETF RFC 791] IETF RFC 791 (1981), Internet Protocol (IP).
- [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 2544] IETF RFC 2544 (1999), Benchmarking Methodology for Network Interconnect Devices.
- [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 3414] IETF RFC 3414 (2002), User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3).
- [IETF RFC 5905] IETF RFC 5905 (2010), Network Time Protocol Version 4: Protocol and Algorithms Specification.
- [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.703] Recommendation ITU-T G.703 (2001), Physical/electrical characteristics of hierarchical digital interfaces.
- [ITU-T G.704] Recommendation ITU-T G.704 (1998), Synchronous frame structures used at 1544, 6312, 2048, 8448 and 44 736 kbit/s hierarchical levels.
- [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.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 G.8264] Recommendation ITU-T G.8264/Y.1364 (2008), Distribution of timing information through packet networks.
- [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.
- [ITU-T Y.1731] Recommendation ITU-T Y.1731 (2006), OAM functions and mechanisms for Ethernet based networks.
- [MEF 6.1] MEF Technical Specification MEF 6.1 (2008), Ethernet Services Definitions - Phase 2

About this Book

Referenced and Related Documents

[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

Document Organization	about-1
Chapters	about-1
Conventions	about-2
Release History	about-3
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
Fiber 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

ENX Description	1-1
General	1-1
Application Areas for the ENX	1-1
ENX Functions at a Glance	1-2
Synchronization	1-2
Switching	1-2
Management	1-3
Housing and Power Supply	1-3
Alarm Conditions and Relay	1-3
Order Information	1-3
Accessories	1-4
Cables	1-4
SFPs (Small Form-factor Pluggable)	1-4

Chapter 2 Getting Started

Delivered Parts	2-1
Preparing the Start-up	2-1
Operating Conditions	2-1
Ambient Conditions.	2-2
Mounting Options	2-2
Rack-Mount 19"-Rack	2-2
Desktop Usage	2-4
Airflow Requirements	2-4
Start-up of the ENX.	2-5
Switching on the Device	2-5
Power-Up Sequence.	2-5
LED Start-Up.	2-5
Configuration Access	2-7
Local and Remote IP-Access	2-7
Inband IP-Access	2-8
Serial Access	2-8
Configuration Methods	2-8
Web Access	2-8
SSH Access	2-9
Telnet Access	2-9
SNMP Access.	2-9
Command Line Interface.	2-9

Chapter 3 Hardware & Interfaces

Hardware Overview	3-1
Block-Diagram	3-1
ENX-F Front Panel	3-3
Management & Status Area	3-4
LAN & LINE Area	3-5
Features of a LINE Port	3-5
Features of a LAN Port	3-6
Labels and LEDs for LINE and LAN Port	3-6
Clock Area	3-7
Console Port.	3-8
Pinning	3-8
RS232 Connection Cable	3-9
Q / F Interface.	3-9
10/100BaseT (RJ45).	3-9
Auto-Cross-Over.	3-10
Combo-Ports.	3-10
Ethernet Loop-Back	3-11
1000BaseTX (RJ45)	3-11
RJ45 Connector	3-12

Auto-Cross-Over	3-12
1000Base-X (SFP)	3-13
Standards	3-13
T3an & T4ab	3-13
T3an	3-13
T4ab	3-14
1PPS Interface	3-15
Pinning	3-16
ENX-F Rear Side	3-16
Alarm Connector	3-16
Push-Button	3-17
Power Supply	3-17
AC Power Supply	3-17
DC Power Supply	3-18

Chapter 4 Functionality

Media Conversion	4-1
Switching	4-1
VLANs	4-2
Introduction to VLAN	4-2
Supported VLAN-Modes of ENX	4-3
VLAN Aware	4-3
Example	4-4
Provider VLAN-Tagging	4-6
How it works	4-6
L2CP Frames Handling	4-7
MEF Services	4-7
EPL	4-8
EVPL	4-8
EP-LAN and EVP-LAN	4-9
EP-Tree and EVP-Tree	4-9
Quality of Service	4-10
Introduction	4-10
Implementation	4-11
Classification	4-12
Priority-Sticker	4-12
Queue-Sticker	4-13
IP Precedence and DSCP	4-15
Limiting	4-16
Packet Selection for Limiter	4-16
Date-Rates for Limiter	4-17
Shaping	4-18
CIR & CBS	4-18
Queue Scheduler	4-19

MAC Address Table	4-20
Link Aggregation with LACP	4-21
LACP Introduction	4-21
Implementation	4-22
LACP Configuration	4-22
Port Group Details	4-22
LACP Aggregators	4-23
Clocking and Synchronization	4-23
Synchronous Ethernet (SyncE)	4-23
Introduction	4-23
Implementation	4-24
Clock Source Properties	4-26
Clock Source Selection	4-27
Synchronization State	4-28
T4ab Driver	4-28
Alarming Capabilities	4-29
PTP and IEEE 1588v2	4-29
Introduction	4-29
L2 MC-MAC Addresses	4-30
Implementation	4-31
PTP-Messages	4-32
Grand-Master	4-33
PTP Analysis	4-33
User & Access Administration	4-34
Access-Options to the ENX	4-34
SSH-Access	4-36
User Administration	4-36
Locally Stored Users	4-36
Rules for Usernames	4-37
Rules for Passwords	4-37
TACACS+	4-37
TACACS Example Configuration	4-38
Auto-Logout	4-39
Time-Based Auto-Logout	4-39
Protocol-Based Auto-Logout	4-40
Hardware-Based Auto-Logout	4-40
Management Port Configuration	4-40
Port Settings	4-40
Management Port "F/Q MGMT"	4-40
Management Port "Inband MGMT"	4-40
IP-Addressing	4-41
Management Port "F/Q MGMT"	4-41
Management Port "Inband MGMT"	4-41
DHCP and Manual Address Assignment	4-42
F- and Q-Interface	4-42

DNS-Support	4-43
Firmware-Update	4-43
File-Transfer to/from Servers and via HTTP	4-44
SFTP and TFTP	4-45
HTTP	4-46
Miscellaneous Features	4-46
Auto Negotiation	4-46
Speed and Duplex	4-46
Clock	4-48
EFM OAM	4-48
EFM (802.3ah) Link-layer OAM	4-49
Alarm Management	4-49
Alarm Types	4-50
Alarm States	4-50
Not Available	4-51
Inactive	4-51
Ignored	4-51
Acknowledged	4-51
Warning	4-51
Error	4-51
Alarm Acknowledgement Behaviour	4-52
Keep Acknowledged Until Inactive	4-52
Unacknowledge When Raising Severity	4-52
Unacknowledge on State Change	4-52
Example	4-52
Alarm Properties	4-54
Common Alarm Properties	4-54
Digital Alarm Properties	4-54
Analogue Alarm Properties	4-54
Alarm Groups	4-55
Global Alarm Status	4-55
Active Alarm List	4-55
Date & Time Settings	4-56
NTP and Encryption	4-56
Configuration Management	4-56
Temperature Shutdown	4-57
Diagnostics	4-58
Logging	4-58
<INFO>	4-59
<AUDIT>	4-59
<ALARM>	4-59
<ERROR>	4-59

Chapter 5 ENX Web-GUI

Introduction	5-1
Access to the Device	5-1
Security Issues	5-1
Web-Menu Body	5-2
Login Screen	5-2
Layout of Web-GUI	5-3
Navigation	5-4
Select a menu entry	5-4
Page Update	5-4
Logout	5-4
Web-Menus of ENX	5-5

Chapter 6 SNMP and MIBs

SNMP Access Generally	6-1
SNMPv2c	6-2
SNMPv3	6-2
Traps	6-2
Installation Prerequisites	6-3
Preparing the SNMP Management System	6-3
Management Information Bases (MIBS)	6-3

Chapter 7 SSH and CLI

Access to the Device	7-1
SSH Connection	7-1
Using User-Name and Password	7-1
Using Global SSH-Password	7-2
Using SSH-Key	7-3
Direct Login Key	7-4
Connection Key	7-4
Security Issues	7-5
SSH Client	7-5
Command Line Interface (CLI)	7-7
Introduction to the CLI	7-7
CLI Editor Features	7-8
Context Sensitive Help	7-8
Command Syntax Check	7-9
Path & Command Completion	7-9
Reduced Entry of Path & Command	7-9
Prompt and Path	7-9
Comment	7-10
Hot Keys	7-10
CLI Commands	7-11
The command CONFIG	7-15

Short-cuts	7-18
Quick Usage Guide for CLI-Commands	7-19
Example for SSH-Script	7-20

Appendix A Technical Specifications

ENX Hardware Specification	A-1
Hardware & Power	A-1
Interfaces	A-4
Dataplane and Switching	A-6
μ Controller, Display & Clock	A-7
ENX Software Specification	A-8

Appendix EC EC Declaration of Conformity

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

List of Figures

Figure 1-1	ENX Application Mobile Backhaul	1-2
Figure 2-1	Rack Mount-Angles	2-2
Figure 2-2	Change Mount-Angles	2-3
Figure 2-3	ENX Bumper Assembly	2-4
Figure 2-4	ENX w/o Mount-Angles	2-4
Figure 2-5	ENX Ventilation Louvres	2-5
Figure 3-1	ENX Block-Diagram	3-2
Figure 3-2	ENX-F Front-View	3-3
Figure 3-3	ENX-F Front: Management & Status	3-4
Figure 3-4	ENX-F Front: LINE & LAN Interfaces	3-6
Figure 3-5	ENX-F Front: Clock Interfaces	3-7
Figure 3-6	Ethernet-Pinout R45 Connector	3-12
Figure 3-7	1PPS-Waveform	3-15
Figure 3-8	ENX-F Rear-View	3-16
Figure 4-1	Provider VLAN Tagging Diagram	4-6
Figure 4-2	P-VLAN configuration	4-7
Figure 4-3	MEF: EPL Diagram	4-8
Figure 4-4	MEF: EVPL Diagram	4-9
Figure 4-5	MEF: EP-LAN Diagram	4-9
Figure 4-6	MEF: EP-Tree Diagram	4-10
Figure 4-7	QoS Packet Flow	4-11
Figure 4-8	QoS Priority-Sticker	4-13
Figure 4-9	QoS Queue-Sticker	4-14
Figure 4-10	Ingress Limiter Selection (per Port)	4-16
Figure 4-11	CIR & CBS	4-19
Figure 4-12	Clock distribution in traditional Ethernet	4-23
Figure 4-13	Clock distribution in Synchronous Ethernet	4-24
Figure 4-14	Block Diagram for Synchronous Ethernet	4-26
Figure 4-15	Clock Quality Level distribution within the ENX	4-27
Figure 4-16	T4ab Driver	4-29
Figure 4-17	PTP Devices	4-30
Figure 4-18	Block Diagram for PTP	4-32
Figure 4-19	PTP Analysis: Offset	4-33
Figure 4-20	PTP Analysis: Path Delay	4-34

Figure 4-21	Management Protocol Stack	4-35
Figure 4-22	TACACS+	4-38
Figure 4-23	File-Transfer	4-45
Figure 4-24	Acknowledge of Alarms	4-53
Figure 5-1	Login Screen	5-2
Figure 5-2	Web-GUI's Appearance	5-3
Figure 6-1	The SNMP ax-MIB Tree (1.3.6.1.2.4.1.31507)	6-4
Figure 7-1	SSH-connection using User-Name and Password	7-2
Figure 7-2	SSH-connection using Global SSH-Password	7-2
Figure 7-3	Secure Shell - Public Key	7-3
Figure 7-4	SSH-connection using SSH-Key (Direct Login)	7-4
Figure 7-5	SSH-connection using SSH-Key (Connection Key)	7-5
Figure 7-6	PuTTY SSH-Connection.	7-6
Figure 7-7	Secure Shell	7-7

List of Tables

Table 0-1	Effects of Cleaning Liquids	0-4
Table 1-1	Order Matrix	1-4
Table 1-2	Accessories (Cables)	1-4
Table 1-3	Accessories SFPs.	1-5
Table 2-1	Ambient Conditions.	2-2
Table 2-2	ENX-F Front-View.	2-6
Table 2-3	LED Start-Up.	2-6
Table 3-1	Pin-assignment Control Port (RS232).	3-8
Table 3-2	Standards	3-9
Table 3-3	Ethernet Standards.	3-13
Table 3-4	Pin-assignment Control Port (RS232).	3-16
Table 3-5	Pin-assignment Alarm Connector	3-17
Table 3-6	Outlines AC Mains Connector.	3-17
Table 3-7	DC-Input Connection	3-18
Table 4-1	Behaviour for Untagged Packets on LAN-port 1	4-4
Table 4-2	Behaviour for Tagged Packets on LAN-port 1	4-4
Table 4-3	Behaviour for Untagged Packets on LINE-port.	4-5
Table 4-4	Behaviour for Tagged Packets on LINE-port.	4-5
Table 4-7	Settings Auto-Negotiation	4-47
Table 7-1	ENX CLI Hot Keys	7-10
Table 7-2	CLI Command CONFIG	7-11
Table 7-3	All other CLI Commands.	7-14
Table 7-4	Menu Indicators and corresponding CONFIG Commands	7-15
Table 7-5	Special CONFIG Commands	7-18
Table 7-6	CLI Short-cuts	7-18
Table 7-7	CLI Quick Reference.	7-19
Table 7-8	Example for SSH-Script	7-21
Table A-1	Physics and Environment	A-1
Table A-2	Security and EMC	A-2
Table A-3	Power Supply	A-2
Table A-4	Power Saving	A-3
Table A-5	Number of Interfaces	A-4
Table A-6	Technical Data of the Interfaces	A-4
Table A-7	Technical Data Dataplane	A-6

Table A-8	Display Functions	A-7
Table A-9	μController and Clock	A-7
Table A-10	Technical Data of the ENX - Software	A-8
Table A-11	Management & Security	A-9

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 ensuring that the procedures are performed safely. You must follow all caution notes ensuring 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, 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 preventing 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 preventing 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.

- 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.

Fiber 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 fiber optics and Laser Class 1 components:

WARNING: Do not look into the fiber optic output. Looking into the fiber 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 fiber optic cables while power is applied. Disconnecting the fiber 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 must be shielded and designed in accordance with proper EMI techniques ensuring 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 GmbH is certified according DIN ISO 9001:2000.

This product is manufactured according to the arcutronix GmbH quality standards.

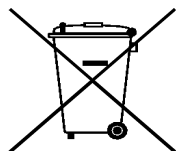
Repair

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 handed 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 according 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 50082-2 (Electromagnetic Immunity for heavy industry).

Instructions to User

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

Electromagnetic Emissions Statements

To achieve satisfactory EMC performance, all interface cables 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.

ENX Description

General

The ENX - Synchronous Ethernet Network Termination is a smart and versatile access network device for Ethernet access links and expanded services, such reducing operating expenses and improving margins. It offers Synchronous Ethernet (SyncE) and Precision Time Protocol (PTP; [IEEE 1588]), which supports expanding provider's clock-domain till the end-customer.

Its functions cover current and future access network requirements and it enables efficient solutions through easy configuration, test and monitoring interfaces.

ENX implements a fully managed demarcation function between customer network and service provider network. It monitors end-to-end connectivity and SLAs via its integrated test functionality.

ENX can derive SyncE from all ports and fulfils ITU requirements for jitter, wander and hold-over. For [IEEE 1588] it can operate as Ordinary Clock (OC) and Boundary Clock (BC). It provides accurate distribution of the PTP protocol across multi-port networks. As boundary clock it may be slaved to a master on one port and act as master on all other ports.

ENX offers independent interface and service control with integrated throughput test functions according to [IETF RFC 2544] (benchmark for network interconnect devices).

It incorporates Ethernet operations management according to Y.1731 (OAM functions), 802.1ag and 802.3ah (EFM), configuration management via HTML browser, via SNMP and SSH.

Application Areas for the ENX

The main application for ENX-F is terminating a fibre-based provider's network. The synchronisation feature makes it perfectly fitting for mobile back-hauling of the 4G LTE standard. Realization of mobile back-hauling for next generation of eNodeB (LTE). The synchronous feature supports the extending demand for clock accuracy and phase alignment.

Also as a Carriers-Carrier solution the ENX-F offers a wide feature-set to generate new and continuing revenue.

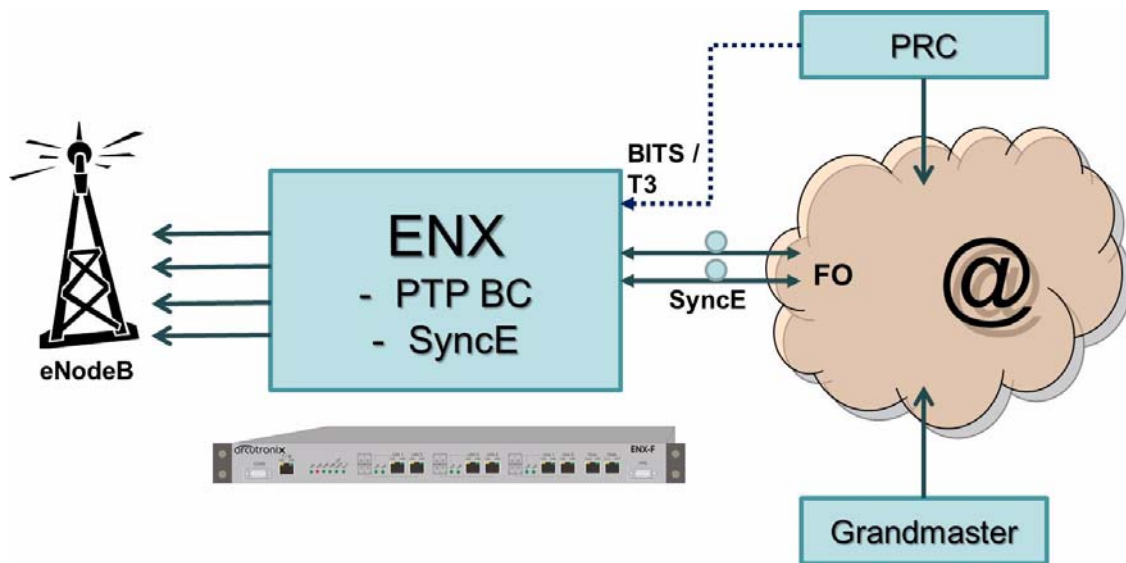


Figure 1-1 ENX Application Mobile Backhaul

ENX Functions at a Glance

The ENX - Synchronous Ethernet Network Termination offers the widest bunch of features a network termination brings into the provider's switched network. It does not only offer state-of-the-art packet handling and forwarding but also a set of protocols for maintenance and supervision. The onboard agent capability makes it easy to integrate the ENX into provider's network management system.

ENX incorporates the following features:

Synchronization

- ENX brings synchronisation to the edge of provider's network
- ITU-T G.8261 etc., G.823; [ITU-T G.8261], [ITU-T G.823]
- IEEE 1588v2 (PTP); [IEEE 1588]
- BITS (T3) input
- 1pps and T4 output for sync of slave devices

Switching

- Jumbo Frames (>10k) supported
- Link aggregation by LACP
- Functions cover current and future access network requirements
- Implements a fully managed demarcation function between customer network and service provider network
- Fibre and copper Ethernet ports

- Offers built-in independent interface and service supervision with integrated throughput test functions (acc. [IETF RFC 2544])
- Connectivity Fault Management

Management

- Network management for monitoring and management
 - HTML based WEB-GUI,
 - Built-in SNMP-agent and
 - SSH (CLI)
- In-band management capability

Two management interfaces are available. One is 10/100BaseT (RJ45) front-access, while the other is the in-band port via LINE-interface(s).

Housing and Power Supply

- Fan less solution at Rack-montage and Desktop Units
- Redundant AC (110/230V) and DC power supply
- Compact design: 19"/1RU ("Pizza Box")

Alarm Conditions and Relay

Alarm conditions can be detected depending on the settings made in the control software. The ENX monitors its power supplies. If there is a failure detected the ENX sets an alarm. When alarm condition is reached, several action (can) take place:

- Alarm-LED is ON,
- Alarm-Relay is closed,
- SNMP-trap is send out (trap receiver must be configured correct!).

Order Information

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

For the time being, the ENX-F is the sole member of ENX - Synchronous Ethernet Network Termination family.

Table 1-1 Order Matrix

Art.- No.	Short Name	Description
1102-1001	ENX-F	Synchronous Ethernet NT: <ul style="list-style-type: none">• 2x GbE (1000BaseSX/LX/ZX/BX), pluggable SFP modules (no modules included);• 4x 10/100/1000BT Combo-port (1x SFP and/or 1x RJ45);• 3x Clock interfaces (1x T3-input (BITS)/ 1x T4-output/ 1x 1pps);• MGMT via 1x 10/100BaseTx (RJ45), 1x RS232 (D-Sub9),• 1x Alarm-Contact;• Jumbo frames (>10000Bytes);• 19" chassis, 1RU;• AC (230V) and DC (-48V).

Accessories

Cables

Table 1-2 Accessories (Cables)

Art.- No.	Short Name	Description
0500-001	PC-E	Power cord, European plug.
0500-002	PC-B	Power cord, Great Britain plug.
9500-0101	DCX-DB9 M-DB9F	Digital Cable: D-Sub9 male to D-Sub9 female; used for VT100-Management via an RS232 (D-Sub9 conn.) interface.

SFPs (Small Form-factor Pluggable)

The ENX 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 ([INF-8074i]) between competing manufacturers.

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

All SFP ports are compliant with [INF-8074i] and must be connected to SFP modules that are class 1 lasers and are compliant with [IEC 60825-1].

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.

ENX 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 ENX 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:

- ENX - Synchronous Ethernet Network Termination,
- Power Cord for AC-power supply,
- 2 Angles for 19"-rack mounting (already mounted),
- 4 Bumpers for desktop-usage,
- Short User-Information.

Preparing the Start-up

Before you switch on the device you need to check the operating conditions and install the ENX on a proper location (rack-mount, desktop etc.).

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 ENX, are shown in Table 2-1.

Table 2-1 Ambient Conditions

Operating Temperature	-25°C to +55°C
• hardened version	• -40°C to +70°C
Max. Relative Humidity (non-condensing)	<100% (30°C)
Input Voltage AC	110 to 240 VAC
Input Voltage DC	-36 to -72VDC
Power Consumption (w/o SFP)	< 16 VA

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.

Mounting Options

Rack-Mount 19"-Rack

The ENX can be mounted into a 19"-rack. For this purpose, a mounting angle is pre-assembled on the unit. Use them to fix the unit as usual



Figure 2-1 Rack Mount-Angles

The FO installation requirements can make it necessary to place the ENX a little more to back of the rack. This is to gain more space between front and door to fit the fibre optics cable. For this reason, the mount-angles can be moved more to the front. To do

this, turn the ENX (1), release the 6 screws on both sides (2), replace the angles (3) and tighten the 6 screws again (4).

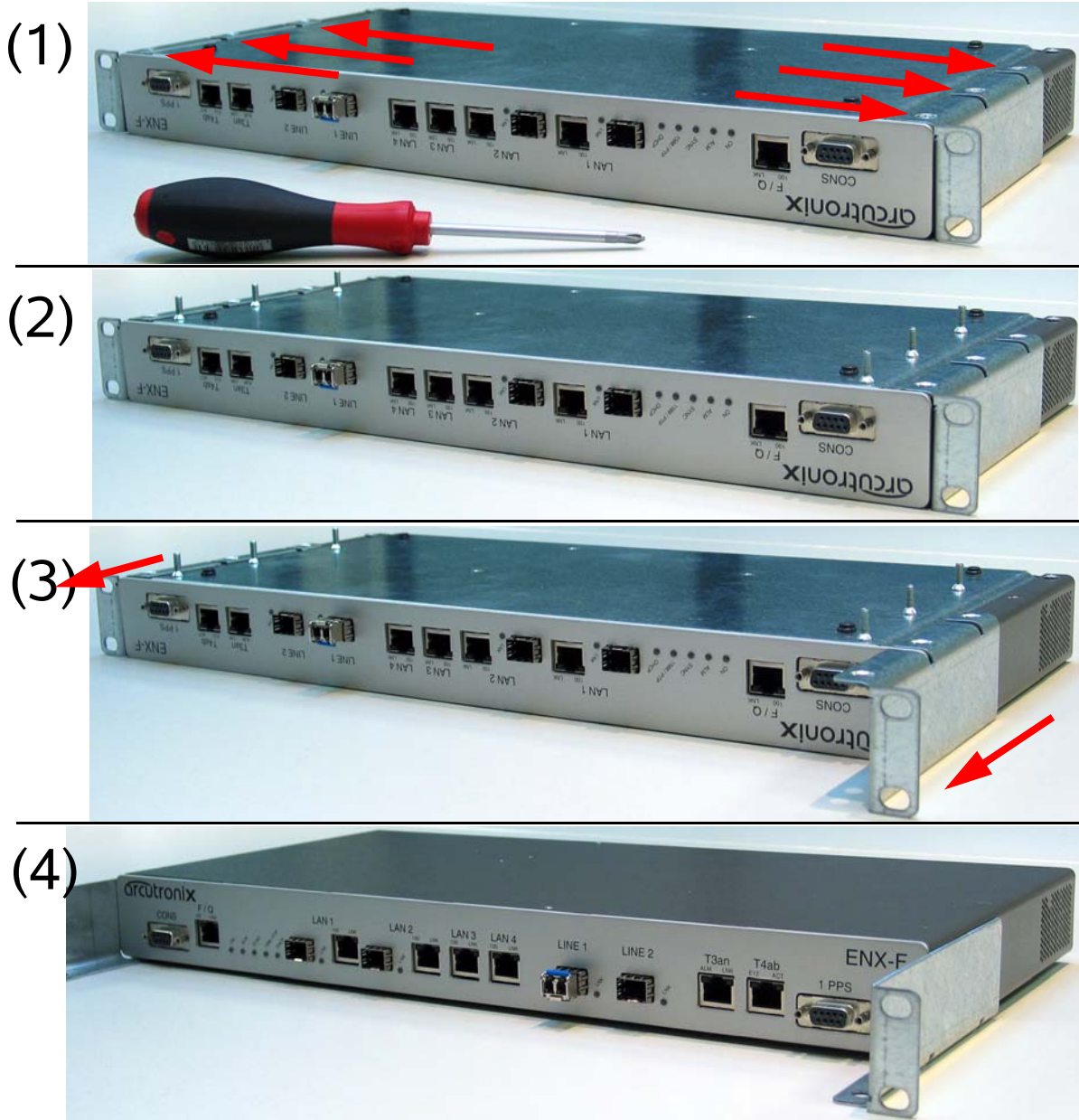


Figure 2-2 Change Mount-Angles

Desktop Usage

For usage as desktop-device, the 4 bumpers should be fixed on the bottom side of the unit.



Figure 2-3 ENX Bumper Assembly

If not needed, the pre-mounted angles for rack installation can be removed. See Chapter 2, Rack-Mount 19"-Rack for details about removing the angles. (Just do step (1), (2) and (4).) The result can be seen below:



Figure 2-4 ENX w/o Mount-Angles

Airflow Requirements

There are no fans installed inside the ENX to cool the unit, but the passive air-flow (thermal) is sufficient in the defined operating conditions. On both sides of the unit, there are ventilation louvres, which should not be covered when the device is installed.



Figure 2-5 ENX Ventilation Louvres

Start-up of the ENX

Switching on the Device

The ENX does not have any power switch. If power (AC and/or DC) is supplied to the unit, it will start. The ENX does have 2 redundant power input: AC (110 / 230 VAC) and DC (48 or 60VDC). The power input can be used independently or in redundant mode. If AC is available, the AC-input is preferred.

Power-Up Sequence

After providing power to the ENX, the ENX will be powered up. The start-up will take several seconds, while internal SW is started and some tests are done to verify the ENX is not damaged and proper operation can be guaranteed.

The power-up sequence is indicated by special behaviour of the LEDs in the front-plate. After finishing the start-up, the LEDs will operate “normal” and indicate status and alarms of the unit, as written in this manual.

The special behaviour of the LEDs allow to user to

1. check, whether all LEDs or operating well and
2. see when the unit's start-up is finished and the ENX is operational.

NOTE: After finishing the start-up, the unit is operational in meaning of data transmission and all services are running. The management access will be started a little later, as additional tasks have to be started here for.

LED Start-Up

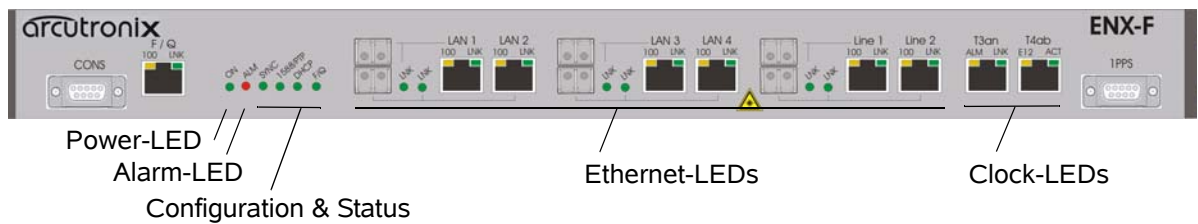
In the front plate, four categories of LEDs are grouped together:

Getting Started
Start-up of the ENX

- Power-LED (green)
- Alarm-LED (red)
- Configuration 6 Status LEDs
- Ethernet LEDs, build-in RJ45 connectors and beside SFPs
- Clock LEDs, build-in RJ45 connectors

See the following picture for the different categories:

Table 2-2 ENX-F Front-View



The flow of the LED groups during start-up is depicted in the following table:

Table 2-3 LED Start-Up

State	ON-LED	Alarm-LED	Config & Status-LEDs	Ethernet-LEDs	Clock-LEDs
S1 "Boot-Seq.", (after Power On) Duration: ~5sec	LED is blinking fast	LED is ON	LEDs are ON	All LEDs are OFF	LEDs are ON
S2 "Boot-Finished" Duration: ~2sec	LED is ON	LED is ON	LEDs are OFF	All LEDs are OFF	LEDs are OFF
S3 "Start Linux" Duration.: ~1 sec	LED is blinking slowly	LED is ON	LEDs are ON	All LEDs are OFF	LEDs are ON

Table 2-3 LED Start-Up (continued)

State	ON-LED	Alarm-LED	Config & Status-LEDs	Ethernet-LEDs	Clock-LEDs
S4 “Test-Eth-LEDs	LED is blinking slowly	LED is ON	LEDs are ON	All LEDs of Port 2 are ON	LEDs are ON
O1	LED is ON	Normal operation = Alarm status of the card/rack is shown.	Normal operation.	Normal operation = Link and traffic of Ethernet-connections are shown.	Normal operation.

Note: Sx = Start-up state; O1 = Operational State reached.

Configuration Access

After successful start-up process, the unit is ready for communication and configuration. A default setup is available as factory settings, but special settings can be done via several ways and methods. These will be depicted hereafter. All configuration settings are made by using the management I/Fs. For the system configuration you can choose one of the following configuration methods:

Local and Remote IP-Access

The ENX has one Ethernet I/F, called “F/Q-Interface”. The “F/Q” can be used for local and/or remote access. Local access means the direct connection of a Laptop and/or PC, while remote access is via LAN or WAN connection from somewhere else.

Remote access allows the user to communicate with the ENX and maintain the chassis via a long distance. The SFP-port or other Ethernet-based transmission systems can be used to hub the ENX into your local environment. The ENX can easily be integrated in umbrella management system or the EM-function can be used, just as if the user is standing in front of the unit.

The “F/Q” port supports the operation as F-interface as well as Q-interface. F-interface suits perfect for Local Access, while the Q-interface mode is perfect for Remote Access. The configuration can be seen by the F/Q-LED in the front. By default

- F/Q is configured as F-interface (IP = 192.168.1.100).

The “F/Q” port is a 10/100BaseT port, supporting Auto-Negotiation and Auto-Cross-Over.

Inband IP-Access

The ENX has the capability to be managed via the LINE-ports. In-band IP-access allows the user to use a LINE-port not only for payload transport but also for management. The ENX can easily be integrated in umbrella management system or the EM-function can be used, just as if the user is standing in front of the unit.

1. For in-band management the administrator's station must have IP-link to the ENX. This can be done in the same subnet or via IP-routers in the network.
2. The ENX in-band (line-) port is configured to act as a DHCP client. Via DHCP an IP-address and all the required routing information will be advertised to the in-band port. To use this feature, a DHCP server must be available in the network. If no DHCP server is available, the in-band IP-address must be set via local access (see above). The default IP-address for in-band management is 192.168.1.100 (without DHCP-server available).
3. The ENX in-band (line-) port is configured to use VLAN-tagging for clear differentiation from the user's payload traffic. The default VLAN-ID for in-band management traffic is 4094.

Serial Access

The ENX has the capability to be managed via serial access ("CONS"-port), using the RS-232 (EIA-232) interface of your Laptop / PC. A Command Line Interface (CLI) is offered to the user.

The serial port is configured to operate as a DCE (Data Communication Equipment), which fits as counterpart to your PC's serial DTE-interface (Data Terminal Equipment). A standard serial cable is sufficient for the communication.

The parameters for the RS-232 are: 115200, 8N1

- 115.2kBaud, 8 Bits, No Stop-bit, 1 Parity-Bit.

Configuration Methods

Web Access

A Web-based GUI is available to configure and maintain the ENX locally and/or remote. All IP-based access methods can be used.

1. Connect your PC / Laptop / LAN via any Ethernet cable (cross-over or straight) to the port.
2. The ENX F/Q-port is configured to act as an DHCP-server and will advertise the connected PC / Laptop an IP-address in the same subnet, as itself (192.168.1.100/24). To use this feature, the PC / Laptop has to be configured as DHCP client. (See Chapter 4, DHCP and Manual Address Assignment for details.)
3. Open your standard internet browser (e.g. Firefox) and enter in the address field **192.168.1.100**. The html-based GUI will allow easy configuration settings.

SSH Access

Secure Shell or SSH is a network protocol that provides secure communication between two computers. If SSH is used correctly, no eavesdropping or tampering with your data is possible, unless you are under attack by an immortal miscreant with extraordinarily powerful computers. Typically, SSH is used to securely log in to remote machines in order to execute commands.

All IP-based access methods can be used.

See Chapter 7, SSH and CLI, for details.

Telnet Access

Telnet access is not supported. Please use SSH access for Command Line Access via TCP/IP.

SNMP Access

The ENX offers an on-board SNMP manager, which can be contacted by any available MIB-browser and/or SNMP manager. It supports SNMPv2c as well as SNMPv3 protocol, as defined by IETF.

As SNMP access is based on TCP/IP suite, the communication is possible via the F/Q-port as well as via the in-band access.

The TCP-settings are the same as written above for the other ways of access. An easy and quick setup is implemented. See Chapter 6, SNMP and MIBs, for details.

Command Line Interface

The CLI is a basic way to do configuration and maintenance. It is very simple in style and requires more knowledge about the device. On the other hand, CLI is very well suited for scripting and replicating configuration. The CLI is depicted in Chapter 7, SSH and CLI.

Chapter 3

Hardware & Interfaces

This chapter provides information about the hardware of ENX - Synchronous Ethernet Network Termination. This consist of block-diagram and a detailed description of all external interfaces and function indicators.

The ENX-F 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.

Hardware Overview

Block-Diagram

The block-diagram shows the principal parts and functions of the ENX-F. The main blocks are shown and their logical connections are presented as lines in between.

The ENX-F can be divided into five functional blocks:

- Data-Plane,
- Control-Plane,
- Power,
- SyncE,
- PTP / 1588.

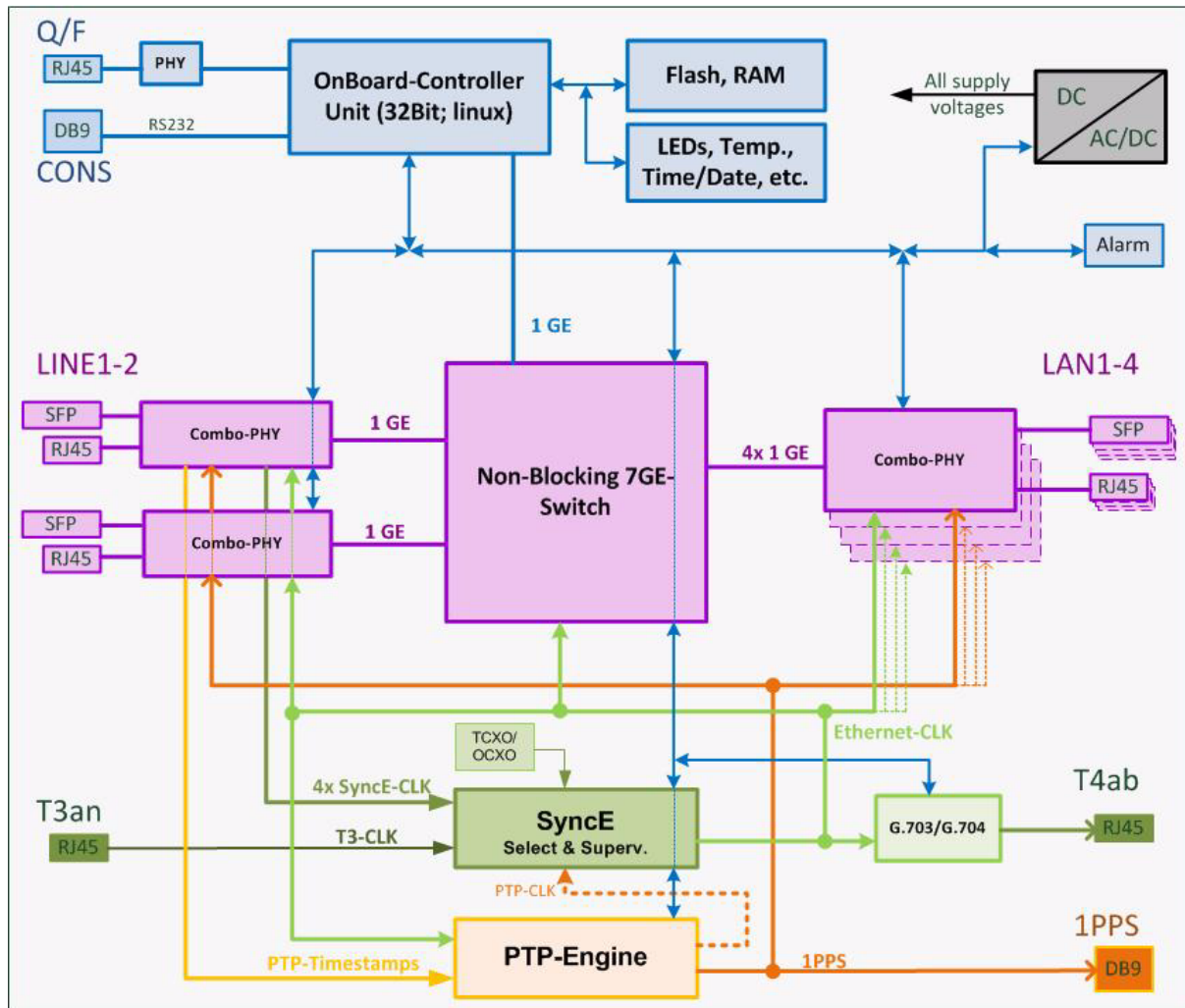


Figure 3-1 ENX Block-Diagram

Figure 3-1 gives an overview to the functional blocks. In the middle one finds the non-blocking Ethernet-switch, which is the heart of the device. Six (combo-) PHYs compose the physical interfaces to LINE- and LAN-interfaces. Each combo-port can be used either for Copper or Fibre Optic infrastructure.

Two Ethernet LINE ports and four Ethernet LAN ports use SFP/Copper combo-ports that can operate as fibre optic SFP-based interfaces or electrical RJ45 interfaces. The SFP/Copper combo-ports are auto detecting and can accommodate a wide range of Ethernet SFP transceivers, allowing service providers to seamlessly connect customers located at different distances from the device.

The OnBoard-Controller configures and maintains the device. It permutes any changes in configuration, reports errors and alarms. The OBC can be accessed via 3 ways:

- Out-of-band management I/F, called “F/Q-Interface”,

- RS-232 serial interface, called “Console”,
- In-band management I/F, accessible via LINE-interfaces.

The power-block generates all required supply voltages out of the AC or DC input. Both inputs are monitored and in case of failure an alarm can be raised.

The SyncE-block does provide the clock-source for the data-plane. It can select one of several sources as reference:

- The recovered clock from the LINE-interfaces,
- T3-clock, which is a 2.048MHz reference clock,
- BITS-clock, which is a 2.048Mbps HDB3-signal (not available in all variants!),
- Onboard 4.6ppm oscillator (either TCXO or OCXO),
- PTP-clock derived from the PTP clock information (not available in all variants!).

The SyncE-block does provide a reference-output at the T4ab-interface, which can be either 2.048MHz (“T12”-mode) or 2.048Mbps HDB3-signal (“E12”-mode).

The PTP / 1588-block synchronizes the unit to a reference clock (Grand-Master) in the network. Incoming and outgoing PTP-packets get a time-stamp inside the PHYs to achieve best results. A 1PPS-signal (peak-per-second) is used to synchronize all PHYs and an external device (via D-Sub9 connector, “1PPS”).

ENX-F Front Panel

The ENX-F has almost all the connectors and status indicators in the front panel of the unit. This makes it easy to install and changes in connection can be done without removing the unit from rack. The status indicators are all low-power LEDs, which are available in red, yellow and green.

The interface LEDs are labelled, so it is easy to use and understand the intent.

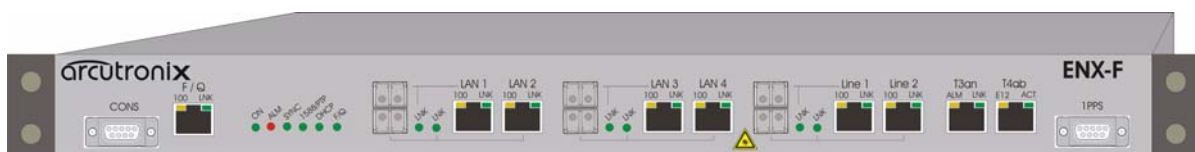


Figure 3-2 ENX-F Front-View

Figure 3-2 shows the complete front. On both sides, the mounting angles for the rack-mounting are visible. The front can be separated in 3 parts, which will be depicted in more details, hereafter:

- Management & Status area,
- LAN & LINE area,
- Clock area.

Management & Status Area

Most to the left of the front panel the access ports for management and the main status LEDs are located. A D-SUB9 connector for serial interfacing followed by the out-of-band management IP-port are building the access points for configuration and supervision. See the following picture and table for details.

The pinning and other electrical specifics are given later in this chapter.



Figure 3-3 ENX-F Front: Management & Status

CONS	Console-Port for EIA-232 access. It is a DCE port with 115200, 8N1 setting.
F / Q	Out-of-band Management port. It can either be in Q- or F-interface mode. Note: One can easily change the setting via the serial port: Enter "Q" or "F" after login to change the mode.
100 (in RJ45)	(Negotiated) Speed of the F / Q -interface. On = 100Mbps (100BaseT). Off = 10Mbps (10BaseT) or IF disabled or No Link detected.
LNK (in RJ45)	Link status indicator of the F / Q -interface. On = Link detected. Off = No Link detected or IF disabled.
ON	ON-LED, which indicates that the unit is operable. On = Unit is operable. Flashing (~10Hz) = Start-up and boot-process. Off = Power down or temperature shut-down.

ALM	Alarm-LED. Lit, when an alarm state is active. On = Alarm active. On (and all others Off) = Temperature shut-down. Unit waits for cooling down to restart. Off = No alarm active.
SYNC	Indicator for synchronization status of the device. On = (internal) PLL locked onto reference. Blinking (1Hz) = PLL locked onto internal oscillator (TCXO or OCXO) @ +/- 4.6ppm. Blinking (4Hz) = PLL in pre-lock phase.
1588 / PTP	Indicator for Precision Time Protocol ([IEEE 1588]). On = Unit synchronized to PTP-Grandmaster (GM). Accuracy +/- 50ns. Blinking (1Hz) = Unit synchronized to GM. Accuracy +/- 1µs. Blinking (4Hz) = In contact to GM, but no synchronization achieved, yet. Off = PTP is disabled.
DHCP	Indicator for IP-address assignment via DHCP to the unit. On = Unit has been assigned an IP-address via DHCP. Blinking (1Hz) = DHCP-server is found and unit waits for IP-address assignment. Blinking (4Hz) = No DHCP-server found, yet. Off = IP-address assignment via DHCP is disabled.
Q / F	Indicator about the mode of the F/Q-interface. On = F/Q interface is in Q-mode. Off = F/Q interface is in F-mode.

LAN & LINE Area

This is the access area for the user-links and uplinks. A user-port is called LAN, while an uplink is called LINE. 2x LINE ports and 4x LAN ports are available for usage.

Features of a LINE Port

A LINE-port can be source for SyncE, can be connected to a PTP-Grandmaster, and may carry in-band management traffic.

Features of a LAN Port

A LAN-port can be clocked with the SyncE and serve subsequent units, may be OC (master), if the unit is working in PTP-BC mode. A LAN-port can never carry in-band management and will never grant access to local access point.

Labels and LEDs for LINE and LAN Port

The pinning and other electrical specifics are given later in this chapter.

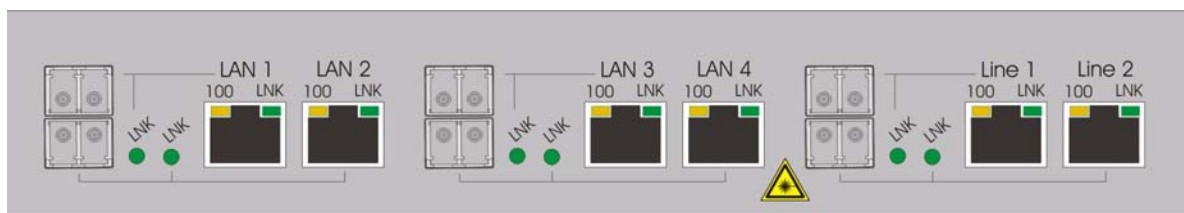


Figure 3-4 ENX-F Front: LINE & LAN Interfaces

LAN _i , $i = 1 \dots 4$	<p>These are the 4 LAN combo-ports. A combo-port consists of a RJ45-Copper Ethernet (10/100/1000BaseT) plus an 1000Base-X SFP-port. Only one of the two slices can be used: Either Copper or Fibre.</p> <p>Warning: Do not place an SFP and a CAT-cable in parallel in one combo-port. This will lead to errors in transmission!</p>
LINE 1, LINE 2	<p>These are the 2 LINE combo-ports. A combo-port consists of a RJ45-Copper Ethernet (10/100/1000BaseT) plus an 1000Base-X SFP-port. Only one of the two slices can be used: Either Copper or Fibre.</p> <p>Warning: Do not place an SFP and a CAT-cable in parallel in one combo-port. This will lead to errors in transmission!</p>
100 (in RJ45)	<p>(Negotiated) Speed of the Copper-part of the combo-port.</p> <p>Blinking (1Hz): 1000Mbps (1000BaseT).</p> <p>On = 100Mbps (100BaseT).</p> <p>Off = 10Mbps (10BaseT) or IF disabled or No Link detected.</p>

LNK (in RJ45)	Link status indicator of the Copper-part of the combo-port. On = Link detected. Off = No Link detected or IF disabled.
LNK (beside SFP block)	Link status indicator of the Fibre-part of the combo-port. On = Link detected. Off = No SFP plugged or No Link detected or IF disabled. Blinking (1Hz) = Plugged SFP detected, but no link yet. Note: The SFP-LNK LED does blink, when a SFP is detected. This is an indicator, that no CAT-cable must be plugged to this combo-port.

Clock Area

On most right side of the unit all the clock interfaces are placed. Reference-input for SyncE (“T3an”), which is a 2.048MHz clock or, in some variants, a 2.048Mbps HDB3 coded signal. The derived SyncE clock can be tapped from the “T4ab” output. The T4ab can be configured to be either 2.048Mhz or 2.048 Mbps HDB3 signal, carrying SSM messages. The 1PPS interface is synchronized to a PTP-grandmaster and gives an edge every second to synchronize or test purpose.

The pinning and other electrical specifics are given later in this chapter.

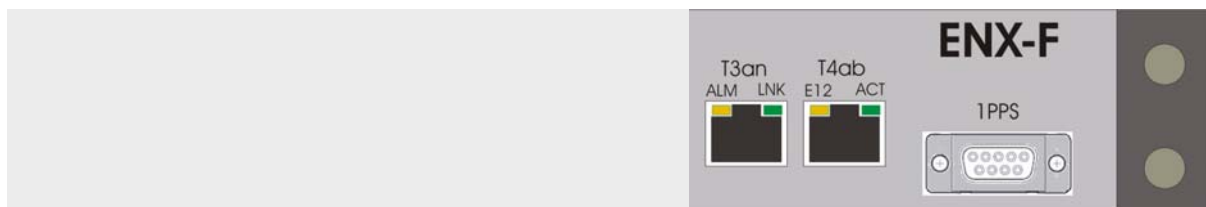


Figure 3-5 ENX-F Front: Clock Interfaces

T3an	Synchronization input according [ITU-T G.703].
ALM	Alarm-LED for the T3an interface. On = T3an enabled and no link detected. Blinking (1Hz) = Short circuitry detected on the link. Off = Input signal detected or IF disabled.
LNK	Link-status of the T3an interface. On = T3an enabled and link detected. Off = No link detected or IF disabled.

T4ab	Synchronization output according [ITU-T G.703].
E12	Mode indicator for the T4ab interface: On: E12-mode = 2.048Mbps, HDB3 coded. Off: T12-mode = 2.048MHz square wave.
ACT	Indicator that the T4ab output is activated via management system. If not used, it can be disabled. On = T4ab enabled and link detected. Blinking (1Hz) = Short circuitry detected on the link. Off = No link detected or IF disabled. Note: Short circuitry detection does not work in T12-mode!
1PPS	1 peak-per-second output.

Console Port

For the ENX, the serial control port gives serial access to the device. The serial port is according ANSI EIA/TIA-232-F-1997 and operates with the following settings:

- Baud rate is 115200 kbps, 8 data-bits, no parity bit, 1 stop-bit: 115200, 8N1

The console port is configured to act as a DCE (data circuit-terminating equipment), which is the natural counterpart of a PC's serial port, which is working as DTE (data terminal equipment).

Pinning

The pin-assignment for the console port (DCE mode) is as follows:

Table 3-1 Pin-assignment Control Port (RS232)

	Pin	Assignment
D-Sub9, female:	1	-
	2	RXD (output)
	3	TXD (input)
	4	DTR (input)
	5	GND
	6	-
	7	RTS (input)
	8	CTS (output)
	9	-



The connector is connected to Shielded Earth.

Note: The ENX operates in DCE mode, so “RXD” is an output, while “TXD” is an input!

Note: You have to connect the DTR signal (Data Terminal Ready) on Pin4 as otherwise the communication will not work!

RS232 Connection Cable

A standard RS-232 “null-modem” cable can be used to connect your PC with the ENX. It must be full equipped cable, with all 9 signals connected (e.g. DCX-DB9M-DB9F [9500-0101] from arcutronix).

Q / F Interface

The ENX does have one out-of-band management interface called “F/Q”. F/Q-interface is a pure copper based Ethernet port with a maximum speed of 100Mbps. The F/Q-interface supports Auto negotiation and auto crossover.

The name of F/Q-interface derives from the two different modes in which this interface can be operated: Q-mode and F-mode. The different behaviour is depicted in “IP-Addressing” on page 4-41 and will not be written here.

In factory default, the F/Q-interface operates in F-mode, which is local access mode with DHCP server activated. This makes it easy to connect a craft person’s PC to the device for configuration.

The default IP-address of F/Q-interface is: 192.168.1.100.

10/100BaseT (RJ45)



The F/Q-interface has indicators to give information on the link state and activity (LNK) and speed (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 “Copper Ethernet Port” on page 5-42. The data rate is either 10 Mbit/s or 100 Mbit/s. The protocol is according to [IEEE 802.3] 10BaseT or 100BaseTX.

Table 3-2 Standards

Item	Values
Standards:	IEEE 802.3, 801.1 p&Q
Ports:	1x 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 s:	RJ45 8-pin

The connector is a RJ45 plug with 2 LEDs, which indicate speed, link and activity. The pin-assignment of the RJ45 is as follows:

RJ45	Pin	Assignment
LED:	1	TD+
	2	TD-
	3	RD+
	4	-
	5	-
	6	RD-
	7	-
	8	-

LED	Label
	100
	LNK

The diagram shows a top-down view of the RJ45 connector. The yellow LED is on the right side, labeled '100', and the green LED is on the left side, labeled 'LNK'. The pins are numbered 1 to 8 from top to bottom.

- The yellow LED (right, '100') indicates the speed of the interface. The speed may vary due to configuration settings and auto-negotiation process.
- The green LED (left, 'LNK') indicates, when the link is established and packets are transferred. It is blinking when the interface is receiving or transmitting Ethernet frames.

Auto-Cross-Over

The interface 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 ensuring 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 negative effect on the reliability of the data transmission.

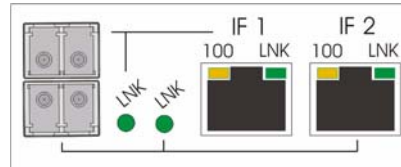
Combo-Ports

Six combo-ports are the data-plane interfaces of the ENX. A combo-port can operate as fibre optic SFP-based interface or electrical RJ45 interface. The SFP/Copper combo-ports are auto-detecting the SFP option.

All SFP ports are compliant with [INF-8074i] and must be connected to SFP modules that are class 1 lasers and are compliant with [IEC 60825-1].

The six combo-ports are grouped to 3 blocks each with 2 combos:

- LAN 1 + LAN 2
- LAN 3 + LAN 4
- LINE 1 + LINE 2



Each combo-port consist of

- 1x SFP-slot for 1000Base-X,
- 1x LNK-LED for SFP-link and activity,
- 1x RJ45-connector for 10/100/1000BaseT,
- 1x Speed-LED (in RJ45) to show speed of copper port,
- 1x LNK-LED (in RJ45) to show copper link and activity.

The combo-port can only use one of the two bonded interfaces: Either the copper port or the fibre (SFP-) port. If a SFP is detected by ENX, this will be signalled by slowly blinking of the SFP Link-LED. In this case, the copper port may not be used!



WARNING: Do not place an SFP and a CAT-cable in parallel (at the same time) in one combo-port. This will lead to errors in transmission! This is always true, even when one part of the combo is in “do-not-use” status.

Combo-ports can be configured by management to disable the auto-detection of SFP and they can be fixed configured to support only fibre or only copper. In this case only the configured medium is supported and the other slice is not usable.

NOTE: Even when the combo-port is locked-up to one medium (fibre or copper), do not place SFP and copper-cable in parallel on a combo-port.

Ethernet Loop-Back

All combo-ports do support Ethernet loop-back for a cost-effective solution of Service Level Agreement (SLA) verification and performance testing. The Ethernet loop-back can be invoked either by management or by EFM OAM protocol.

NOTE: To avoid uncertain behaviour and to keep up layer 2 management all time, the Ethernet loop-back does not loop Layer 2 Control Protocol (L2CP) frames. See chapter “L2CP Frames Handling” on page 4-7 for more details on L2CP.

1000BaseTX (RJ45)

The ENX provides six copper Gigabit Ethernet interfaces as combo-ports. Separate indicators give information on the Link state (LNK) and activity (ACT) of the interface. 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. 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.

NOTE: If the ENX detects an SFP in a combo-port, the adjacent copper-port will be disabled! If a SFP is detected the LNK-LED of the SFP will blink until the FO-link is established.

RJ45 Connector

The connector is a RJ45 plug with 2 LEDs, which indicate speed, link and activity. The pin-assignment of the RJ45 is as follows:

RJ45	Pin	Assignment
LED:	1	BI_DA+
	2	BI_DA-
	3	BI_DB+
	4	BI_DC+
	5	BI_DC-
	6	BI_DB-
	7	BI_DD+
	8	BI_DD-


100	LNK
	
8	1

Figure 3-6 Ethernet-Pinout R45 Connector

The integrated LEDs in the RJ45 connector, do have the following behaviour:

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

Auto-Cross-Over

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 ensuring 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.

1000Base-X (SFP)

The ENX provides six fibre Ethernet interfaces as combo-ports. LAN 1 and LAN 2 can be equipped with an 100BaseFX or an 1000BaseFX module according the SFP industry standard. LINE 1, LINE 2, LAN 3 and LAN 4 can be equipped with an 1000BaseFX module according the SFP industry standard.

For each interface one indicator gives information on the link state and activity (LNK).

- The green LED ('LNK') indicate(s) that the optical link is established.
- If a SFP is detected in the SFP-slot and there is no link established, yet, the LNK-LED is blinking. This is to indicate that the copper port is disabled, as the SFP is plugged.

Standards

Table 3-3 Ethernet Standards

Item	Values
Standards:	IEEE 802.3, 801.1 p&Q
Data rate:	Copper Port: 10Mbit/s, 100Mbit/s or 1000Mbit/s auto negotiation, full- or half-duplex, bandwidth limitation Fibre Port: 1000Mbit/s auto negotiation, full- or half-duplex, bandwidth limitation
MTU	10240 Bytes (also selectable 1522 or 2048 Bytes)
Flow Control:	IEEE 802.3x, PAUSE frames

T3an & T4ab

The T3an and T4ab ports are synchronization interfaces of the ENX.


T3an

T3an is an input for clock reference to synchronize the unit to an external clock. If selected as source for the unit, the Ethernet physical layer will be synchronized to this clock.

T3an timing input has the following properties: 2.048Mhz, 120 Ohm unshielded, symmetrical, short-circuit proof. The interface corresponds to T12 according to [ITU-T G.703], Section 13.1 and 13.2. The jitter and wander tolerance applies to [ITU-T G.813] (8. Noise tolerance).

The connector is a RJ45 plug with 2 LEDs, which indicate an alarm and link. The pin-assignment of the RJ45 is as follows:

RJ45	Pin	Assignment
LED:	1	RD- (TIP)
	2	RD+ (RING)
	3	-
	4	-
	5	-
	6	-
	7	-
	8	Digital GND

ALM	LNK
	
8	1

- The yellow LED (right, 'ALM') indicates an alarm of the interface. This is normally a not established link, when the interface is enabled. When a short circuitry on the physical line is detected, the ALM-LED is blinking.
- The green LED (left, 'LNK') indicates, when the link is established.

T4ab

The T4ab is a reference output for subsequent devices. It is synchronized to the unit's Ethernet physical clock layer.


T4ab timing output has the following properties: 120 Ohm unshielded, symmetrical, short-circuit proof. The clock (or data-) rate is 2.048MHz.

Timing output T4ab supports two operating modes: T12 and/or E12, which is configurable by customer.

- In T12 mode, the signal complies with [ITU-T G.703], Section 13.1 and 13.2., which describes a 2,048MHz signal.
- In E12 mode it complies with [ITU-T G.703], Section 9.1 and 9.2., which describes a HDB3-coded 2,048Mbps data-stream. On top of this data-stream a multi-frame structure according to [ITU-T G.704] is inserted. This gives the possibility for sending messages to the peer.

The connector is a RJ45 plug with 2 LEDs, which indicate mode and active status. The pin-assignment of the RJ45 is as follows:

RJ45	Pin	Assignment
LED:	1	-
	2	-
	3	-
	4	RD- (TIP)
	5	RD+ (RING)
	6	-
	7	-
	8	Digital GND

E12	ACT
	
8	1

- The yellow LED (right, 'E12') indicates the mode of the interface. When the LED is on, E12 mode is enabled, otherwise it is T12.
- The green LED (left, 'ACT') indicates, when the interface is enabled. When a short circuitry on the physical line is detected, the ALM-LED is blinking.

NOTE: When T4ab is configured to T12-mode (2.048MHz), the interface can not detect any shorties or unconnected cables. This is only possible in E12-mode!

1PPS Interface

The 1PPS interface is for synchronization and test purposes. It is part of the PTP / 1588 block of the ENX. It generates one peak-per-second, which is derived from the Grandmaster's information. The 1PPS-output has the IEEE 1588-2008 phase accuracy at the UNI, which means the maximum permissible deviation is 20ns. The impedance is 50 Ohm, symmetrical. The 1 PPS output is short -circuit proof. The electrical specification is according to EIA-422/ ITU-T V.11 ([ITU-T V.11]).

The connector for the 1PPS-signal is a D-SUB9 female.

The waveform of the 1PPS-signal is shown in the following picture:

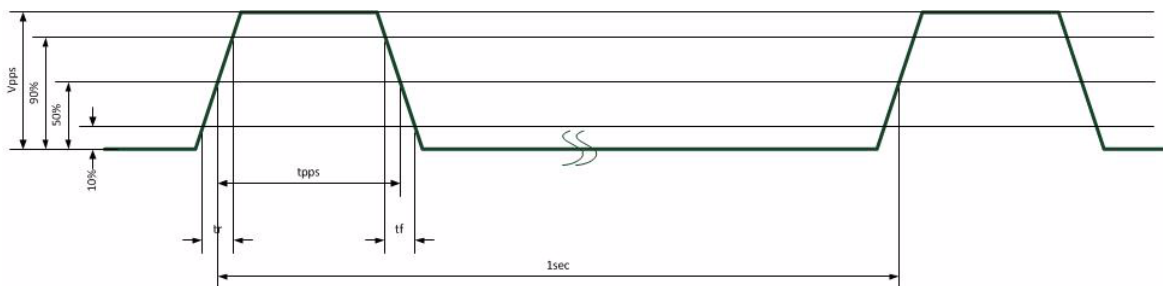


Figure 3-7 1PPS-Waveform

Parameter	Value	Comment
V_{pps}	2.48 V	Differential voltage of 1PPS-signal
t_{pps}	100 μ s	Duration of the 1PPS-signal's high pulse.
t_r	7ns	Rise-time of the 1PPS-pulse (10% to 90%)
t_f	7ns	Fall-time of the 1PPS-pulse (10% to 90%)

Pinning

The pin-assignment for the 1PPS-interface is as follows:

Table 3-4 Pin-assignment Control Port (RS232)

	Pin	Assignment
D-Sub9, female:	1	1PPS-A
	2	-
	3	-
	4	-
	5	-
	6	1PPS-B
	7	-
	8	-
	9	-

The connector is connected to Shielded Earth.

ENX-F Rear Side

On the rear side of the ENX-F the power connectors, an earthing bolt, the alarm relay contact, a reset push-button and the device-label are located.

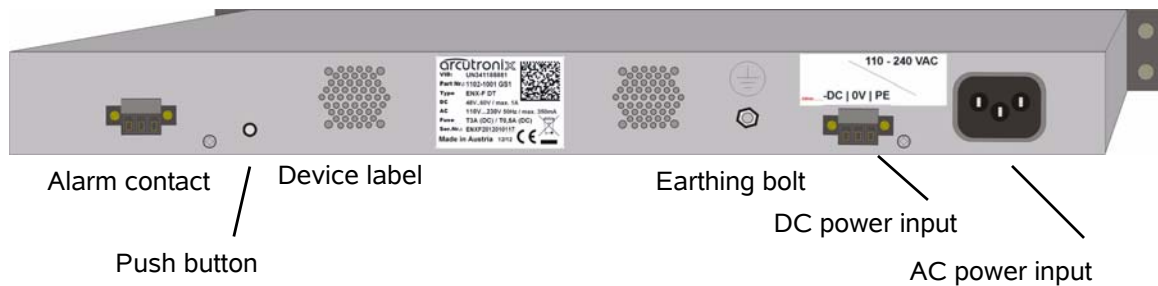


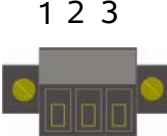


Figure 3-8 ENX-F Rear-View

Alarm Connector

An alarm connector is used in order to indicate an alarm of the system.

Table 3-5 shows the alarm connector settings.

Table 3-5 Pin-assignment Alarm Connector

	Normal status	Alarm status	Pin:	Connect to:
			1	Normally open "NO"
			2	Centre contact
			3	Normally closed "NC"

NOTE: The contact is galvanic separated. The contact rating allows a resistive load with max. 1 A, 30 V AC/DC.

Push-Button

This button is for future use. For the time being, there is no functionality bonded to the button.

Power Supply



While working with the system, always adhere to the appropriate safety measures for handling electronic devices. Read the power precaution in Chapter 0, **Power Precautions** carefully before using the device.

AC Power Supply

The ENX offer one AC power supply. It can operate at in a range of 110 to 240 VAC. The AC input is protected by an 1.0A fuse.

Table 3-6 Outlines AC Mains Connector



The device is to be operated at 115/230 V 60/50 Hz AC. Please check for appropriate line voltage before connecting any system to the mains.

The AC power supply can be operated in parallel to the DC power supply to achieve redundancy in case of failure of one power system.

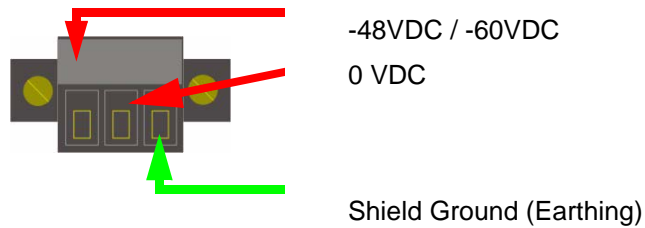
The availability of the AC Power Supply is permanently checked by the device. In case the AC input is less than 110VAC, an alarm can be raised. This alarm is called "AC Power Status".

DC Power Supply

The ENX offer one DC power supply. It can operate at in a range of -48 to -60 VDC (+/-20%). The DC input is protected by a 1.5A fuse.

Table 3-7 shows the right connection of the DC input connector.

Table 3-7 DC-Input Connection



The DC power supply can be operated in parallel to the AC power supply to achieve redundancy in case of failure of one power system.

The availability of the DC Power Supply is permanently checked by the device. In case the DC input is less than 39VDC, an alarm can be raised. This alarm is called "DC Power Status".

Chapter 4

Functionality

Media Conversion

The ENX-series offers an easy way to do media conversion on Gigabit-Ethernet network between optical and copper infra-structure. 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 ENX 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.

Switching

The ENX 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 ENX. The ENX interconnects Networks by transparent protocol communication in accordance with IEEE Standard 802.1D ([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.

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 creating a network that is independent of physical location and group users into logical working groups. Using VLANs it is possible to confine broadcast traffic for each working group 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. Per 250 configured VLANs, one must calculate about 2 seconds of operation.

Supported VLAN-Modes of ENX

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

- Provider VLAN-Tagging

The ENX 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 loose 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 ENX.

VLAN Aware

In "VLAN Aware"-mode the ENX 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.

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

Tagged Packets	
Mode	Behaviour
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 ENX.
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 ENX.

Provider VLAN-Tagging

An additional feature supported by ENX is VLAN stacking defined in 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 and setup a MEF service. 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 (Inband MGMT) is also expected to be double-tagged! As soon as the VLAN-mode is configured to Provider-Tagging, you will lose your in-band management connection, if the in-band is not already configured to Double-VLAN-Tagging!

Figure 4-1 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.

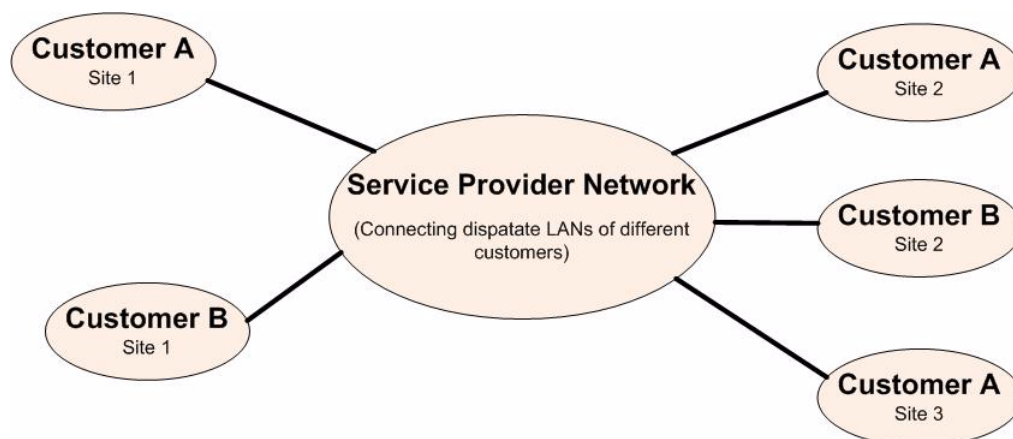


Figure 4-1 Provider VLAN Tagging Diagram

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 4-2.

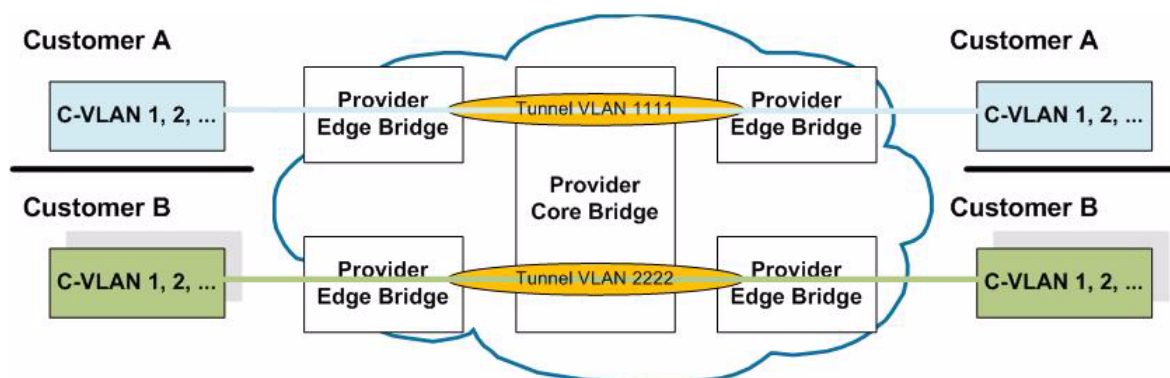


Figure 4-2 P-VLAN configuration

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.

L2CP Frames Handling

When Provider VLAN-tagging is enabled, the handling of L2CP (Layer 2 Control Protocol) frames must be treated in a special way. L2CP are used in Ethernet to set up basic infra-structure such as Spanning Tree (STP) and Link Aggregation (LACP). L2CP frames are normally forwarded to management plane of ENX and treated from there together with the peer device.

When working as a provider bridge, the behaviour on the UNI concerning L2CP handling can change (see [MEF 6.1]):

- Tunnel all L2CP frames to the remote side just as the other payload traffic coming from service I/F,
- Discard all ingress L2CP frames and do not generate any L2CP frames towards peer,
- Keep up communication with Peer and handle L2CP frames locally.

MEF Services

ENX is designed to support several services as defined by the Metro Ethernet Forum (MEF). On a customer interface (LAN-I/F; UNI) the following MEF-defined services are supported:

- Ethernet Private Line (EPL)
- Ethernet Private LAN (EP-LAN)
- Ethernet Private Tree (EP-Tree)

On a LINE interface (NNI) the above mentioned services plus the following three services are supported:

- Ethernet Virtual Private Line (EVPL)
- Ethernet Virtual Private LAN (EVP-LAN)
- Ethernet Virtual Private Tree (EVP-Tree)

EPL

Ethernet Private Line (EPL) is a data service, providing a point-to-point Ethernet Virtual Connection (EVC) between a pair of dedicated User-network interfaces (UNIs), with a high degree of transparency.

- Ethernet Private Line (EPL)
 - Replaces a TDM Private line
 - Dedicated UNIs for Point-to-Point connections
 - Single Ethernet Virtual Connection (EVC) per UNI
 - The most popular Ethernet service due to its simplicity

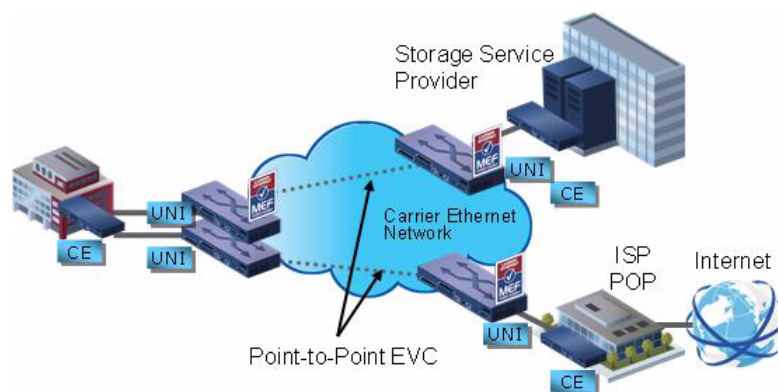


Figure 4-3 MEF: EPL Diagram

EVPL

Ethernet Virtual Private Line (EVPL) is a data service, providing a point-to-point Ethernet connection between a pair of User-network interfaces (UNIs).

EVPL service is specified using an E-Line service type, very similar to a Ethernet Private Line (EPL) service, via a point-to-point Ethernet Virtual Connection (EVC). However, unlike EPL, EVPL allows for Service Multiplexing, i.e., multiple EVCs or Ethernet services per UNI.

- Ethernet Virtual Private Line (EVPL)
 - Replaces Frame Relay or ATM services
 - Supports Service Multiplexed UNI (i.e. multiple EVCs per UNI)
 - Allows single physical connection (UNI) to customer premise equipment for multiple virtual connections

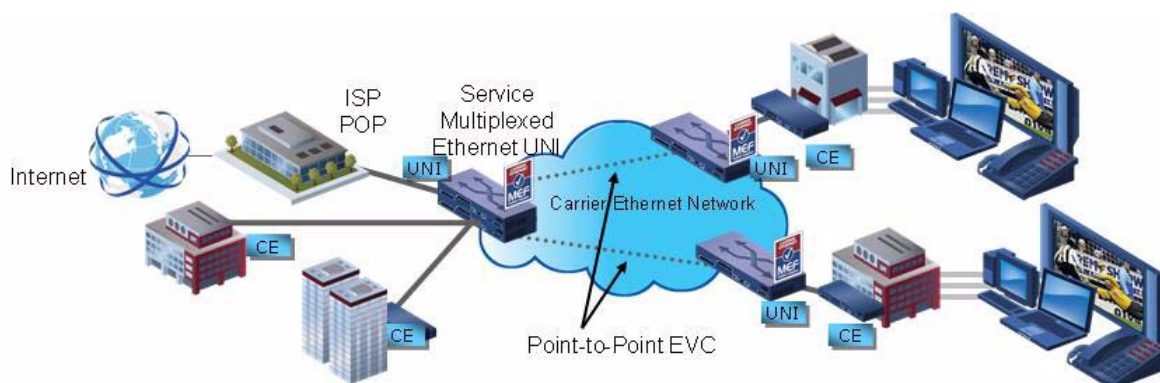


Figure 4-4 MEF: EVPL Diagram

EP-LAN and EVP-LAN

Ethernet Private LAN and Ethernet Virtual Private LAN make use of the EPL and EVPL, but the number of participants to the service is higher than just two. It allows the connection of several sites over the provider’s network.

- Ethernet Private LAN
 - Supports dedicated or service-multiplexed UNIs
 - Supports transparent LAN services and multipoint Layer 2 VPNs

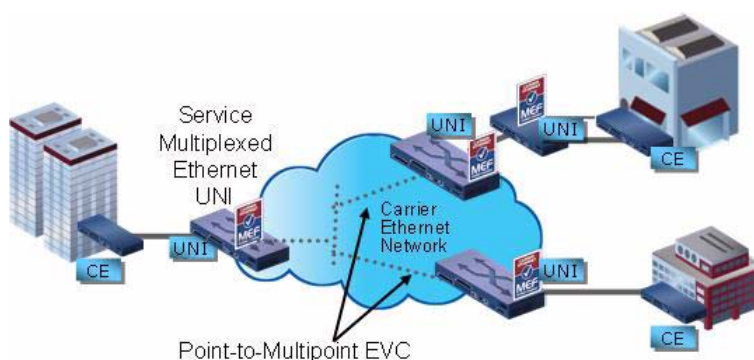


Figure 4-5 MEF: EP-LAN Diagram

EP-Tree and EVP-Tree

Ethernet Private Tree and Ethernet Virtual Private Tree are special variants of the “LAN” services EP-LAN and EVP-LAN. The communication between the different sites is limited. One or more “roots” exists in the tree-network and several “leaves”. The leaves can only communicate with roots but not to each other. This makes the service-network directed towards the roots.

- Ethernet Private Tree (EP-Tree) and Ethernet Virtual Private Tree (EVP-Tree) Services

- Provides traffic separation between users with traffic from one “leaf” being allowed to arrive at one of more “Roots” but never being transmitted to other “leaves”
- Targeted at multi-host and where user traffic must be kept invisible to other users
- Anticipated to be an enabler for mobile backhaul and triple-play infrastructure rather than end-user SLAs

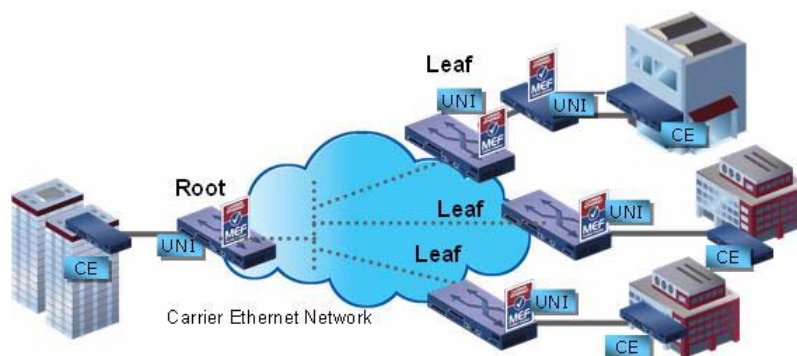


Figure 4-6 MEF: EP-Tree Diagram

Quality of Service

Introduction

The ENX supports QoS (Quality of Service) functionality to treat ingressing packets individually and to define service parameters for different ports. QoS is the ability to provide different priority to customers, or to guarantee a certain level of performance to a data flow. QoS guarantees are important if the network capacity is insufficient, especially for real-time streaming multimedia applications such as voice over IP, online games and IP-TV, since these often require fixed bit rate and are delay sensitive, and in networks where the capacity is a limited resource, for example in cellular data communication.

The approaches of ENX to QoS is called Differentiated Services (“DiffServ”). DiffServ implements a prioritizing model. In the DiffServ model, packets are marked according to the type of service they need. In response to these markings, the unit use various queuing strategies to tailor performance to requirements. At the IP layer, differentiated services code point (DSCP) markings use the 6 bits in the IP packet header. At the MAC layer, VLAN IEEE 802.1Q and IEEE 802.1p can be used to carry essentially the same information.

Devices supporting the DiffServ model use multiple queues for packets awaiting transmission from bandwidth constrained (e.g., wide area) interfaces. The ENX provides different capabilities to configure this behaviour, to include the relative priorities of queues, bandwidth reservations, and mapping of incoming priorities to internal behaviour and new values. In practice, when a packet must be forwarded from an interface with queuing, packets requiring low jitter (e.g., VoIP or video-conferences) are given priority over packets in other queues. Typically, some bandwidth is allocated by default to network

control packets (such as Internet Control Message Protocol and routing protocols), while best effort traffic might simply be given whatever bandwidth is left over.

In the ENX the Media Access Control (MAC) layer is used for DiffServ model. It uses VLAN IEEE 802.1Q and IEEE 802.1p to carry the essential information.

Implementation

The QoS implementation of ENX is a 5-step solution:

1. After packet ingress the Classification of each packet is done. At the end of the classification, the packets carries two additional information sticker, which are used in the further processing.
2. Subsequent the Limiting of the ingress packet stream to the maximum bandwidth is done. Four different limiters are available, to limit the incoming traffic. The selection of the right limiter for each stream is based on the result of the classification.

After classification the packet switching is done, which is not really part of the QoS plane but pure data forwarding.

3. On the Egress side, the packets will be assigned to one of four priority queues. This assignment is based on step 1 “Classification”.
4. The packets are taken by a Queue Controller from the different priority queues. This is done by a configurable mechanism to make sure even the lowest priority stream will be considered time by time and the higher priorities can not block transmission of lower levels at all.
5. For each port a traffic shaping is done to smooth and prevent the net from becoming overloaded.

A short overview to the packet flow and the 5 steps are given in the figure below. The detailed description of configuration and options are presented in the following chapters.

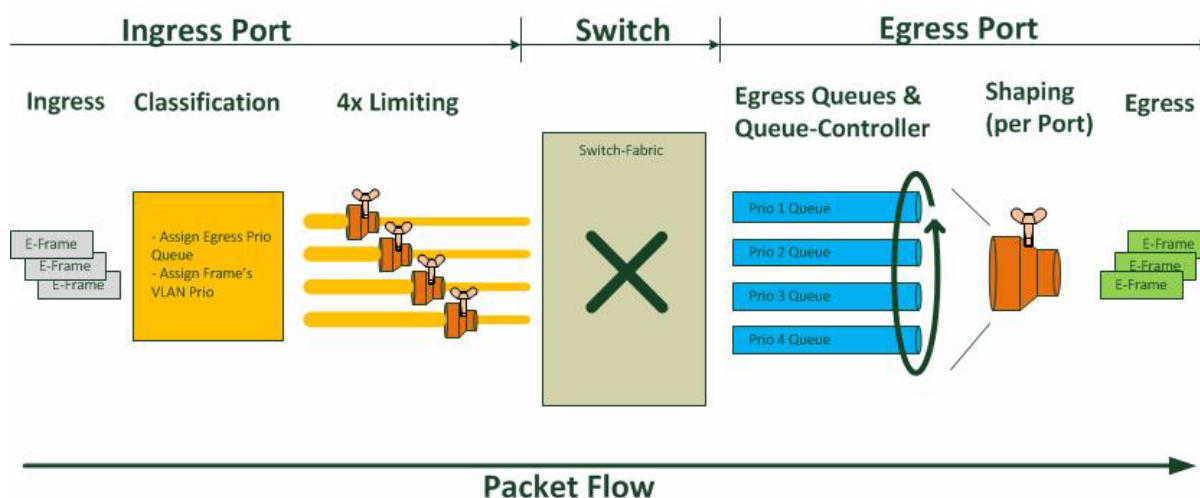


Figure 4-7 QoS Packet Flow

Classification

The classification of ingressing packets is the first step of packet handling inside the ENX. Two decisions are made based on the result of the classification:

1. An egress priority-sticker is generated and tagged as additional information to each packet. The priority-sticker is used as info-store, to fill the VLAN-priority field at the egress of the packet. Here it is not important whether an untagged packet will be tagged at egress, an already tagged packet must be double-tagged at egress or an already tagged packet shall be assigned the new priority value at egress.
2. The egress queue (queue 1-4) is selected already based on information collected at ingress of each packet. The selected choice is also stucked to the packet for its further flow through the device. This queue-sticker can be based on the above mentioned priority-sticker or IP-DSCP values.

Priority-Sticker

The priority-sticker is a special tag, which is attached to each packet in the classification block. The sticker “stays” with the packet during its ways through the device. At the egress of the packet the priority-sticker is used and copied into the packets most-outer VLAN-tag. If the packet leaves the device without any VLAN-tag, the priority-sticker’s value is unneeded.

The value of the priority-sticker can be based either on

- Default Priority of the port or
- VLAN-priority value of an ingressing (already tagged) frame or
- IP DSCP/TOS-field value of the ingressing frame.

Note: The DSCP/TOS value can only be considered for untagged frames!

The three possible sources of the priority-sticker can be combined or used as single rule. If combined, the sequence must be configured and the first match in the sequence will determine the priority-stickers result for the packet.

For example, the sequence is first DSCP/TOS-field and second is default priority. When a frame is ingressing, which carries an IP-packet, the decision is made based on DSCP/TOS. When a frame is ingressing, which is carrying a non-IP content (e.g. ARP packet) the priority-sticker is deduced from the default priority of the port.

The value range of the priority-sticker is Prio0 (p0, low) to Prio7 (p7, high). A mapping must be defined by user assigning possible source values (VLAN-prio, DSCP/TOS-field) to the 8 priority-stickers. For DSCP/TOS the assignment has to be done once and this is valid at all ingress ports. The VLAN-priority assignment to priority-sticker has to be done for all ingress ports individually. This is the case, as DSCP-values are defined globally by IETF, while the VLAN-prio does not have such a global definition. Prio7 can be highest prio in one LAN, while it is lowest priority-level in another LAN setup.

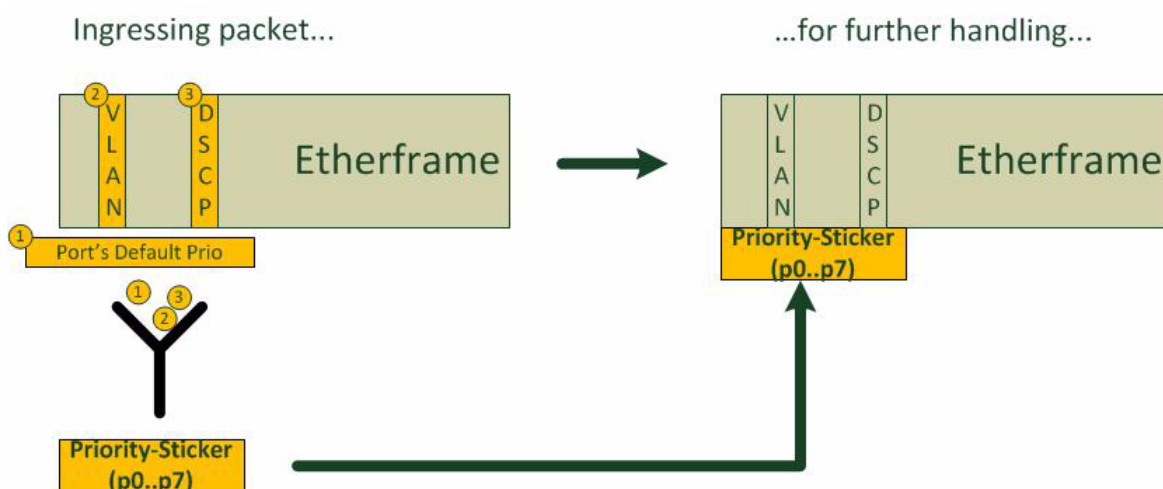


Figure 4-8 QoS Priority-Sticker

The default mappings for the priority classification are as follows:

- Per port mapping from incoming VLAN priority to priority-sticker:

Incoming VLAN prio	0	...	7
Priority-Sticker	p0	...	p7

- DSCP mapping from incoming (IP) frame to priority-sticker:

Incoming DSCP value	000000- 001111	010000- 011111	100000- 101111	110000- 111111
Priority-Sticker	p0	p2	p4	p6

Queue-Sticker

The queue-sticker is a special tag, which is attached to each packet in the classification block. The stickers “stays” with the packet during its ways through the device. At the egress of the packet the queue-sticker is used to find the correct egress queue for each packet. Each egress port does have 4 egress-queues, representing different “importance-level”. Frames in the higher queue get preference to those in lower queues. This helps to achieve service levels for latency, bandwidth and packet loss. See chapter “Queue Scheduler” on page 4-19 for details of queues.

The value of the queue-sticker can be based either on

- Priority-Sticker, which is already stucked to the frame or
- IP DSCP/TOS-field value of the ingressing frame.

The two possible sources of the queue-sticker can be combined or used as single rule. If combined, the sequence must be configured and the first match in the sequence will determine the queue-stickers result for the packet.

For example, the sequence is first DSCP/TOS-field and second is priority-sticker. When a frame is ingressing, which carries an IP-packet, the decision is made based on DSCP/TOS. When a frame is ingressing, which is carrying a non-IP content (e.g. ARP packet) the queue-sticker is deduced from the priority-sticker, which is already stucked to the packet.

The value range of the priority-sticker is Queue1 (Q1, low queue priority) to Queue4 (Q4, high queue priority). A mapping must be defined by user assigning possible source values (priority-sticker, DSCP/TOS-field) to the four queue-stickers. The assignment has to be done once and this is valid at all ingress ports.

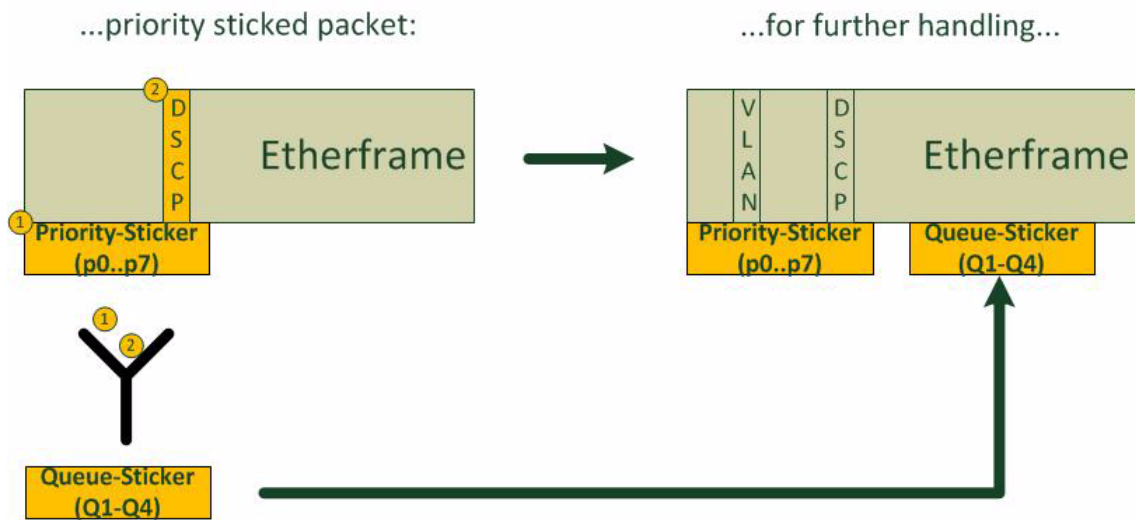


Figure 4-9 QoS Queue-Sticker

The default mappings for the queue classification are as follows:

- Per port mapping from incoming VLAN priority to queue-sticker:

Priority-Sticker	p0, p1	p2, p3	p4, p5	p6, p7
Queue-Sticker	Q1	Q2	Q3	Q4

- DSCP mapping from incoming (IP) frame to queue-sticker:

Incoming DSCP value	000000-001111	010000-011111	100000-101111	110000-111111
Queue-Sticker	Q1	Q2	Q3	Q4

IP Precedence and DSCP

Originally the DSCP field was called the TOS-field (Type-of-Service). TOS was defined in [IETF RFC 791], while DSCP is defined in [IETF RFC 2474]. For the TOS-field usage, the so-called IP-Precedence was defined, a value of 0 to 7. At its simplest, the higher the value of the IP Precedence field, the higher the priority of the IP packet.

For DSCP three ways of usage are defined by IETF, which define a sub-set of code-points for easier usage:

- CL Class Selector ([IETF RFC 2474])
- AF Assured Forwarding ([IETF RFC 2597])
- EF Expedited Forwarding ([IETF RFC 3246])

IP Precedence as well as DSCP with its 3 pre-defined sets are used mixed up. The short overview of the corresponding values shall help to find the correct configuration:

Table 4-5 DSCP vs. IP Precedence Conversion Table

DSCP Name	DS Field Value		IP Precedence
	Binary	Decimal	
CS0	000 000	0	0
CS1	001 000	8	1
AF11	001 010	10	1
AF12	001 100	12	1
AF13	001 110	14	1
CS2	010 000	16	2
AF21	010 010	18	2
AF22	010 100	20	2
AF23	010 110	22	2
CS3	011 000	24	3
AF31	011 010	26	3
AF32	011 100	28	3
AF33	011 110	30	3
CS4	100 000	32	4
AF41	100 010	34	4
AF42	100 100	36	4

Table 4-5 DSCP vs. IP Precedence Conversion Table (continued)

DSCP Name	DS Field Value		IP Precedence
	Binary	Decimal	
AF43	100 110	38	4
CS5	101 000	40	5
EF	101 110	46	5
CS6	110 000	48	6
CS67	111 000	56	7

Limiting

Each port offers 4 independent (ingress) limiter, which can be configured to be used for all or only for certain frames (subset of frames). The assignment to the limiter is done in a 2-step procedure, which allows very decided configuration. If less than all 4 limiters are required on a port, just disable the unused ones to avoid uncertain behaviour.

Packet Selection for Limiter

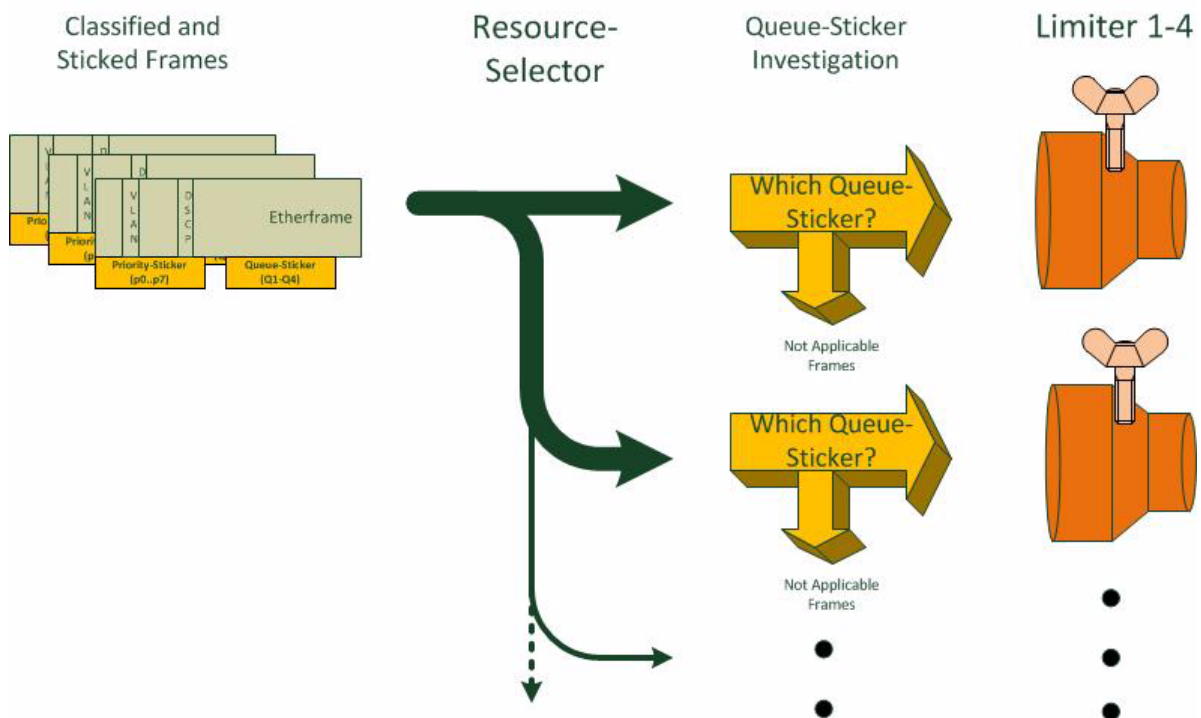


Figure 4-10 Ingress Limiter Selection (per Port)

First step is to select, which resources of frames shall be limited by the limiter. The resource of a frame is its "cast-type":

- Unicast,
- Multicast or
- Broadcast.

Four limiter are available and it is possible, that two or more limiter do use the same resource. So it is allowed, that all 4 limiter are configured to act on Unicast-frames, only. The next step in selection will then distinguish which frames are really limited by the single limiter.

After the resource-selector, the packet's queue-sticker is taken for next step of selection. The queue-sticker was added to each packet in the classifier-block (see "Classification" on page 4-12) and represents the packet's priority-queue at the egress. Four different queue-stickers are defined and only those packets with the matching queue-sticker will be forwarded to the limiter itself. All other packets, which had matched the resource-selector will not be limited by the single limiter.

Example: One needs to limit all unicast frames distinguished by queue-priority. Limiter 1-4 are configured to use Unicast frames as resource. Limiter 1 is configured to act on Q1-frames, limiter 2 on Q2-frames on so on.

Overlapping Resource Selectors

It is allowed and possible that the limiters resource selectors do have overlapping ranges. E.g. one limiter does work an "All Broadcast Frames", while a second limiter does act on "All Frames". If a broadcast packet is arriving the device, both limiter can drop such a packet due to the given SLA settings.

If any of the matching limiters does drop a packet, it will be dropped. Even if a second limiter could accept this packet!

In the above example of "All Broadcast Frames" and "All Frames" limiters the setting could be as follows:

- Limit "All Broadcast Frames": 10kbps
- Limit "All Frames": 500Mbps

When a "Broadcast Frame" is ingressing the device and the limit of 10kbps is reached, the frame will be dropped, even if the limit for "All Frames" is not reached, yet.

Date-Rates for Limiter

The date-rate for each limiter can be defined in either (kilo / Mega) bits-per-second or frames-per-seconds. If the limit is given in bits-per-second, the value represents the CIR (Committed Information Rate), which is allowed. The ENX does have a granularity for the limiter, which is accommodation of information rates from 64kbps to 1Mbps in

increments of 64kbps, from 1Mbps to 100Mbps in increments of 1Mbps and from 100Mbps to 1000Mbps in increments of 10Mbps:

Bandwidth on Port	Units for Limiter
0 - 1Mbps	64 kbps - steps
1 - 100 Mbps	1000 kbps - steps
100 - 1000 Mbps	10 Mbps - steps

If the configuration does not match the possible values, the device will step down the user's wish to the next allowed value. Both values (wish and effective) will be stored and displayed.

Shaping

The per port Egress Shaper can be individually configured for a maximum egress bandwidth. The ENX does have a granularity for each shaper, which is accommodation of information rates from 64kbps to 1Mbps in increments of 64kbps, from 1Mbps to 100Mbps in increments of 1Mbps and from 100Mbps to 1000Mbps in increments of 10Mbps:

Bandwidth on Port	Units for Shaper
0 - 1Mbps	64 kbps - steps
1 - 100 Mbps	1000 kbps - steps
100 - 1000 Mbps	10 Mbps - steps

If the configuration does not match the possible values, the device will step down the user's wish to the next allowed value. Both values (wish and effective) will be stored and displayed.

CIR & CBS

Thee ingress limiter can be configured to operate either in a rate-limiting mode or frames-limiting mode. In the second, the limiter has a number of frames, which it does accept in a given time-interval (normally seconds). No matter how long the frames are, the maximum number is fixed.

If the limiter is operating in a rate-limiting mode, a maximum data-rate plus a burst rate can be configured. The burst rate is a kind of a piggyback, where "rate assets" are stored. The size of this bank is called "Rate Burst Size" or Committed Burst Size (CBS).

The maximum data-rate, which is accepted by the ingress limiter is the so-called Committed Information Rate (CIR).

If the traffic, ingressing from customer is smaller than the CIR, the limiter will fill the “Rate Burst Buffer” till the maximum value (CBS). When the incoming traffic is above the CIR, the limiter will allow this traffic to ingress, until the “Rate Burst Buffer” is emptied. The next figure will explain these relationship in detail.

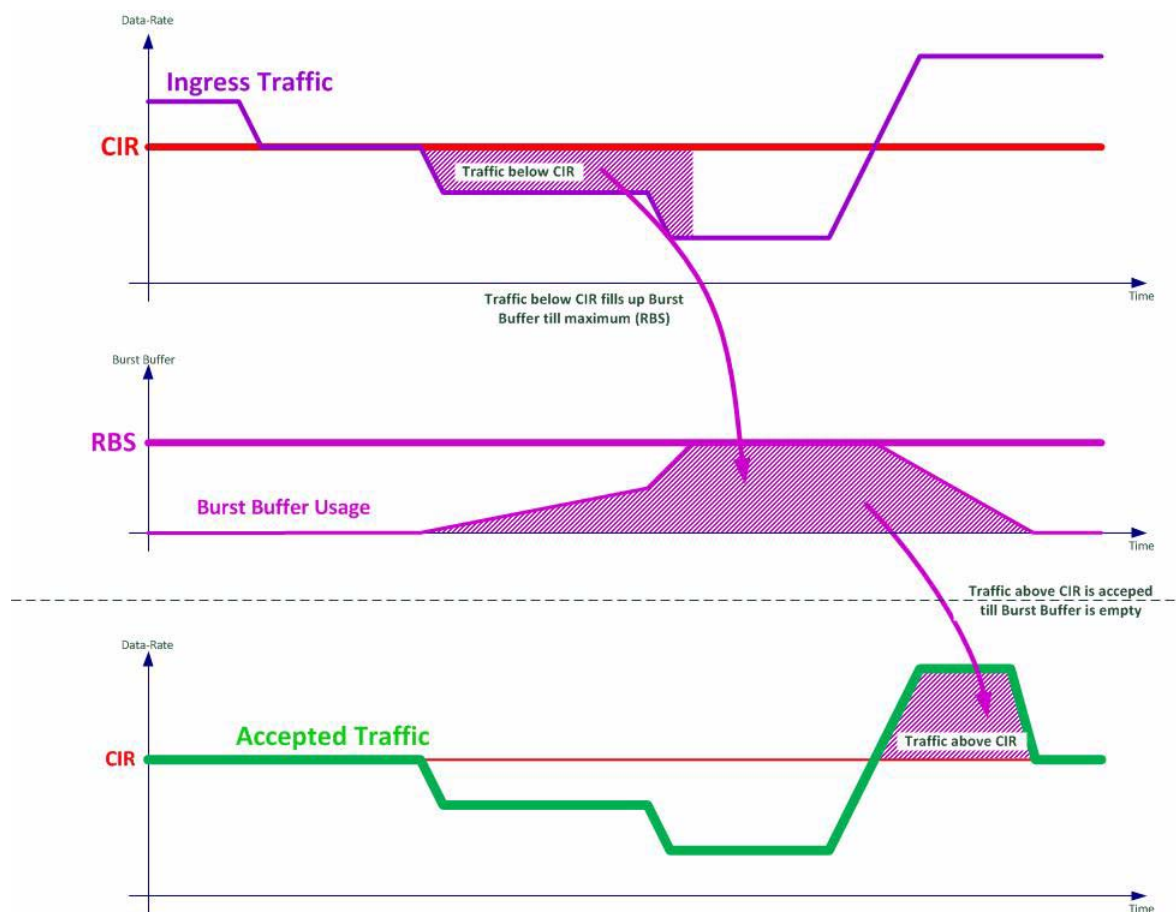


Figure 4-11 CIR & CBS

Queue Scheduler

Each port contains four independent output queues, one for each priority (Prio1,high to Prio4, low). At the ingress of a packet into the ENX each packet is classified and the decision is already than made, to which output queue the packet will be sorted. (The decision which port is used for egressing is done in the switching fabric after the classification.) The queue decision at the classifier is sticked to the packet in the queue-sticker (see “Queue-Sticker” on page 4-13) and at the egress this sticker is removed before the packet is sorted into the right queue. So keep in mind, the decision which queue will be used at the egress is done already at the ingress!

The output queues will be emptied as fast as they can - but they could empty at different rates. This is due to the priority-level of each queue and the configuration of a sched-

uler. The scheduler checks the output queues and the MAC layer of each port. If there is one or more frames in the queues and the MAC layer is free, the scheduler will take one of the attending frames and put it onto the MAC.

In its most simple form, the scheduler gives always priority to packets in the queue with the highest priority (Queue4). This could lead to the situation, that packets in lower queues will never be transmitted. This is called “Strict Priority”, but the scheduler can be configured to more distinctive behaviour.

The ENX supports strict priority, weighted round robin, or a mixture on a per port selection basis. In the strict priority scheme all top priority frames egress for a port until that priority’s queue is empty then the next lower priority queue’s frames egress etc. This approach can cause the lower priorities to be starved out preventing them from transmitting any frames but also ensures that all high priority frames egress the device as soon as possible. In the weighted scheme an 8,4,2,1 weighting is applied to the four priorities unless an alternative weighting is selected. This approach prevents the lower priority frames from being starved out with only a slight delay to the higher priority frames.

The standard weighting scheme (8,4,2,1) has the meaning, that queue Q4 will get 8 times more grants to send packets than queue Q1 and double the grants than Q3. Other optional schemes are the progressive scheme (64,16,4,1) and smooth (4,3,2,1).

If a mixture of strict priority and weighted scheme is required, 2 options are available:

- Q4 strict; else weighted scheme: This is that Q4 has strict priority above all other three queues. When Q4 is emptied, the other three queues are handled according the selected weighted scheme. The value of Q4 in the scheme is ignored.
- Q4 and Q3 strict; else weighted scheme: This is that Q4 has strict priority above Q3 and Q3 above the other two queues. When Q4 is emptied, Q3 will be served. When Q4 and Q3 are empty, the other two queues are handled according the selected weighted scheme. The values of Q4 and Q3 in the scheme are ignored.

MAC Address Table

Ethernet devices learn and store (source-) MAC addresses of ingressing frames. This helps to forward packets and reduce traffic in switched networks. The learned MAC addresses and the appropriate Ethernet ports are stored in a table. When topologies are changing, it must be possible to remove entries of this MAC address table and to learn new combinations of ports and addresses.

The ENX does have a MAC address range of 8192 (8k) entries in the MAC address table. The device’s MAC address table uses the destination address (DA) and source address (SA) fields from each frame received from each port. The ENX performs all address searching, address learning, and address aging functions for all ports at ‘wire-speed’ rates. This means a DA and an SA look-up/learn process can be performed for all ports in less time than it takes to receive a 64 byte frame on any port!

The MAC address table uses a hashing technique for quick storage and retrieval. Hashing a 48-bit MAC address into fewer bits result in some MAC addresses having the same hash entry. This hash-collision is solved by using 4 bins per hash-entry allowing for storage of up to 4 MAC addresses at each hash location. This allows the MAC

address table to be smaller while holding the same number of active, random value MAC addresses.

NOTE: If all 4 bins of a hash location are occupied and a new MAC address must be stored in this hash location, the least used MAC address is removed to store the new one. If all 4 MAC addresses have the same age time, then the first entry (bin #1) is removed.

The ENX does store by default new learned address-port combination in the MAC address table for the time of 300 seconds. After this time the entry will be removed automatically and it must be re-learned. To speed up the integration in a changed topology, it is possible to flush all learned entries.

Link Aggregation with LACP

LACP Introduction

Link aggregation (or trunking or link bundling or bonding or teaming) is terms to describe various methods of combining (aggregating) multiple network connections in parallel to increase throughput beyond what a single connection could sustain, and to provide redundancy in case one of the links fails.

Aggregation can be implemented at any of the lowest three layers of the OSI model. Commonplace examples of aggregation at layer 1 are power line (e.g. [IEEE 1901]) and wireless (e.g. [IEEE 802.11]) network devices that combine multiple frequency bands into a single wider one. Layer 2 (data link layer, e.g. Ethernet frame in LANs or multi-link PPP in WANs) aggregation typically occurs across switch ports, which can be either physical ports, or virtual ones managed by an operating system. Aggregation is also possible at layer 3 in the OSI model, i.e. at the network layer (e.g. IP or IPX), using round-robin scheduling, or based on hash values computed from fields in the packet header, or a combination of these two methods. Regardless of the layer on which aggregation occurs, the network load is balanced across all links. Most methods provide failover/redundancy as well.

LACP (Link Aggregation Control Protocol) is a way for computer systems to dynamically agree on their Ethernet link bonding capabilities and to automatically aggregate links as possible. It was originally defined as IEEE 802.3ad and has now moved to [IEEE 802.1AX].

LACP operates layer 2 (data link layer). Systems supporting LACP exchange link-local, multicast Ethernet frames with their link partner to negotiate their aggregation capabilities. LACP operates transparently to higher OSI layers by introducing virtual MACs (called Aggregators) that represent the aggregation. Those virtual MACs behave similar to physical MACs up to the fact that they have an entry in the SNMP specific interface-table (ifTable).

A system considers a number of links to be aggregatable under the following conditions:

- the links terminate in the same partner system
- the links are all operated with the same link speed and in full duplex mode

- the partner system indicates that the links are aggregatable

If those conditions are fulfilled, each group of links that can aggregate together is assigned to one of the aggregators (the virtual MACs) to form a single logical link with higher data rate.

Aggregation capability of LAN/LINE-ports of the ENX device as well as LACP protocol details can be configured for every ENX port group separately. A separate LACP system is simulated for each port group preventing ports in different groups to aggregate.

Implementation

The ENX supports vendor-independent standard [IEEE 802.1AX] Link Aggregation Control Protocol (LACP) for wired Ethernet. Within the IEEE specification the Link Aggregation Control Protocol (LACP) provides a method to control the bundling of several physical ports together to form a single logical channel. LACP allows a network device to negotiate an automatic bundling of links by sending LACP packets to the peer (directly connected device that also implements LACP).

LACP Configuration

The ENX device has built-in support for LACP that can be enabled or disabled with the “LACP Support” variable. If enabled, the ENX will start to generate and respond to LACP messages on all LAN/LINE-ports and show a table containing a row for each port group.

The “Port Operation” setting determines whether the ENX device allows Ethernet ports within the port group to be aggregated. If set to “Standard”, the ports will never be bonded. If set to “LACP”, the Ethernet ports within the group will automatically be bonded if possible.

Port Group Details

The “LACP Mode” setting determines whether the ENX does Active or Passive LACP on the ports within the port group. “Active LACP” implies a regular exchange of LACP status information between link partners, whereas “Passive LACP” reduces exchange of LACP messages to cases of LACP configuration changes.

The “LACP Transmit Interval” determines the frequency of LACP status message exchange in case of active LACP. The setting “Long LACP Interval” requires an LACP status message exchange every 30 seconds, whereas “Short LACP Interval” reduces the communication interval to one second.

The “Aggregation Configuration” setting determines whether the port aggregation configuration on the ENX device is done automatically by the device itself or manually by the device administrator. The manual configuration mode allows maximum flexibility and allows to achieve aggregation even in the absence of LACP capable link partners, whereas the automatic mode works well with LACP capable link partners, requires no further configuration and will automatically adjust to changes in the wiring.

LACP Aggregators

This menu shows a table containing the aggregators (virtual MACs) defined for this port group. The number of aggregators is the same as the number of ports in this group to have sufficient resources available in case links cannot be aggregated.

Clocking and Synchronization

The ENX is a synchronous device, which can make benefit out of 2 clock distribution concepts:

- SyncE, which is a layer 1 technology, specified by ITU-T G.8262/Y.1362 ([ITU-T G.8262]).
- Precision Time Protocol, which is a higher layer protocol specified by [IEEE 1588].

Both concepts do work independently from each other, but it is foreseen that interworking can be configured.

Synchronous Ethernet (SyncE)

Introduction

Synchronous Ethernet is one of several ways to achieve synchronization over Ethernet, SyncE uses the physical layer interface to pass timing from node to node in the same way timing is passed in SONET/SDH or T1/E1. This gives telecom and wireless providers confidence that networks based on SyncE will be not only cost-effective, but also as highly reliable as SONET/SDH and T1/E1 based networks.

Traditional Ethernet was originally intended for transmission of asynchronous data traffic, without any requirement to pass synchronization from source to destination. Each Ethernet switch does have its own reference clock, an internal free-running oscillator with +/-100ppm accuracy. Figure 4-12 shows the isolated clock sources in traditional Ethernet.

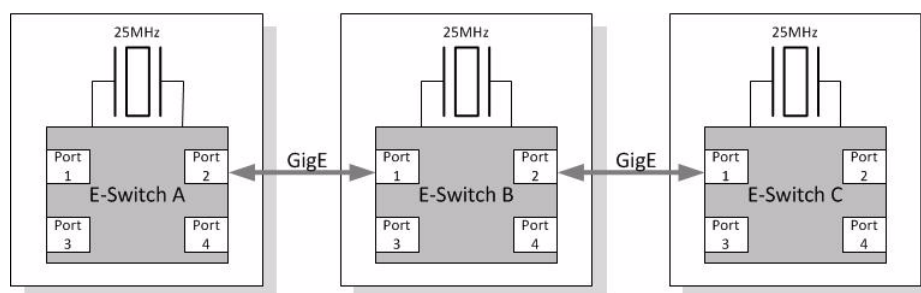


Figure 4-12 Clock distribution in traditional Ethernet

Synchronous Ethernet is just to recover the transmission clock from one device and use this clock as reference for the local switch. Together with the option of external synchronized clock on the “entry-switch”, a chain of synchronous switches can be built.

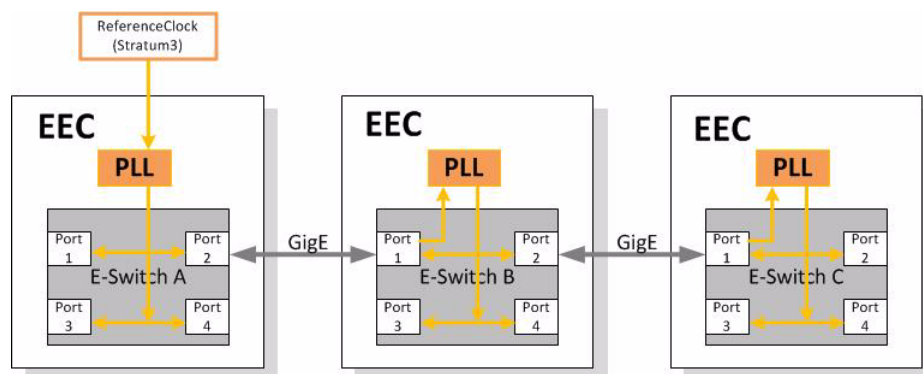


Figure 4-13 Clock distribution in Synchronous Ethernet

The recovered clock-signal needs to be cleaned with a PLL to remove jitter generated from the clock recovery circuit before being fed to the transmitter.

In case of interruption of the clock-reference link, the PLL needs to keep the frequency as long as possible. The PLL used in SyncE must be able to detect failure of the recovered clock and switch to either another good reference in the system or into holdover mode. Requirements for SyncE are outlined in the timing characteristics of synchronous Ethernet equipment slave clock (EEC) by ITU-T recommendation G.8262/Y.1362 [ITU-T G.8262]. These specifications are based on [ITU-T G.813] specification for SDH clocks. The major requirements of ITU-T G.8262/Y.1362 are:

- Free-run accuracy: The accuracy of PLL output when it is not driven by a reference is equal or better than ± 4.6 ppm over one year. This is a very accurate clock relative to the clock accuracy for traditional Ethernet (± 100 ppm).
- Holdover: If the reference fails and no other references are available, the PLL goes into holdover mode and generates an output clock based on the last frequency value.
- Reference monitoring: The PLL monitors constantly the quality of its input references. If the reference is getting worse (disappears or drifts in frequency), then the PLL switches to another valid reference.
- Hitless reference switching: If the PLL's reference fails, then it will lock to another available reference without phase disturbances at its output.
- Jitter and wander filtering: The PLL is a jitter and wander filter. The narrower the loop bandwidth, the better the jitter and wander attenuation.
- Jitter and wander tolerance: The PLL tolerates large jitter and wander at its input and still maintain synchronization.

Implementation

ENX's implementation of SyncE does meet all the above mentioned requirements of a synchronous Ethernet equipment slave clock (EEC). It can use 7 different sources for its SyncE clock (see Figure 4-14):

- T3an: a 2,048MHz clock.
- Internal oscillator: a temperature compensated oscillator (TCXO) is equipped.

- A special version is available, where a OCXO (Oven Controlled Crystal Oscillator) is equipped for higher stability of the clock, when temperature is changing.
- LINE ports: Both LINE ports can be used as source for SyncE. The LINE ports are combo-ports and allow selecting their RJ45 (SyncE LINE X Electrical) and fibre (SyncE LINE X Optical) function independently as clock source, resulting in a total of four clock sources.
 - 2x SyncE from Copper ports
 - 2x SyncE from fibre ports
- In some variants, the PTP clock can be used as reference for SyncE

The ENX uses a simple and straightforward algorithm to automatically select one of the available clock sources for device synchronization that is described below. The algorithm includes user-defined settings describing the preference of clock sources as well as clock quality information in its decision when selecting a clock signal for synchronization.

External clock inputs need to be enabled before they can be used for synchronization. For LINE ports this means that the port must be enabled, auto negotiation for the port must be enabled (for Master/Slave negotiation to work) and that the “SyncE Mode” for the port must be set to “Slave”.

For T3an this means enabling the port itself and selecting a suitable operation mode. Available for selection are:

- T12 - a 2,048 MHz clock signal.

External clock outputs need to be enabled before they distribute clock information to further slaves. For LAN ports this means that the port must be enabled, auto negotiation for the port must be enabled (for Master/Slave negotiation to work) and that the “SyncE Mode” for the port must be set to “Master”.

For T4ab this means enabling the port itself and selecting a suitable operation mode. Available for selection are:

- T12 - a 2,048 MHz clock signal (no clock quality information).
- E12 - a 2048 Mbps HDB3-coded data stream (clock quality level in TS0 Sa8 bits).

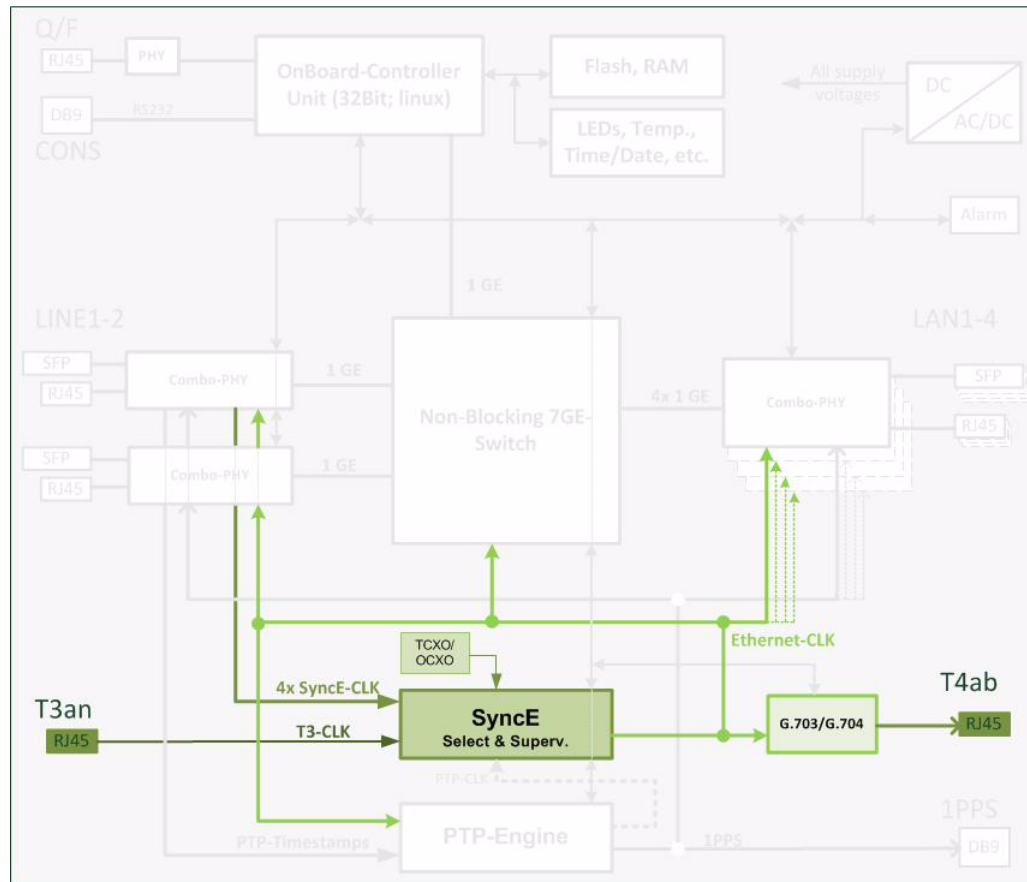


Figure 4-14 Block Diagram for Synchronous Ethernet

Clock Source Properties

Each clock source has a number of properties associated with it that allow monitoring the status of the clock input or aid the clock selection algorithm in its decisions.

Each clock source can independently be assigned a Priority value by the device administrator. This priority is a simple numerical value (1: highest priority, 15: lowest priority) that determines the user-preferred ordering of the clock sources. The clock source with the highest priority will automatically be chosen for device synchronization provided that the clock quality is determined to be acceptable. It is possible to disable use of a clock source by setting the corresponding priority value to “do-not-use”.

Each clock source has a set of quality levels associated with it: the Line, Overwrite and Effective Clock Quality level. Where supported, the Line Quality Level is determined from the clock master connected to the port via protocol (e.g. SSM messages on LINE ports set to “Slave” mode). Where this is impossible (e.g. T3an in T12 mode, TCXO), the Line Quality Level stays fixed at a value of DNU (Do Not Use). The device administrator is given the possibility to overwrite the determined Line Quality Level with a selectable Overwrite Quality Level. This is the only possibility assigning a different value than DNU to clock source types that have no means of distributing clock quality level information via protocol. The Effective Clock Quality level is always used to represent the clock source further on, aids the clock selection algorithm and results from the

other quality levels. If overwriting the Line Clock Quality is enabled by the device administrator, it reflects the current Overwrite Clock Quality level, otherwise it reflects the current Line Clock Quality.

The administrator can select one of two different algorithms to determine whether a clock signal is of acceptable quality or not (Clock Valid Decision). The first algorithm compares the constantly monitored MDvXO value (Mean Deviation vs. XO, frequency deviation of the clock signal from the internal reference oscillator) against a user-defined threshold. If the clock frequency differs too strongly from the frequency of the TCXO (or the jitter of the clock frequency becomes irrecoverably high), the clock is considered to have a bad quality and is not used for device synchronization. The second algorithm additionally compares the current value of the Effective Clock Quality against a user-defined threshold. If the clock quality falls below that limit, the clock is again considered to be of bad quality and not used for device synchronization.

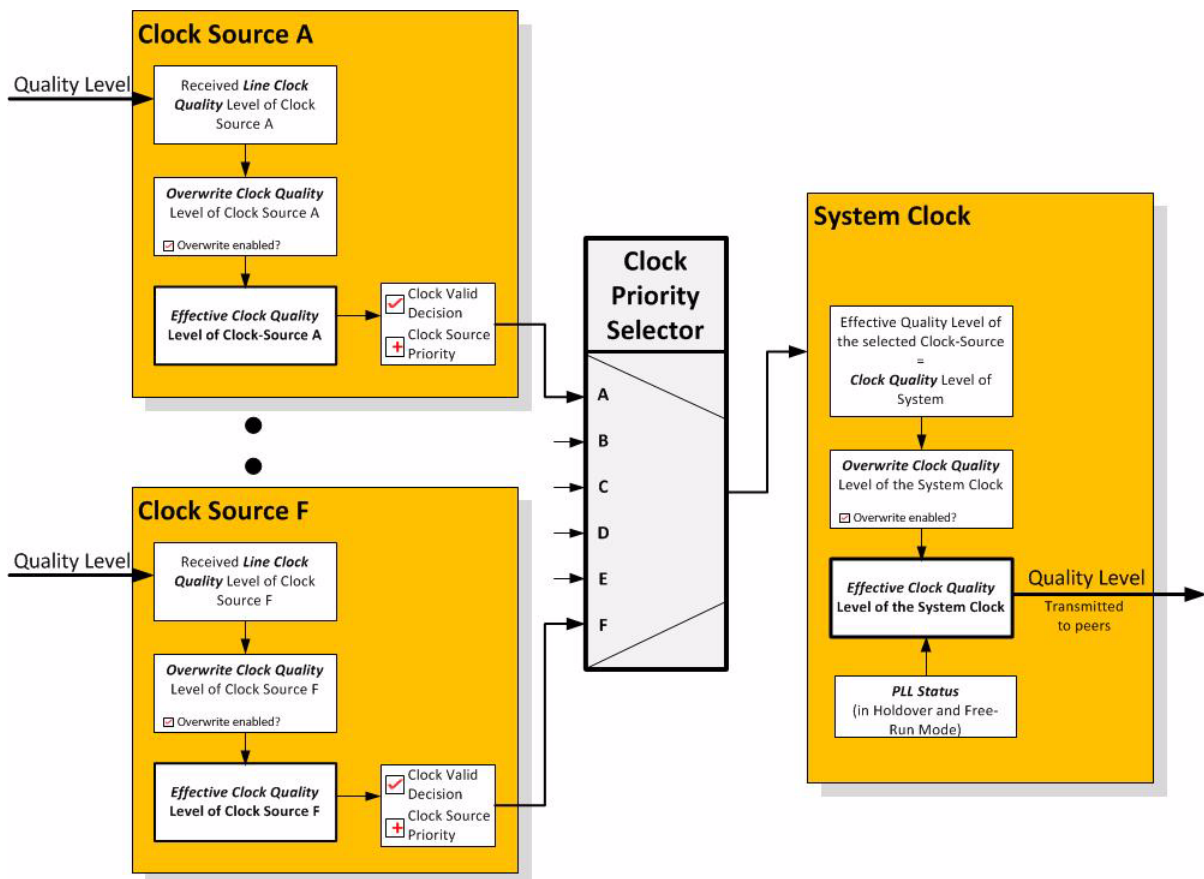


Figure 4-15 Clock Quality Level distribution within the ENX

Clock Source Selection

Usually, the clock source with the highest priority will automatically be chosen for device synchronization provided that the clock quality is determined to be acceptable. If the clock with the highest priority is not of acceptable quality, the second highest priority clock is considered and so forth.

It is allowed to specify the same priority for more than one clock source. If more than a single clock with the same priority has an acceptable quality, the order in which those sources are selected for device synchronization is unspecified. To enforce a given order, the priority of the clock sources must be set to unique values.

When a higher priority clock is of unacceptable quality and the device is synchronized to a clock with lower priority, the Revertive Mode specifies the behaviour of the ENX if the higher priority clock becomes acceptable again. If set to Revertive, the device automatically switches back to the higher priority clock even when the lower priority clock is still acceptable. In non-revertive mode, the ENX remains synchronized to the lower priority clock (for clock stability reasons) until that clock becomes unacceptable.

Synchronization State

The global synchronization state of the ENX describes whether the device is successfully synchronized to one of the available clock sources and the quality of that source. The information sent out by the ENX to synchronization slaves (via LAN ports and T4ab) also depends on the synchronization state.

The PLL Status indicates whether the ENX was able to synchronize to one of the acceptable clock sources. If it shows anything else than “Locked”, the ENX is not properly synchronized.

The ENX also shows the currently selected Synchronization Clock Source and the effective quality level associated with that source. This quality level can be overwritten here as well, affecting the global device state independent of the selected clock source.

The global Effective Clock Quality level is reported to synchronization slaves. If the PLL Status indicates that the ENX is in Holdover or Free-Run mode, it always reports a quality level of EEC1 (Ethernet Equipment Clock class 1). If the PLL is not locked, it always reports DNU. Otherwise it reflects the selected Overwrite Clock Quality level or the effective quality level of the synchronization clock source, depending on the configuration.

T4ab Driver

The T4ab port is reference port for subsequent devices. With the help of T4ab the clock information of the SyncE-layer can be distributed. To avoid propagation of a faulty clock, T4ab is automatically turned off when the ENX is not successfully synchronized to an external SyncE synchronization source (LINE).

Note: This is in contrast to LAN ports which always distribute clocking information and the current quality level when configured as SyncE masters.

In case the T3an reference clock is available and selected as synchronization source for the device, the T4ab port can be used or turned off. This behaviour can be configured by user. Figure 4-16 shows the possible dependencies for T4ab driver.

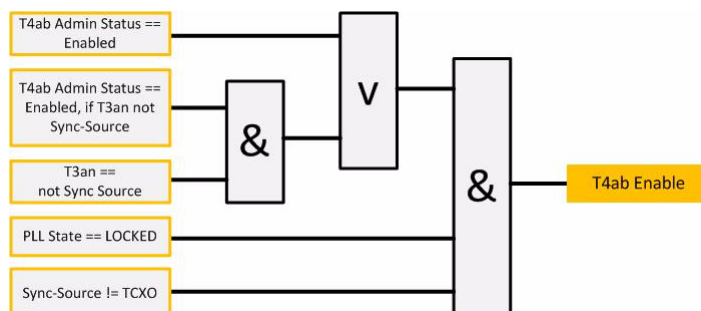


Figure 4-16 T4ab Driver

For bottom to top one can see, it is mandatory to have the PLL in the Locked-State and the Sync-Source must not be the internal oscillator.

The user has two option to configure the T4ab: Either “Enable” or “Enable, if T3an is not Sync-Source”. In the first case, the driver will enable T4ab, as soon as the above mentioned two mandatory conditions are true.

In the second case, the two mandatory conditions must be true and T3an is not selected as synchronization source.

Alarming Capabilities

The ENX device defines several alarms in the alarm group “Clock Alarms” that constantly monitor SyncE operation. The PLL Status alarm is raised when the PLL loses lock to the currently selected clock source. A Clock Priority alarm is raised with warning (error) severity when the user-defined priority of the currently selected clock source drops below a defined warning (error) threshold. Other alarms in the alarm group monitor the quality of the detected clock signal. If the clock is determined to be unacceptable, the alarm becomes active.

PTP and IEEE 1588v2

Introduction

In opposite to Synchronous Ethernet the Precision Time Protocol (PTP) does not rely on layer 1 synchronization, but on higher layer’s protocol transport. This makes it more independent from physical changes in the network and - in principle - a partial introduction into the network is possible. PTP is written in [IEEE 1588] an now released in version 2.

PTP does not deliver a frequency, but a high accuracy clock information, allowing all attached devices running time-synchronized to a grand-master clock with less 5 nano-seconds deviation to the master-clock. All the delay in between grandmaster clock and slave clock is calculated by a high sophisticated algorithm, so the slave clock can adjust its clock to the grandmaster.

Four different types of devices can be found in a PTP network:

- Grand-Master Clock (GM): The reference clock for the system. There might be more than one grandmaster in the network. In this case, the “best-Master-Algorithm” will lead to find the reference. If the best-master does fail, the second-best can take over.
- Ordinary Clock Slave (OC): the slave synchronizes its internal clock to the grand-master.
- Boundary Clock (BC): A boundary clock does incorporate slave and master functionality. It does synchronize its internal clock to the grand-master, just as an OC. Towards the subsequent units the BC does act as a master and the subsequent slaves will synchronize to the clock of the BC.
- Transparent Clock (TC): A transparent clock does not synchronize itself to the (grand-) master and does not have an incorporated PTP-engine. But a TC does participate in the PTP-protocol, allowing the slaves to determine the exact delay between grand-master and slave.

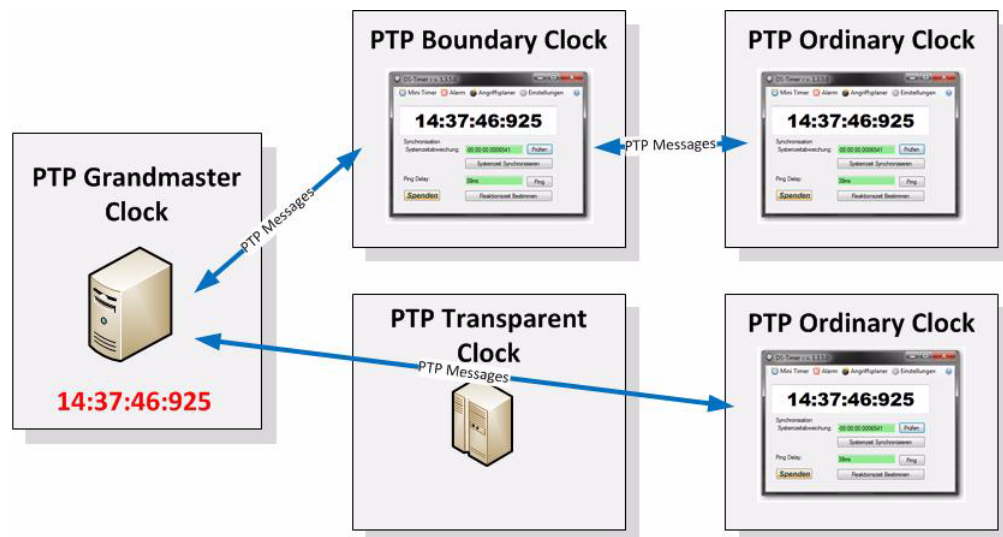


Figure 4-17 PTP Devices

- PTP messages between the devices can be sent across a switched (L2) or routed network (L3). In switched networks special L2-Multicast addresses are reserved for PTP. In L3 networks multicast as well as unicast is defined by IEEE.
- L2 Multicast: 01-1B-19-00-00-00 and 01-80-C2-00-00-0E.
- L3 Multicast: 224.0.1.129 and 224.0.0.107.
- For L3 Unicast IEEE 1588-2008 introduces an option for devices to negotiate unicast transmission on a port-by-port basis. This is supported by ENX.

For more details about PTP please refer to internet. A detailed understanding of the protocol is not required for usage of ENX and would go beyond the scope of this manual.

L2 MC-MAC Addresses

The communication with the other PTP clock in the network uses several different types of packets.

- Peer delay (PD) mechanism messages
- All except peer delay (nonPD) mechanism messages

IEEE and ITU-T do recommend slightly different usage of MAC addresses. For this reason, ENX can be widely configured. The default is the IEEE recommendation.

Table 4-6 PTP Multicast MAC Addresses

Name	Abbr.	MAC Header	
		IEEE	ITU-T
Peer delay (PD) mechanism messages	PD	01-80-C2-00-00-0E	01-80-C2-00-00-0E
All except peer delay (nonPD) mechanism messages	nonPD	01-1B-19-00-00-00	01-80-C2-00-00-0E

Implementation

ENX's implementation for PTP is the implementation of a Boundary-Clock. Each port can be configured to be a PTP-slave, a PTP-master or non-PTP. If no port is configured to be PTP-master, the ENX is just an OC-slave. It is also possible to use the ENX as PTP.master (OC), if no slave-port is configured. So the implementation of BC offers all possibilities.

All ports can be freely configured to be PTP-master, PTP-slave or no-PTP. Standard configuration is LINE 1 and/or LINE 2 as PTP-slave, LAN 1 - LAN 4 as PTP-master or no-PTP.

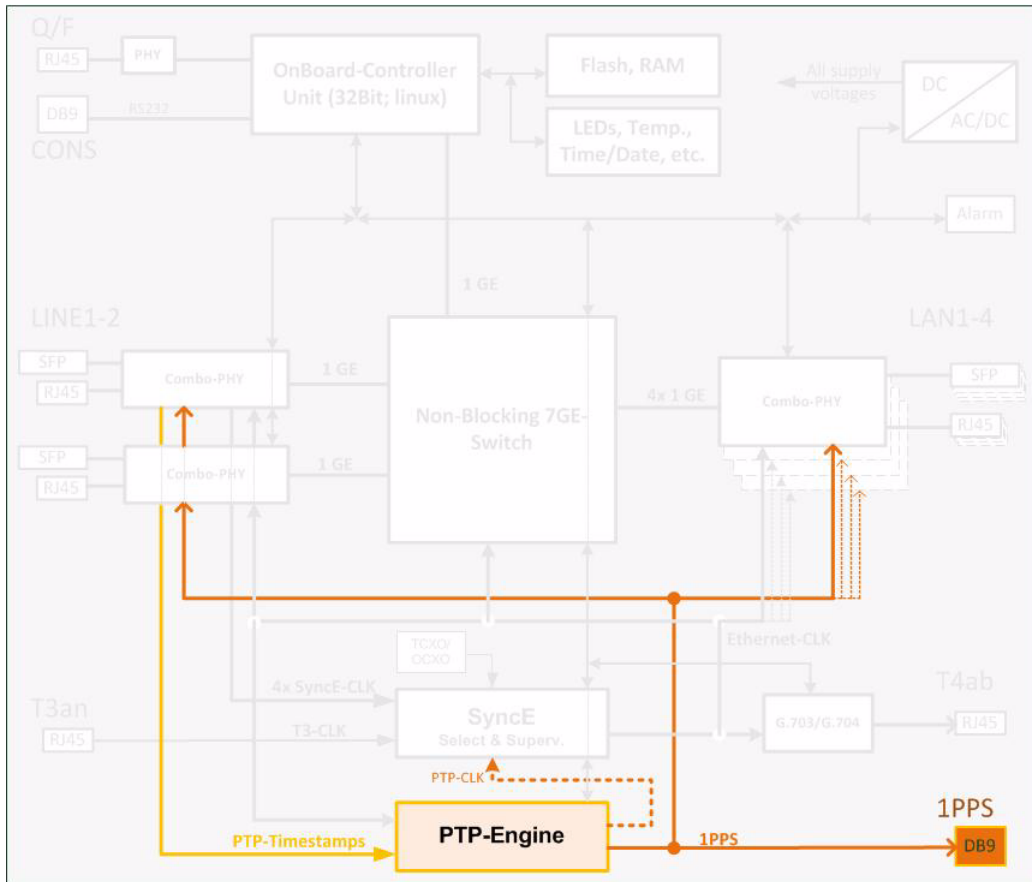


Figure 4-18 Block Diagram for PTP

To achieve best results in the PTP the ENX does stamp the incoming and outgoing PTP-packets almost on the edge of the device. This avoids internal calculation errors due to uncertain packet delays within the device. Special PHYs (Physical interface) are used to make sure that no additional non-monitored and/or unpredictable delay is added in the device. This is the base for very accurate calculations and very small deviation as well between ENX and Grandmaster, but also between ENX and subsequent Ordinary Clocks.

PTP-Messages

For the time being the ENX supports Layer2-Multicast packets for distributing PTP-packets. The following MAC addresses are used:

Message types	Address (hex)
All except peer delay mechanism messages	01-1B-19-00-00-00
Peer delay mechanism messages	01-80-C2-00-00-0E

Grand-Master

It is foreseen that several PTP-Grandmasters can be installed in the network. The ENX supports the “Best-Master-Clock Algorithm” (BMC) to find the best Grandmaster in the system. If this GM fails, the ENX will search again for the next-best to keep PTP-updates.

The clock-ID of the Best-Master (BM) is stored on the device and can be read via management applications. Any change of the BM can raise an alarm, warning or can be ignored.

PTP Analysis

The ENX - Synchronous Ethernet Network Termination has a built-in logging function for the PTP engine. The device does store at dedicated point of time the actual result of the PTP algorithm: The actual Path-Delay (PD) to the Grandmaster and the actual Clock-Offset to the Grandmaster.

The time frame, which can be observed can be up to 1130 days (more than 3 years).

The stored values of PD and Offset can be exported to a server and analyses with calculation tools like Excel. The analysis can show changes in the network (changed PD) and availability. Mean value and standard deviation can be calculated to show the quality of the clock and as a result adjustments can be carried out.

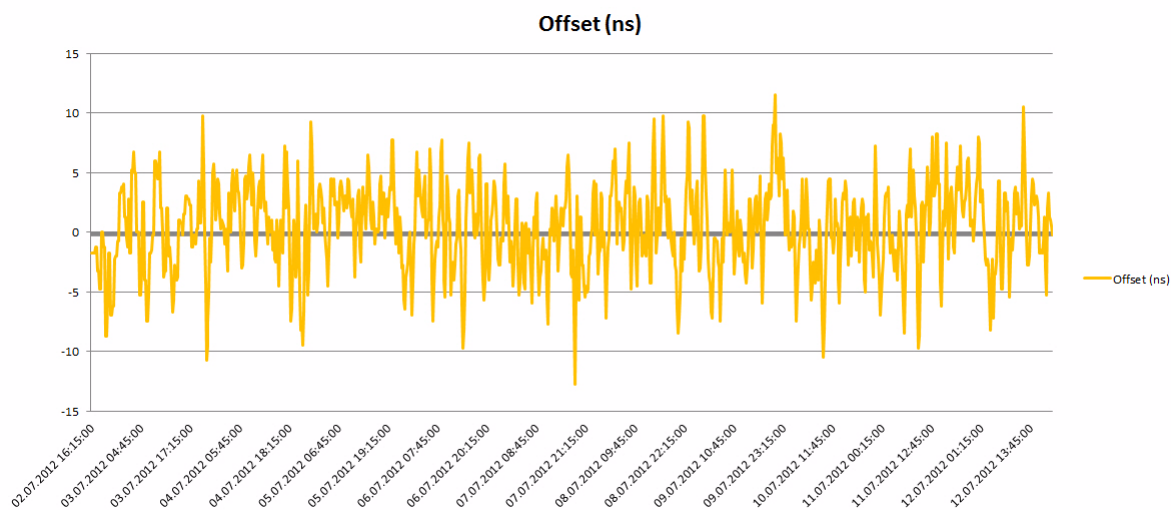


Figure 4-19 PTP Analysis: Offset

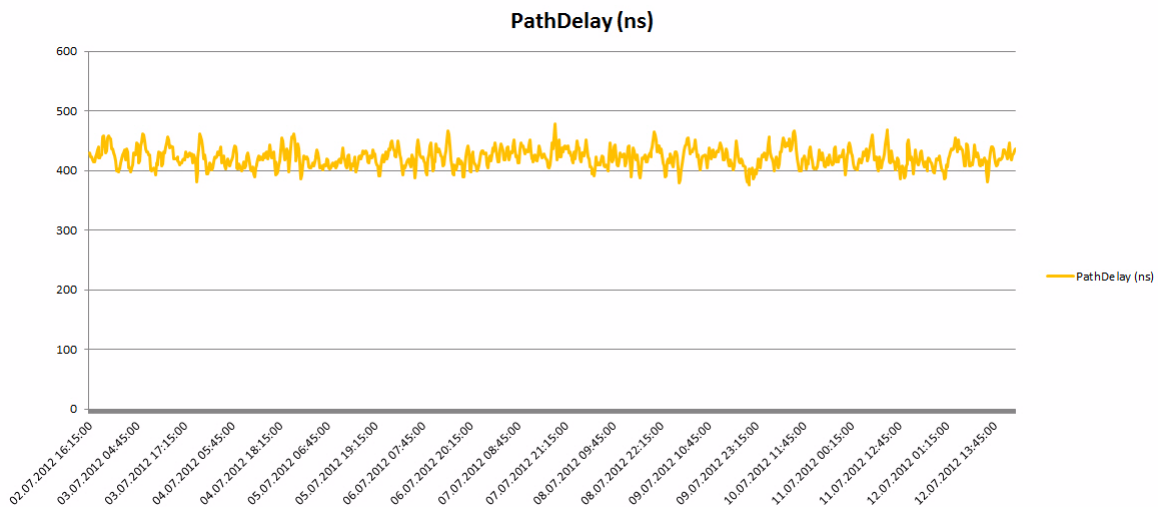


Figure 4-20 PTP Analysis: Path Delay

When the PTP-logging is stored, the device gathers also all the available entries in the system logging, which are correlated the PTP-engine like link status, PTP-GM ID, etc. As the PTP-logging can run over a long very time-frame, the actual system log may not allow to collect messages for the complete time-frame, but only a smaller amount.

User & Access Administration

Access-Options to the ENX

The ENX offers several physical ways to get access to the device together with different options to authenticate and authorize. In total, one can differentiate four protocol stacks, which are supported. These four protocols to get management access to the ENX are

- HTTP (Web-based GUI via TCP/IP)
 - See Chapter 5, ENX Web-GUI, and [axRefGuideWebGUI_ENX].
- SNMP (including traps)
 - SNMPv2c and SNMPv3 are supported.
 - See Chapter 6, SNMP and MIBs.
- SSH-CLI (command-line-interface via secure shell)
 - See Chapter 7, SSH and CLI, and [axRefGuideCLI_ENX].
- CONSOLE-port (command-line-interface via RS-232)
 - See Chapter 7, SSH and CLI, and [axRefGuideCLI_ENX].

All four access-options can be disabled individually, but at least one of them must be active.

NOTE: If the last of the four access-options shall be disabled, the ENX will deny to accept this.

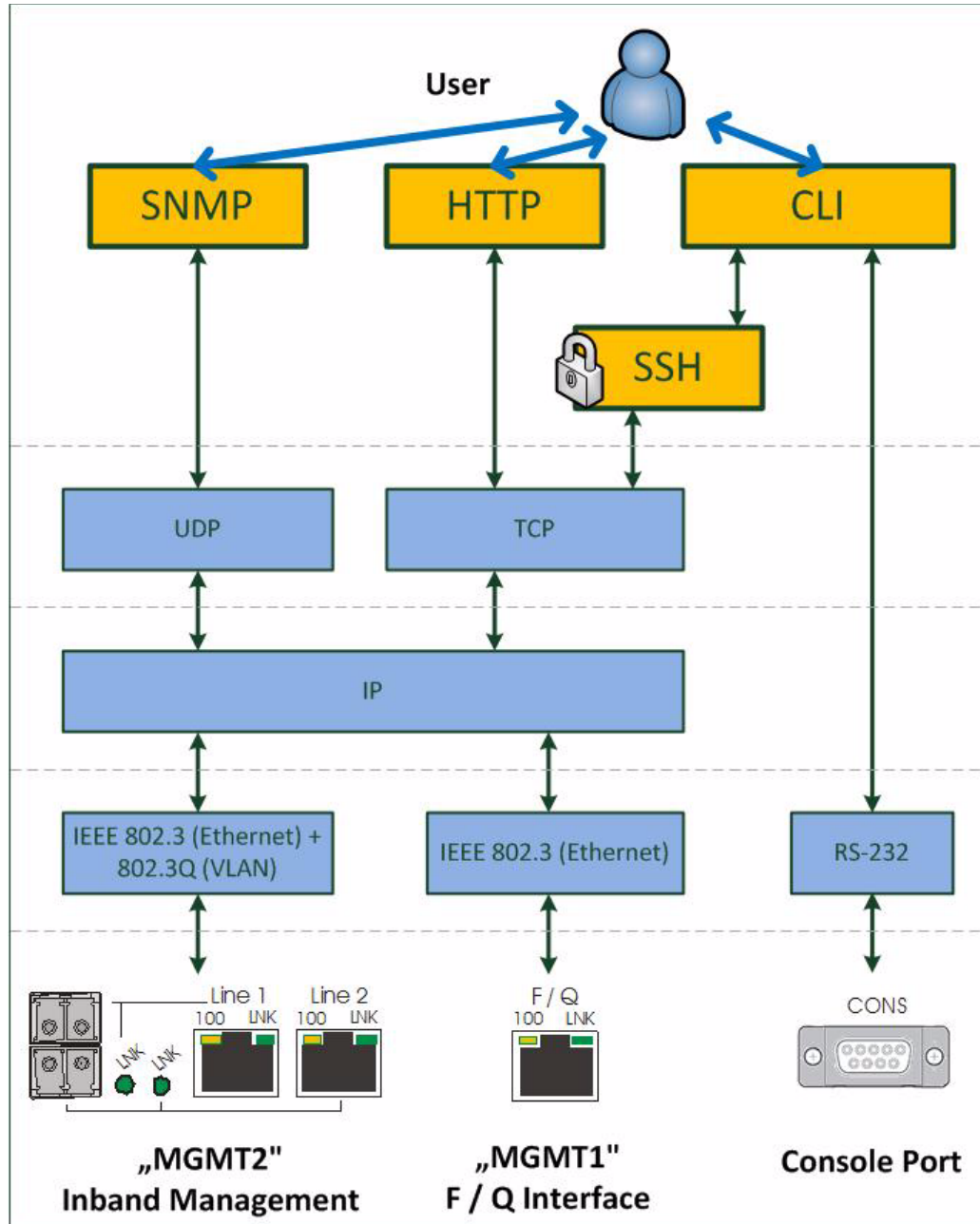


Figure 4-21 Management Protocol Stack

Figure 4-21 shows the protocol stack for the management access to the ENX and the attestant physical interfaces to be used.

SSH-Access

The SSH-access offers a secure connection to the device. Keys and passwords might be used to make the communication safe and secure. If required by the user, the SSH access can be disabled at all, to avoid illegal access to the device. In factory default, the SSH access is enabled.

Details about the usage, configurations and options of the SSH-access is written in Chapter 7, “SSH and CLI”.

User Administration

All the different access-options to the ENX are protected by user-name and password. Several users can be configured on the ENX 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 ENX locally with access-level, user-name and password. Or it can be stored on a NAS (Network Access Server). When a NAS is used, the protocol TACACS+ is used.

The administrator of the ENX can decide, whether the locally stored users, the TACACS-users or both shall be accepted and access granted. Any not successful attempt to login to the device is stored in the log-file and a trap can be configured to inform higher level management system about this.

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 ENX 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 ENX. 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.

TACACS+

On ENX, TACACS+ is used to have central login administration in opposite to locally stored user-names and passwords.

Terminal Access Controller Access-Control System Plus (TACACS+) is an access control network protocol for network access devices and other networked computing

devices. TACACS+ provides separate authentication, authorization and accounting services. TACACS+ is an open, publicly documented protocol.

TACACS+ separates authentication and authorization in a user profile, which makes it more secure than other access control protocols. Another benefit is the usage of TCP instead of UDP.

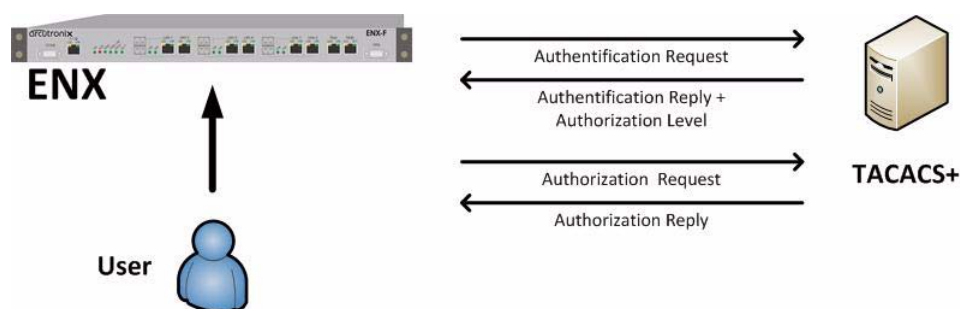


Figure 4-22 TACACS+

When TACACS+ is enabled on the device the IP-address of the TACACS+ server and the shared secret for secure communication has to be configured. Time-outs can be defined to avoid endless waiting in case the TACACS+ server is not reachable due to network problems, bad configuration or unattainability of the server.

When TACACS+ is enabled, it can be selected, whether the local users shall still be accepted or not. And if yes, whether the local user data-base shall be preferred or not.

TACACS Example Configuration

The configuration of users and their adjacent access levels are done on the TACACS+ server with the help of a configuration file. The conf-file is written in ASCII and can be easily edited. A simple example for such a configuration file is listed below. Read the manual of your TACACS+ server carefully for further options.

```
#-----
#
# EXAMPLE CONFIGURATION T A C A C S +
#
#-----
# Shared secret to TACACS+ server
key = public
#
#
# Configure User(s)
user = andreas {
#
# user andreas is not a member of any group
login = cleartext "maxjonas"
#
# Access-level definition for user andreas:
service = management {
    priv-lvl = 8      # number between 0..15
                    # guest = 0; user = 1-7; admin = 8-15
}
}
```

```
}  
# repeat this for all users  
# ...  
#  
#  
# End file
```

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 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.

Protocol-Based Auto-Logout

A CLI-over-SSH session will be automatically terminated, when the SSH-link is closed.

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 ENX can be managed via different protocols using the TCP/IP stack (see Figure 4-21) across the management interfaces “MGMT 1” (F/Q-interface) and “MGMT 2” (in-band port).

Both ports need a valid IP configuration (host address) and the physical layer (“Port Settings” of both can be configured.

Port Settings

The port settings of the management ports are the physical setup and status (Layer 1). The ports can be enabled and the speed and duplex capability can be defined. In standard networks it will be the best to keep the autonegotiation feature of the port, but it might be necessary to adopt this. Autonegotiation options are depicted in chapter “Auto Negotiation” on page 4-46.

The name of the port can be adopted to make it better readable and more meaningful for user. This name will be used in traps, which can be enabled to announce changes in the link state of the ports.

Some entries show the status of the port and some high-level counters to see whether the port is operational and working or not.

If the MAC address of the port is needed for other application, one find it here as an read-only entry.

NOTE: The MAC address of a port can not be changed by user.

Management Port “F/Q MGMT”

For F/Q MGMT nothing more than the above mentioned must be noted here. Nothing special to be considered.

Management Port “Inband MGMT”

In-band MGMT is slightly different as it does not has one single dedicated physical port but does use the configured LINE-ports in parallel to other payload data. For this rea-

son, there might be more than one single physical interface, which can carry information dedicated to and from in-band MGMT.

Each of the interface, which are configured as “LINE” (= belonging to the LINE Port Group) do have individual settings for the physical layer.

IP-Addressing

Both ports need to be configured with a valid host-address before usage is possible. Defaults are stored on the device, but these will seldom fit into the given environment.

Both ports do support manual address assignment as well as the dynamic host configuration protocol DHCP.

NOTE: The host address of the two ports **MUST** be in different IP-subnets, otherwise the dive will have unpredictable behaviour and IP-based communication will not work correctly.

The Default GW and the TTL-value (time-to-live) is a global settings, valid for both ports. So this setting is not related to one of the two ports, but a common part which can be configured globally.

Management Port “F/Q MGMT”

The out-of-band management port F/Q MGMT can be used in local (F-interface mode) and remote (Q-interface mode), which has influence on the IP-address scheme. The different behaviour are depicted in “F- and Q-Interface” on page 4-42.

To integrate F/Q MGMT into a larger network management environment, it can be configured to use VLAN-tagging on the port. This makes only sense, when it is operated in Q-mode, as the F-mode is for real local access. The VLAN-tagging can be enabled on demand and all valid VLAN-IDs can be used. This VLAN-ID is really separated on the device and does never interfere with other VLAN-IDs configured, e.g. for the payload or in-band traffic.

- Default Mode: F-interface
- Default IP-address: 192.168.1.100/24
- Other Defaults: Act as DHCP-Server

Management Port “Inband MGMT”

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. Provider VLAN-tagging (Double-tagging) is possible and can be enabled additionally.

As the in-band management port is operating as DHCP-client by default, a DHCP-server will be searched at the beginning. The server’s address and the resulting settings can be verified on the unit.

- Default IP-address and mask: <empty>

- Default VLAN-ID: 4094
- Other Defaults: Act as DHCP-Client



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

DHCP and Manual Address Assignment

The IP-address of the two management ports can be assigned by an DHCP-server or manually. If an DHCP-server is used, it must be connected to the interface. If no DHCP-server is available for this interface (or just not reachable), the unit starts with the Default IP-address of the interface (see above).

Note: We have sometimes seen problems with DHCP communication over some available USB-to-Ethernet adaptors. This problem is not related to ENX, 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 ENX is reachable within the existing IP-network. It makes no difference whether the communication uses the out-of-band or in-band interface.

F- and Q-Interface

F- and Q-interface are two different behaviours of a management interface port.

The behaviour of an interface configured as “F-interface”, is defined by ITU for local access. The F-interface implementation of arcutronix does incorporate a DHCP-server, which makes it very easy to connect your laptop via Ethernet-cable. In your standard laptop configuration, it will get a valid IP-address from the ENX and the IP connection can be used.

NOTE: The DHCP-server can only assign one(!) IP-address, so it makes no sense to connect a complete LAN to this port, using the ENX as DHCP-server for the LAN!

If the interface shall be used for remote access, the proper configuration will be “Q-interface”. In Q-interface mode, the ENX will act as a DHCP-client and gets an IP-address via the connected network (as long as a DHCP-server is setup somewhere in the network).

The configuration of the F/Q-interface to the proper mode can be done via all management protocols. A short-cut to switch quickly between the modes is using the CONS-interface:

```
$>F [ip <ip-address>] [netmask <netmask>] [nodhcp]
```


makes it a F-interface. If no IP-address is specified, the IP-address will be set to 192.168.1.100. For an explanation of all options, see “Short-cuts” on page 7-18.

```
$>Q [ip <ip-address>] [netmask <netmask>] [vlan <vlan-id>] or
```

```
$>Q [dhcp] [vlan <vlan-id>]
```

makes it a Q-interface. An IP-address need not to be specified, the interface can be configured to be DHCP client. For an explanation of all options, see “Short-cuts” on page 7-18.

DNS-Support

ENX does support name service (DNS) to support easy access to the device. In f-interface mode, one can reach the ENX by using “ax-<device-type>” instead of the IP-address. For the ENX-F it would be **ax-ENX-F**.

An example is shown below. The ENX-F has been assigned the IP-address **192.10.4.10**. A ping-command will result in the following:

```
C:\> ping ax-ENX-F

Ping ax-ENX-F [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:\>
```

Firmware-Update

It might be necessary to update the software (firmware) on the ENX. In this case the new firmware can be uploaded to the device via several ways:

- HTTP, TFTP and SFTP

Only SFTP is a secured way to upload the new firmware and is highly recommended to be used. See chapter “File-Transfer to/from Servers and via HTTP” about the configuration and usage of the different protocols.

The update-file has the extension “*.upx” and is a special arcutronix file format. It is secured by a checksum and other mechanism to make sure only correct files will be accepted for firmware update. If the file transfer did not work properly or any other damage of the update-file is discovered, the new file will not be accepted for update.

NOTE: A corrupted file can be uploaded to the ENX, 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, one can start the proper update. When update (not upload) is started, the unit will do a reset right after successful installation of the new firmware. If the update process did not work properly, or the new firmware does not start correct, the old FW-version will be used instead. The old version will be stored on the device till the next update process.

File-Transfer to/from Servers and via HTTP

The ENX can upload and download different files for internal usage or external storage:

- New Firmware-Update file to be used on the device to offer new features:
 - Files need to be loaded onto the device.
- Actual configuration can be stored externally for backup or further usage:
 - Files need to be stored on a server.
- Profile configuration can be installed for quick setup of the device:
 - Files need to be loaded onto the device:
- Log-files can be stored externally to be analysed:
 - Files need to be stored on a server.
- SSH-keys can be stored on the device for proper authentication:
 - Files need to be loaded onto the device.

For these storage- and loading-operation of files three ways are foreseen in the ENX:

- HTTP, TFTP and SFTP

NOTE: Only SFTP is a secured way for file transfer and it is highly recommended to use SFTP.

The different ways of file-transfer to diverse servers and the direction of up- and download is shown in the following picture:

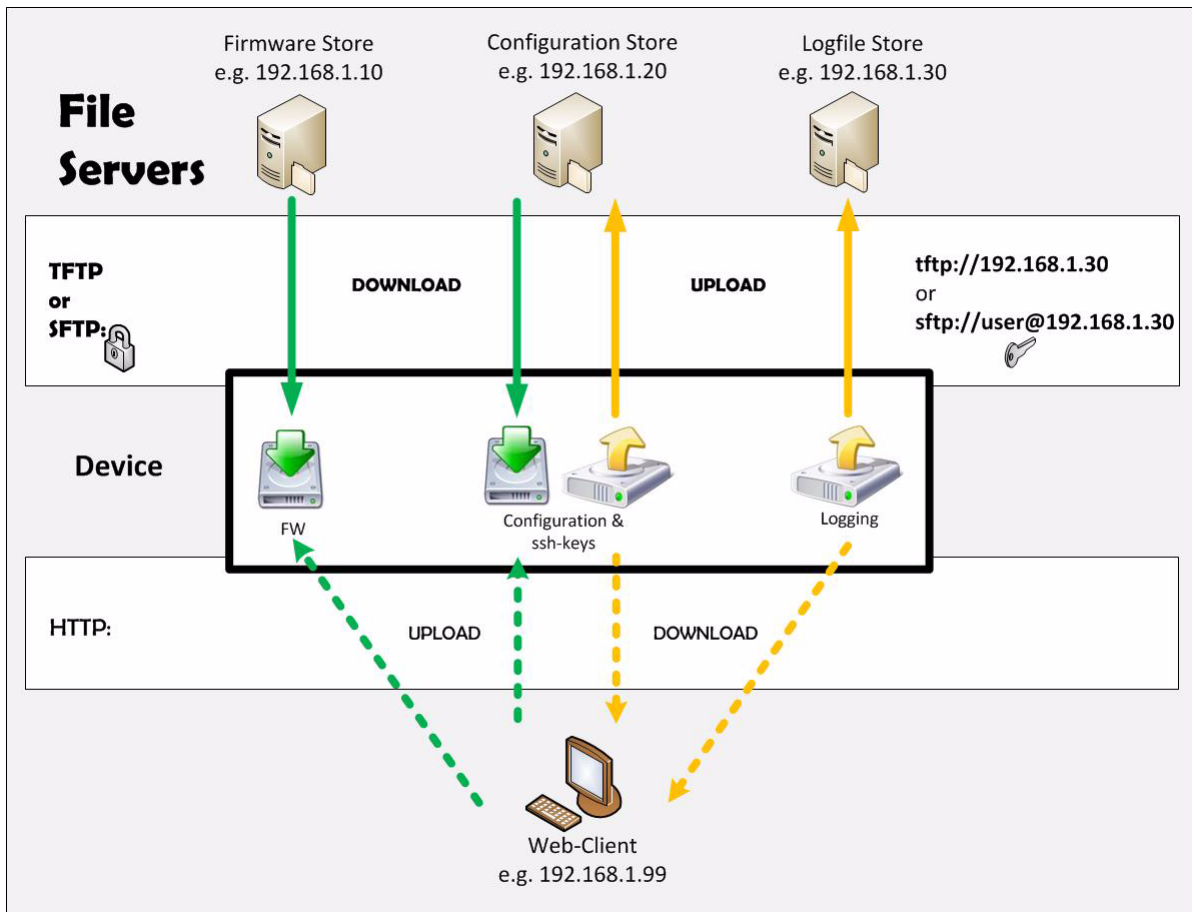


Figure 4-23 File-Transfer

While SFTP and TFTP are providing download from the server to the device, the http protocol is uploading to the device. The same opposed naming applies for the transferring files from the ENX to a server.

SFTP and TFTP

Three servers can be configured for SFTP or TFTP file-transfer:

1. Firmware-Store to download new firmware
2. Configuration Store to download config-files and SSH-keys and to upload config-files
3. Logfile Store to upload log-files.

The 3 servers can use the same IP-address, but for security reasons the servers can be divided to different physical locations and use different rights of access. For each server it can be defined, whether it speaks SFTP or TFTP and the proper user settings must be made before usage.

If no valid server settings are provided, no SFTP and TFTP access is possible.

Note: If the usage of SFTP or TFTP must be disabled, just avoid valid settings.

HTTP

The usage of HTTP for file-transfer is a very easy (and insecure) way to move files with the help of your browser. In the http-case of file-transfer, the ENX is acting as the (web-)server and the user at the terminal can upload and download files to it.

HTTP-file transfer can be disabled entirely due to security reasons.

NOTE: The usage of http is only possible via a http-session and not available for SSH or CLI applications!

WARNING: When the file-dialogue windows is opened for file-selection or storage, a security feature is implemented to avoid uncontrolled usage: After a time-frame of 5 minutes with opened file-dialogue, the user will be logout from the system automatically.

Miscellaneous Features

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, ENX 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 4-7 Settings Auto-Negotiation

Setting (Port Speed)	Speed	Result	
		Duplex	Remark
Automatic	10, 100 or 1000 Mbps ⁱ	Full or Half Duplex ⁱⁱ	Full Auto-neg takes place; no limitations are given. The variable "Autonegotiation" is not changeable, but always "ON".
10 Half Duplex	10 Mbps	Half Duplex	Auto-neg communication with peer can be enabled via the "Autonegotiation" variable.
10 Full Duplex	10 Mbps	Full Duplex	Auto-neg communication with peer can be enabled via the "Autonegotiation" variable.
100 Half Duplex	100 Mbps	Half Duplex	Auto-neg communication with peer can be enabled via the "Autonegotiation" variable.
100 Full Duplex	100 Mbps	Full Duplex	Auto-neg communication with peer can be enabled via the "Autonegotiation" variable.

Table 4-7 Settings Auto-Negotiation (continued)

Setting (Port Speed)	Speed	Result	
		Duplex	Remark
1000 Half Duplex ⁱⁱ	1000 Mbps	Half Duplex	Auto-neg communication with peer can be enabled via the "Autonegotiation" variable.
1000 Full Duplex ⁱⁱ	1000 Mbps	Full Duplex	Auto-neg communication with peer can be enabled via the "Autonegotiation" variable.

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

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

Clock

The auto-negotiation process is absolutely important to find the right settings for Copper-based ports. As the Gigabit-Ethernet traffic via Copper (1000BaseT) is a real duplex traffic, the peers need to agree upon the clock-source for the link. In standard Ethernet, this is free choice and one of the two peers will be clock-master for the link. When SyncE is enabled, the choice is not longer free, but it must fit the SyncE demands: The SyncE-master MUST be clock-master for the link and the SyncE clock-slave accordingly.

So two things have to be considered when SyncE is enabled:

- On both sides of the 1000BaseT link, auto-negotiation must be disabled
- The clock-settings on both sides of the 1000BaseT link must match.

The ENX raises an alarm, if the auto-negotiation process does fail.

EFM OAM

OAM (Operation, Administration, and Maintenance) describes the monitoring of network operation by network operators. OAM is a set of functions used by the user that enables detection of network faults and measurement of network performance, as well as distribution of fault-related information. OAM may trigger control plane or management plane mechanisms, e.g. by activating rerouting or by raising alarms, but such functions are not part of the OAM itself.

Ethernet originated as a Local Area Network (LAN) technology. Since LANs usually consist of a relatively small number of co-located stations, all managed by a single entity, defect detection was manual, and performance was never really a concern. As

Ethernet developed, physically separated LANs were interconnected but still managed by a single entity (although now an enterprise). OAM was still not a major concern, and network defects were handled by manual activation of simplistic tools such as ping. In order to enable Ethernet service providers to operate and maintain their networks, there is a need to include OAM on the Ethernet layer. This new OAM must integrate seamlessly with existing Ethernet protocols in order to encourage its adoption while enabling coexistence with conventional non-OAM-capable Ethernet devices.

Belatedly, two Ethernet OAM protocols have emerged. One has been developed for “Ethernet in the first mile” (EFM) applications, operating at the level of the single link, while the other tackles the wider problem of end-to-end Ethernet connectivity and service guarantees. The link-layer OAM was developed by the 802.3ah EFM task force in the [IEEE 802.3] working group, and thus is often called the “802.3ah” or “EFM” OAM.

The service-layer of Ethernet OAM is covered by IEEE as well as ITU-T. In the IEEE the work is being conducted under the name 802.1ag (Connectivity Fault Management), while in the ITU-T the draft Recommendation was known as Y.17ethoam, although it is now called [ITU-T Y.1731].

EFM (802.3ah) Link-layer OAM

As mentioned before, Ethernet link-layer OAM was developed for “Ethernet in the First Mile” (EFM) applications. The capabilities of link-layer OAM are limited, being restricted to placing the remote device into loopback, setting flags indicating critical events, and querying the remote device’s configuration. There is no performance measurement and the information exchanged about the state of the link being monitored is minimal. More significantly, since this OAM is limited to a single link there can be no AIS indication of failure of a previous path segment and thus no end-to-end service guarantee.

IEEE link-layer OAM operates purely at the Ethernet layer, and so (unlike SNMP or ping) does not require an IP address. This means that Ethernet service providers don’t need running IP protocols or manage IP addresses. Furthermore, special Ethernet features may be directly supported, such as Ethernet multicast and slow protocol frames.

Link-layer OAM messages are sent in untagged slow protocol frames called OAM Protocol Data Units, or OAMPDUs. Slow protocols are protocols used to control operational characteristics of the Ethernet device, such as the Link Aggregation Control Protocol (LACP, “Link Aggregation with LACP” on page 4-21) which also utilizes slow protocol frames. Slow protocols are slow in the sense that they are restricted in the number of protocol frames that may be transmitted per second (for OAMPDUs – no more than 10 frames per second), thus facilitating software implementations of the OAM client.

Alarm Management

The ENX does have an outstanding alarm management, which allows users to get a quick overview of the current device status, but also to get detailed information about individual alarm states. The alarms are grouped by function or hardware component, each group can be configured and acknowledged as group. Or one can navigate into the groups and configure each alarm in detail for the personal preferences.

Alarm Types

In general terms, an alarm monitors the value of a certain quantity for exceptional values. If such an exceptional value is detected, the alarm condition is said to be active. Depending on the configuration of the alarm, this may cause the alarm to become active as well.

There are two fundamentally different types of quantities that can be monitored by alarms. The first one are quantities that have a well-know set of discrete states, some of which may represent exceptional values. An example is the link state of an ethernet interface which may have the states “Link Up”, “Link Down”, and “Port Disabled”. Here “Link Down” represents the exceptional value that causes the alarm condition to become active. Alarms that monitor these discrete-state quantities are called **digital alarms**.

The second type of quantities represent physical quantities that usually vary continuously. Here, exceptional values are defined in terms of thresholds that limit the acceptable operational range for the physical quantity. Depending on the quantity being monitored, the device checks upper and/or lower bounds for the acceptable operational range and allows to define the corresponding threshold values. An example of this type of variables is the device temperature, for which an acceptable operational range may be defined as -20°C ... 60°C. Alarms that monitor these continuously varying quantities are called **analogue alarms**.

NOTE: For analogue alarms it is possible to define the warning level at a higher value than the error level. E.g. for the temperature it is possible to define the warning @60°C and the error @55°C. This is not forbidden by the system, as there might be customer’s reason to do so.

Alarm States

The state of each alarm is determined by several factors.

The first one is the **alarm condition**. The alarm condition can be unavailable which means that the quantity being monitored is not well-defined, which may occur due to the current device configuration. In case of the Ethernet interface example above, the link status is not defined if the Ethernet port is disabled by the administrator. The alarm condition can also be active or inactive, which indicates that the monitored quantity has an exceptional value or indicates normal operational conditions, respectively.

The second factor that affects the alarm state is the alarm configuration. It may affect the state of the alarm when the alarm condition becomes active, but it may also define parameters for detecting the alarm condition:

- Alarm configuration can force the alarm condition to be ignored.
- Alarm configuration can limit the severity of an active alarm.
- Alarm configuration specifies the severity with which an active digital alarm is reported.
- Alarm configuration specifies the Hold Time for an active alarm.

- Alarm configuration specifies the thresholds and hysteresis used to detect alarm conditions for analogue alarms.

The third factor that affects the alarm state is alarm acknowledgement. Once the device operator has received knowledge of the occurrence of an active alarm, he can indicate this to the ENX device by acknowledging the alarm. The ENX device will then ignore this alarm in the calculation of the global device alarm state so that newly occurring alarms will immediately be brought to the operators attention.

Given all the influences explained above, the alarm can be in one of the following states:

Not Available

This indicates that the alarm condition is not available. The alarm is always considered to be inactive in this case and the corresponding alarm state value is “n.a.”.

Inactive

This indicates that the alarm condition is inactive. The alarm is always considered to be inactive in this case and the corresponding alarm state value is “Ok”.

Ignored

This indicates that the alarm condition is active, but the alarm condition was configured to be ignored. The alarm is always considered to be inactive in this case and the corresponding alarm state value is “Ignored”.

Acknowledged

This indicates that the alarm condition is active and the alarm is not configured to be ignored. However, the device operator has acknowledged the alarm and the corresponding alarm state value is “Acknowledged”.

Warning

This indicates that the alarm condition is active and the alarm is considered to be active, having a severity of “Warning”.

This state occurs for analogue alarms if a warning threshold has been crossed, but the corresponding error threshold is not yet reached. This state occurs for digital alarms if the alarm was configured to be a “Warning” by the device administrator.

A warning level usually indicates that the device is operating close to the limits of the operational parameters and that actions should be taken to ease the situation.

Error

This indicates that the alarm condition is active and the alarm is considered to be active, having a severity of “Error”.

This state occurs for analogue alarms if an error threshold has been crossed. It occurs for digital alarms if the alarm was configured to be an “Error” by the device administrator.

An error level usually indicates that the device is operation outside of the limits of the operational parameters and that the device is no longer operating reliably.

Alarm Acknowledgement Behaviour

Any active alarm can be acknowledged by the device operator. Even though the alarm condition is still active, this has the effect of making the alarm “silent” by excluding it from the global device alarm state calculation. Informally speaking, this makes the alarm a “known problem”.

It may happen that the alarm severity changes while the alarm is acknowledged. In case of analogue alarms this may happen if an additional threshold is crossed, whereas for digital alarms it implies a configuration change. In any case, the severity of the acknowledged alarm may either increase (from “Warning” to “Error”) or decrease (from “Error” to “Warning”). Any other value (“Ignored”, “Inactive” or “Not Available”) means that the alarm becomes inactive.

The device administrator can select from three different policies that decide whether the alarm gets reactivated by the alarm severity change or remains acknowledged. This is a global setting and valid for all alarms.

Keep Acknowledged Until Inactive

This policy keeps acknowledged alarms in their acknowledged state until the alarm becomes inactive. Neither the increase nor the decrease of the alarm severity have any effect.

Unacknowledge When Raising Severity

This policy keeps the alarm acknowledged as long as “the situation gets better”. When the severity decreases from “Error” to “Warning”, the alarm remains acknowledged. However, if the situation gets worse and the alarm severity increases from “Warning” to “Error”, the alarm is reactivated and brought again to the device operators attention. This is the default behaviour.

Unacknowledge on State Change

This policy will always reactivate an acknowledged alarm whenever the alarm severity changes.

Example

The next figure displays an example, of temperature alarm and the behaviour when alarm is raised, acknowledged and raised again.

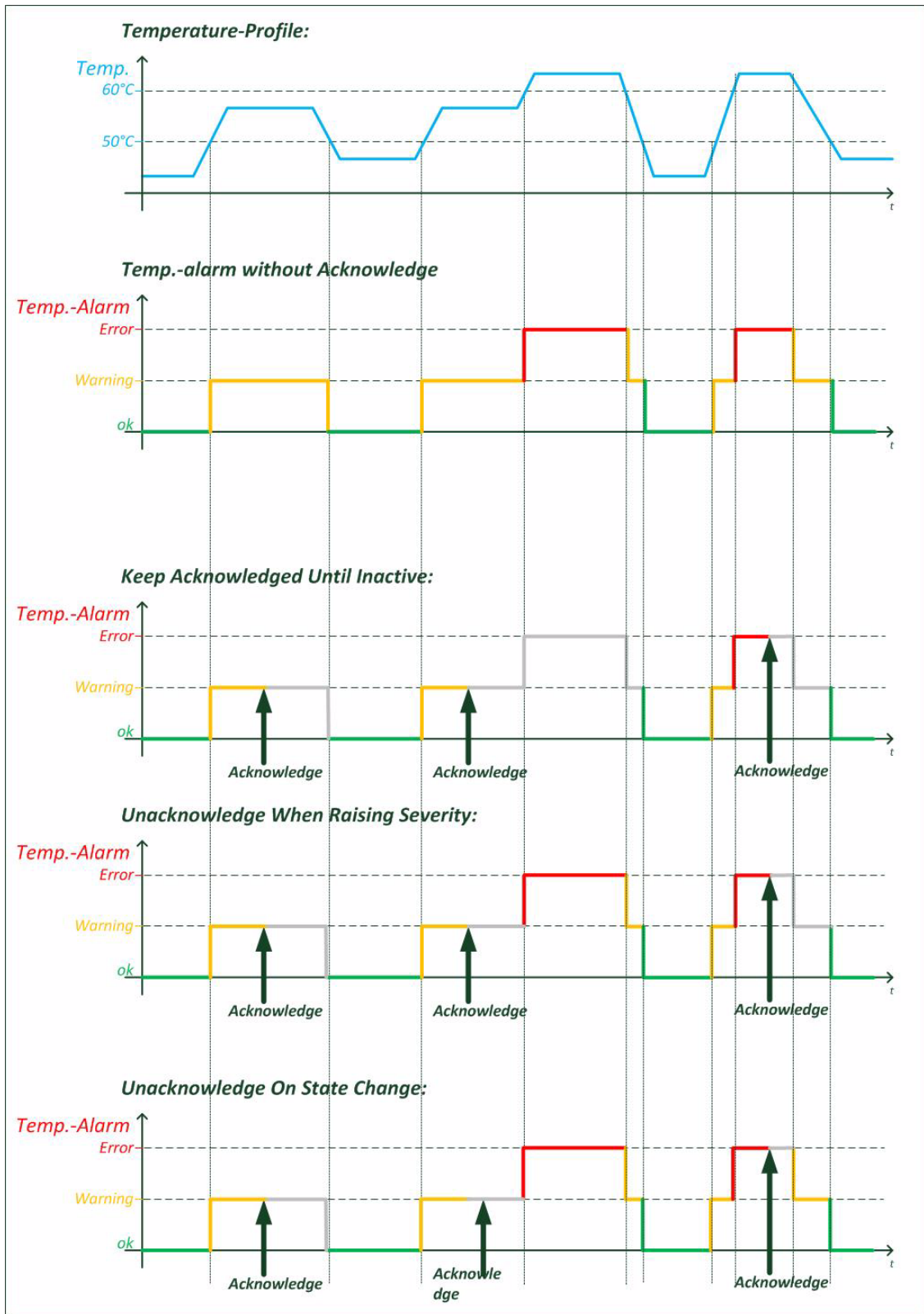


Figure 4-24 Acknowledge of Alarms

Alarm Properties

Each alarm has a certain set of properties associated with it that depends on the alarm type (analogue or digital alarm).

Common Alarm Properties

These properties are defined for both, analogue and digital alarms.

- Alarm Group: the group that the alarm belongs to (see below).
- Alarm Name: a descriptive name of the alarm.
- Alarm Value: the current value of the observed quantity.
- Alarm State: the current alarm state.
- SNMP Notification: whether to generate SNMP traps if the alarm state changes (editable).
- Hold Time: The hold time indicates the minimum time an alarm is active after rising. This is to reduce the number of alarms in a certain time-frame and to tune the system to special requirements.

Digital Alarm Properties

Digital alarms have one further property:

- Alarm Severity: the device administrator must decide for each digital alarm whether it represents an error condition, a warning condition, or an ignorable condition (editable).

Analogue Alarm Properties

Besides the common alarm properties, analogue alarms have the following properties as well:

- Overrun Warning Threshold: If the physical quantity has a meaningful upper limit for its operational range, the threshold above which the alarm becomes active with "Warning" severity (editable).
- Overrun Error Threshold: If the physical quantity has a meaningful upper limit for its operational range, the threshold above which the alarm becomes active with "Error" severity (editable).
- Underrun Warning Threshold: If the physical quantity has a meaningful lower limit for its operational range, the threshold below which the alarm becomes active with "Warning" severity (editable).
- Underrun Error Threshold: If the physical quantity has a meaningful lower limit for its operational range, the threshold below which the alarm becomes active with "Error" severity (editable).
- Hysteresis: A hysteresis applied to threshold values when checking whether an active alarm condition is cleared (editable).

Alarm Groups

Due to the large number of alarms already defined, the alarms are divided into a number of different alarm groups. These alarm groups serve multiple purposes:

- Logical subdivision of alarms for a better overview.
 - Alarms are grouped by function or hardware component they refer to (e.g. “System Alarms” for general device management alarms, “Clock Alarms” for SyncE and PTP-related alarms, ...)
- Alarm status summary.
 - The alarm group keeps track of the most severe alarm state of any alarm in the group and provides the current number of alarms that are ignored, acknowledged, or are active with “Warning” or “Error” severity.
- Easy acknowledgement of multiple alarms.
 - All alarms within an alarm groups can be acknowledged with a single action.
- Limiting the alarm severity of multiple alarms.
 - The alarm group defines a maximum alarm severity setting that overrides the alarm severity of all alarms in the alarm group.

Global Alarm Status

The ENX device provides a summary of all alarms. Besides showing the number of acknowledged alarm and active alarms with “Warning” or “Error” severity, the global (overall) alarm status keeps track of the maximum severity of any active alarm. Furthermore, the global alarm status is reflected by the ALM-LED on the front panel of the device and the alarm relay.

The ALM-LED will be turned on if the global alarm state is “Error”, it will blink if the global alarm state is “Warning” and be turned off otherwise.

The alarm relay will be activated if the global alarm state is “Error” and be deactivated otherwise.

Active Alarm List

The Active Alarm List is an overview to all alarms which are active at the current moment. When an alarm turns to “Warning” or “Error” it will be added to this list. When the alarm returns inactive state, it will be removed from this list without further notice. Any “ignored” alarm is also not shown in the Active Alarm List.

When an alarm is acknowledged, it will remain in the “Active Alarm List”, but it will be re-sorted at a lower level.

For the time being, the Active Alarm List is ordered by

1. Alarm Severity (Error - Warning - Acknowledged),
2. Group Name (alphanumeric order) and
3. Alarm Name (alphanumeric order).

Date & Time Settings

The ENX does have an internal clock, which can be set by either user or via NTP-server(s). This gives the ENX the chance to provide proper time-stamps in logging and alarms. In case of power-failure, the ENX will keep the correct date and time for a period of at least 10 days.

NOTE: After 10 days without power supply, the internal clock of the ENX has to be re-set again.

If there is no NTP-server is configured in the designated variables, the NTP feature is disabled. In this case, the date, time and time-zone can be specified by user during installation process or whenever needed.

The ENX does support versions and version 4 of NTP:

- NTPv3 ([IETF RFC 1305]).
- NTPv4 ([IETF RFC 5905]).

Up to 8 different servers may be configured on the ENX to make sure always a valid link to an available time-server is found.

When the device can't get (valid) timing information of the given NTP-servers, an alarm can be raised to indicate this problem. The NTP-Status alarm can be found in the System alarm group.

NTP and Encryption

NTP provides an accurate hardware time reference for network infrastructure. It can pose a security risk, particularly if malicious users attempt modifying or replicate time-stamps in order to generate a false time on a networked computer or device.

Therefore the ENX works with authentication on NTP to overcome the inherent security risks and ensuring that any response received from a time server was generated from the intended reference. Basically, the ENX sends a request for time to a NTP-server. The server responds to the ENX with a time-stamp along with any one of a number of pre-agreed encrypted keys. On receipt of the time-stamp, the ENX un-encrypts the supplied key and verifies it against a list of trusted keys. The ENX can then be sure that the received time-stamp was indeed transmitted from the intended server. ENX utilizes MD5 encryption (Message Digest Encryption 5), which is a 128-bit cryptographic hash function, which outputs a fingerprint of the key.

Configuration Management

The (actual) configuration of the ENX can be stored locally and remote (via SFTP) to recall it later or to use it as profile for other devices. The configuration is stored in a special file-format (*.cfgx) which is protected against not allowed changes and keeps the data-base clean and consistent. Any change of settings, which are not made in the correct context could lead into inconsistency and this is avoided here.

It can be necessary that some items of the current configuration shall not be stored, as these settings shall not be used in the future. Or a stored configuration shall not be taken in total, but only partial. A reason could be that the stored IP-address is not longer valid and the actual address shall not be overwritten by the new configuration. For this reason some topics can be selected to be stored or not stored and/or overwritten or kept during (re-) call of configuration:

Item	Description
IP Config F/Q MGMT	All the IP settings for the F / Q interface (out-of-band management port), including: IP-address, net-mask, Default-GW and VLAN-tag (if defined).
IP Config Inband MGMT	All are the IP settings for the in-band management port, including: IP-address, net-mask, Default-GW, VLAN-tag and Provider-VLAN-tag (if defined).
SNMP Trap Targets	All SNMP trap-receiver, including: IP-address, UDP-port, user-name, SNMP-version and state.
SNMPv2 Communities	All defined communities, including: Name, access-level and state.
SNMPv3 User	All defined users, including: Name, authentication, access-level, encryption and state.
SSH keys	All defined SSH-keys, including: Cipher, key-ID, user, comment and state.
User Accounts	All local stored user-accounts, including: Password, user-group and state.
All Other Configuration	All the rest of configuration. Of course this can be not stored or denied during re-call to have e.g. pure account profiles.

Temperature Shutdown

The device does have several temperature sensors to measure and check the onboard temperature. This temperature can be higher than the ambient temperature.

The measured temperature can be read-out via management application and alarms and traps can be raised in case of to high (and to low) temperature.

If the device does detect a critical temperature of ~85°C (onboard), it will shutdown itself for security reasons. 85°C (onboard) equates to approximately 70°C ambient tempera-

ture. The shutdown is an almost complete separation from power supply and will reduce the power demand of the unit to almost 0W. Only a small part will be kept powered to switch on the unit again, as soon as the onboard temperature is below 60°C, equating 45°C ambient temperature. The device's restart is done automatically without the need of any external support.

Before the shut-down, the device can send out an SNMP-trap to inform management system about the coming shut-down and the reason for it. When the device is restarted again due to lower temperate, a cold-start trap will signal the successful restart.

Diagnostics

Wrong IP settings or un-proper setup of cables are often causes for problems in the network. To check all these, the diagnostic-menu is implemented to the ENX. The reachability of a given IP-address of remote host or router can be tested by

- PING command,
- Trace route (via UDP),
- Trace route (via ICMP).

The result is presented as command output and helps to get better view of your (management) network.

Logging

The ENX does provide a logging function, which notices all events in the log-file. This file is stored onboard and the last 999 entries can be (re-)viewed. If necessary the log-file can be stored on a server or downloaded via http.

The events, which are added to the log-file, are divided into 4 groups:

- Information: Messages from the SW about system status and successful started or stopped applications. An information entry is indicated by the <INFO> label.
- Alarm: All variables, which can raise an alarm, will be logged, when the alarm gets error-, warning- or idle-state. An alarm entry is indicated by the <ALARM> label, followed by <ERR>, <WARN> or <OFF>. An alarm-variable, which is configured as "ignore" will not be added to the log-file, independent from its status. It is ignored.
- Audit: The audit entry is added to the log-file, when the configuration of the device is changed by user. This action is logged for better traceability. The audit entry is indicated by the <AUDIT>-label.
- Device-Error: This are failed attempts to login to the device or the device detects an extraordinary status. Device-errors may be solved by the SW itself by restarting applications, but it can be an indicator for severe problems.

Each entry in the log-file has the date/time information, when the event did occur, followed by the type-label and a short description about the event. Some examples are listed below:

<INFO>

```
2013-01-22 09:15:54 < INFO> Rebooting device
2013-01-22 13:01:17 < INFO> Starting HTTP server
2013-01-22 13:01:20 < INFO> System started.
2013-01-22 13:01:20 < INFO> Starting SNMP server
2013-01-22 14:03:25 < INFO> Web login via LOCAL authentication from 192.168.1.1: admin
(admin)
2013-01-22 14:47:08 < INFO> CLI login via LOCAL authentication from CONS: admin
(admin)
```

- The <INFO>-entry gives information about started applications and attempts to login.

<AUDIT>

```
2013-01-22 09:15:54 <AUDIT> Administration/Reset System/Start Reset executed by admin
from CONS (cli)

2013-01-22 14:07:07 <AUDIT> Alarm Management/LAN 1 <...> Alarms/Group Details/Link
Status/Settings/Alarm Severity set to "Warning" by admin from 192.168.1.1 (web)

2013-01-22 14:07:25 <AUDIT> Alarm Management/LAN 2 <...> Alarms/Group Details/Link
Status/Settings/Alarm Severity set to "Ignore" by admin from 192.168.1.1 (web)
```

- The <AUDIT>-entry traces the changes of configuration.

<ALARM>

```
2013-01-22 13:01:05 <ALARM> [ERR] : SFP removed
2013-01-22 14:07:54 <ALARM> [OFF] LAN 1: Link Up
2013-01-22 14:08:16 <ALARM> [WARN] LAN 1: Link Down
2013-01-22 14:08:22 <ALARM> [OFF] LAN 3: Link Up
2013-01-22 14:08:31 <ALARM> [ERR] LAN 3: Link Down
```

- The <ALARM>-entry traces the alarm status of the system.

<ERROR>

```
2013-01-22 14:47:02 <ERROR> CLI authentication failure from CONS: admin
```

- The <ERROR>-entry indicates an unsuccessful try to login.

Chapter 5

ENX Web-GUI

The ENX can be configured via a html-based Web-GUI (Graphical User Interface). Just a standard web browser is needed and an IP-connection to the device. This chapter will explain how to connect to the Web-GUI and its usage.

NOTE: A detailed presentation of all Web-GUI variables and menus is given in [axRefGuideWebGUI_ENX].

Introduction

Access to the Device

The ENX Web-GUI can be accessed via the both management ports (out-of-band “F/Q” and in-band management interface). Both interfaces use different IP-addresses, but the behaviour and the usage from html-point of view is just the same.

arcutronix’ devices are proved to be used with different web browsers:

- Internet Explorer (Microsoft): IE 7 or higher
- Mozilla Firefox (Open Source): Firefox 6 or higher
- Opera (Opera Software ASA): Opera 10 or higher
- Safari (Apple): Safari 5 or higher
- Google Chrome (Google): Chrome 9.0 or higher



Security Issues

The Web-GUI is accessible via any TCP/IP link to the device, so it might be that other persons than the intended ones get connection and will see the login screen. To avoid forbidden configuration or burglary of information, the access is protected against intruders via user-name and password. Any not successful attempt to login to the device is stored in the log-file and a trap can be configured to inform higher level management system about this.

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

Be careful with 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 4-34, how to define the other users and how to change the user password.

Web-Menu Body

Login Screen

After a management connection has been established towards the ENX, the Login screen is displayed. The management software may be accessed by the user with different access levels (see “Security Issues” on page 5-1).

The Login screen is shown in the figure below. For a first quick overview, the type, name, alarm status and the serial number of the connected device is displayed on the top-right side. This makes it easy to verify, whether one has reached the right unit (the entered URL might be wrong or mistyped) and its actual status. If all is fine, it might be no need to login and one can turn towards the next device to check and work with.

The fields user-name and passwords must be filled and after pressing the “Login”-button, the inscription is verified against the local or remote data-base. If the login is accepted, the next screen will open, otherwise the login attempt is denied and one will remain on this screen.

NOTE: A refused attempt to login to the unit is logged.



The screenshot shows the login interface of the ENX Web-GUI. At the top left is the Arcutronix logo. At the top right, there is a warning icon followed by the text "ENX-F: ENX-F" and "Serial: 2012010114". Below this, there is a red horizontal line. Underneath the line, there are two input fields: "User Name" and "Password". Below the "Password" field is a blue "Login" button.

Figure 5-1 Login Screen

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

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 user and password. The entry of strings is case-sensitive.

Layout of Web-GUI

After Login, the ENX Web-GUI is seen in its full glance. The Web-GUI is designed according the latest rules for web-based GUIs and you will find it very easy to navigate.

The Web-GUI's body is divided in 6 major parts, which are shown in the next figure and will be explained a little bit after this.

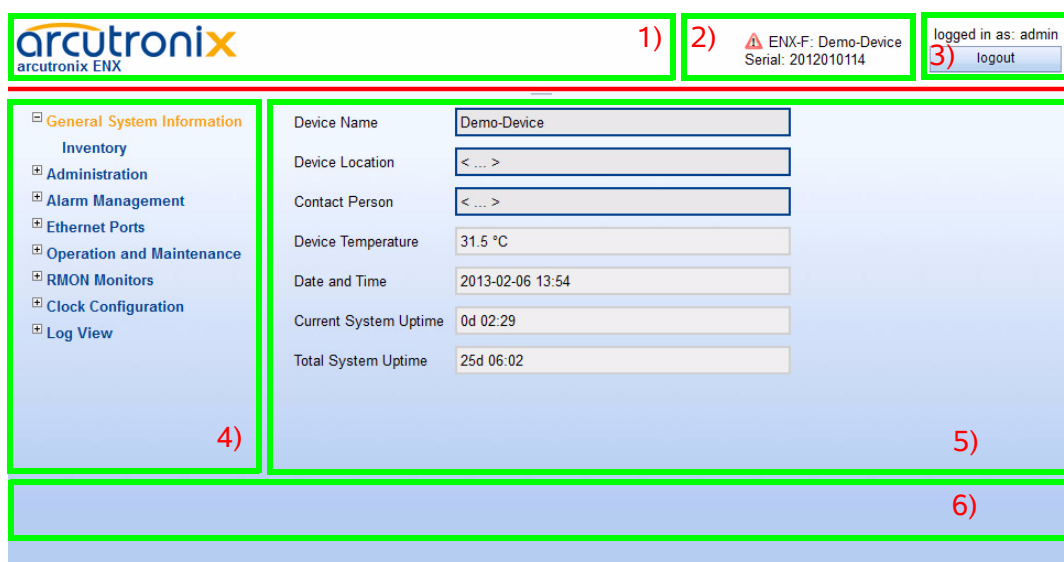


Figure 5-2 Web-GUI's Appearance



1. Logo/Family Pane.
2. Info Pane: Info about
 - device-type (here ENX-F),

- device-name (here Demo-Device),
 - serial number,
 - and alarm status (status icon).
3. Login/Logout Pane: Info, who is logged in and a button for Logout.
 4. Navigation Pane: Navigating in the Web-GUI is easy with the Navigation Pane. The settings are grouped in different categories, which can be exploded and collapsed.
 5. Main Pane: This is the pane, where all the information is listed and the configuration can be changed and adopted. The next chapter will mainly handle the settings in this section.
 6. Message Pane: Here status and error-messages are shown.

Navigation

The Web-GUI is a graphic user menu. The best way to navigate between the different pages is to use your mouse. Open and collapse the menus in the Navigation Pane (see above) and select the page, you want to see and/or edit.

Select a menu entry

When you move the mouse-pointer over the Navigation Pane, you can see the pointer change its face: When you move the pointer over a selectable item, it will look like a this:  , if there is no selectable value, it is standard (normally arrow): 

When you want to open or select the given entry, press the left button on your mouse to complete the selection.

The selected menu-entry is displayed in orange-coloured text, while all the others are marked blue (see Figure 5-2).

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

Page Update

To update the actual menu, just use your browser's reload button.

Logout

Use the Logout-Button terminating the session and leave the unit. Never forget to log-out, as otherwise unauthorized persons could get access to the unit and damage your services.

The auto-logout feature adds additional security in case the regular logout has been forgotten.

WARNING: If your PC/Laptop is very busy and does not reply on the devices cyclic

“Hello”-messages, the web-session will be terminated after 15 seconds without reply. This auto-termination is implemented due to security reasons if you close your browser or browser-tab without logout.

Web-Menus of ENX

The main view of the ENX is the top-level. From here all other (sub-)menus can be entered. It provides a general overview of the menu structure.

All menu entries and the optional usage and settings are explained in detail in an extra document: [axRefGuideWebGUI_ENX]. Please refer to this document for details.

Chapter 6

SNMP and MIBs

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

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 arcutronix Multi Service System supports two versions of SNMP: SNMPv2c (version2, community-based) and SNMPv3.

SNMPv2c

Community-Based Simple Network Management Protocol version 2, or SNMPv2c, is defined in [IETF RFC 1901]. SNMPv2c 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 the former variant SNMPv1. While officially only a “Draft Standard”, this is widely considered the de-facto SNMPv2 standard.

SNMPv3

SNMPv3 makes no changes to the protocol aside from some addition of cryptographic security. SNMPv3 primarily added security and remote configuration enhancements to SNMP. Security has been the biggest weakness of SNMP since the beginning. Authentication in SNMP Versions 1 and 2 amounts to nothing more than a password (community string) sent in clear text between a manager and agent.

Each SNMPv3 message contains security parameters which are encoded as an octet string. The meaning of these security parameters depends on the security model being used.

SNMPv3 provides important security features:

- Confidentiality - Encryption of packets preventing snooping by an unauthorized source.
- Integrity - Message integrity ensuring that a packet has not been tampered with in transit including an optional packet replay protection mechanism.
- Authentication - to verify that the message is from a valid source.

Traps

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

You can download the MIB from the ax intranet (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.

Management Information Bases (MIBS)

The MIBs (Management Information Bases) define the variables which are used to control a (SNMP-) device or to retrieve operational data from the device. The MIB consists of collections of managed objects identified by object identifiers (see below). MIBs are accessed using the simple network management protocol (SNMP). A managed object (sometimes called a MIB object or an object) is one of a number of characteristics of a managed device.

System MIB variables are accessible through SNMP as follows:

- Accessing a MIB variable—Function is initiated by the SNMP agent in response to a request from the NMS. The agent retrieves the value of the requested MIB variable and responds to the NMS with that value.
- Setting a MIB variable—Function is initiated by the SNMP agent in response to a message from the NMS. The SNMP agent changes the value of the MIB variable to the value requested by the NMS.

SNMP and MIBs

Management Information Bases (MIBS)

An object identifier (OID) uniquely identifies a MIB object on a managed network device. The OID identifies the MIB object's location in the MIB hierarchy, that can be depicted as a tree with a nameless root. The levels of which are assigned by different organizations, such as IANA. This model permits management across all layers of the OSI reference model.

The MIBs for arcutronix's SNMP management 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)

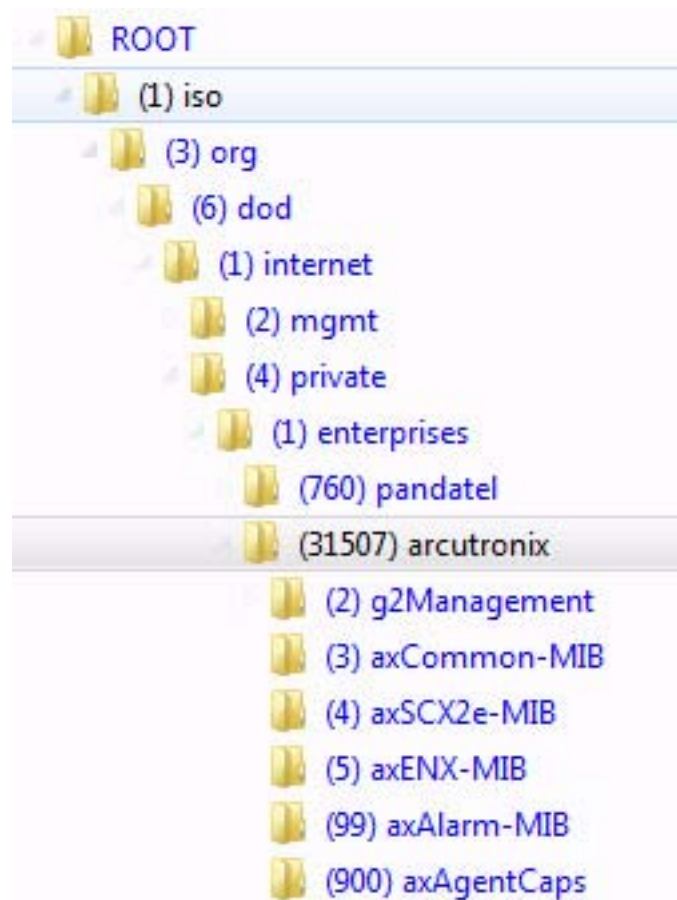


Figure 6-1 The SNMP ax-MIB Tree (1.3.6.1.2.4.1.31507)

Each number in the OID corresponds to a level of MIB hierarchy. For example, the OID 1.3.6.1.4.1.31507.3.xyz represents the .xyz with the location in the MIB hierarchy as follows. (Note that the numbers in parentheses are included to help show correspondence to the MIB hierarchy. In actual use, OIDs are represented as numerical values only.)

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).arcutronix(31507).axCommon-MIB(3).nn-MIB

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) and are plain ASCII text. Thus they can be read using any available editor.

The MIBs can be enhanced at any time, so please refer to the MIBs itself for documentation.

Chapter 7

SSH and CLI

The ENX can be configured via a text-based Command Line Interface (CLI), which can be reached over a Secure Shell (SSH) connection or the CONS-port. For the SSH-connection, only a SSH-client and an IP-connection to the device is needed.

This chapter will explain how to connect to the CLI/SSH and the usage of CLI.

NOTE: A detailed presentation of all CLI variables and menus is given in [axRefGuideCLI_ENX].

Access to the Device

The ENX CLI can be accessed either via

- CONSOLE port (115200, 8N1),
- F/Q-interface,
- In-band interface (VLAN tagged).

The access via CONSOLE port is simply serial connection (RS-232) and will not be depicted here after in detail. For details about the connector see “Console Port” on page 3-8.

The setup for the SSH connection will be explained in the following chapter.

SSH Connection

To establish the SSH connection between ENX and client a user-name/password or a key is required. Several options can be selected by the administrator.

The SSH protocol is using a TCP/IP connection. As default, TCP port 22 is used for it. If necessary, this can be changed.

Using User-Name and Password

The SSH connection is established by using one of the user-names and password, which are defined locally or by NAS. See chapter “User Administration” on page 4-36 for defining local users and usage of TACACS+.

As soon as user-name and password are verified and the access is granted, the SSH-connection is established and the login to the CLI is done. No further inquiry is needed.

Note: If this option is selected, also CONSOLE-port uses the given user-names and passwords for login.

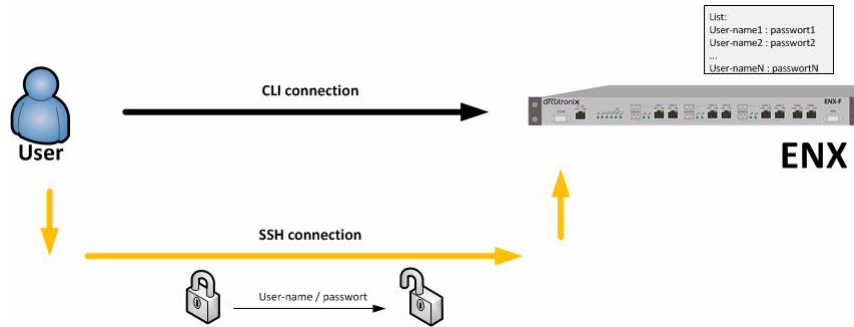


Figure 7-1 SSH-connection using User-Name and Password

Using Global SSH-Password

The SSH connection is established by using a dedicated user-names (“cli”) and a special password, which is defined locally. The user “cli” is pre-defined on the device, the “Global SSH-Password” must be configured. This option is intended to define a common (“global”) SSH-access for all devices to make SSH-connection independent from user’s login data.

The user “cli” and the global SSH-password is solely used to establish the SSH-connection. After successful SSH-setup, the user is asked for his login data (user-name and password). The user’s login data may be locally stored and/or on a NAS. See chapter “User Administration” on page 4-36 for defining local users and usage of TACACS+.

NOTE: The global SSH-password must fulfil minimum demands on security. It is required to use lower- and upper-case letters and digits. The minimum length of the password is 8 characters. If the internal check for strength of password fails, an error message will be sent.

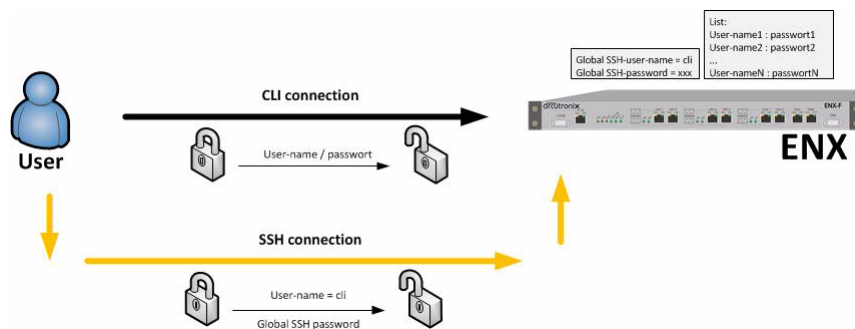


Figure 7-2 SSH-connection using Global SSH-Password

Using SSH-Key

A more secure method of authentication is through the use of RSA keys. The basic principle is as follows: RSA involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key.

Any host to which the user wants to connect must be aware of his public RSA key, as the server uses it during the authentication process. The user must place his public key living on the originating client machine, into his own `authorized_keys` file on the server.

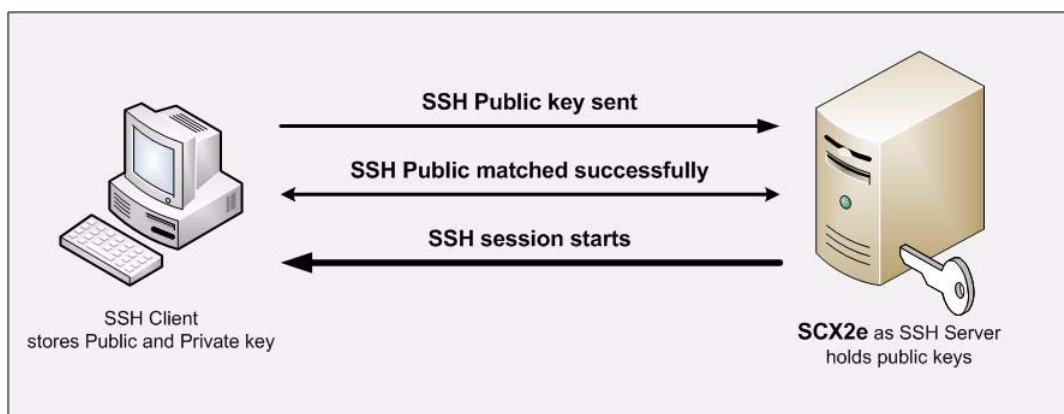


Figure 7-3 Secure Shell - Public Key

When the user wants to connect to that server, SSH will first negotiate an encrypted session, then send the server the client's public key. The server checks that the public key is in the user's `authorized_keys`. If so, the server sends the client a challenge (a random number encrypted with the user's public key). If the client can then send back the random number decrypted, it has just proven that it has the private key (there is no other way to decrypt the challenge number), and is therefore authentic.

The user's private key is a very sensitive piece of data - with it, anyone can connect to any host on which the corresponding public key is in the `authorized_keys`. Therefore, the user's private key is never written to disk decrypted.

Public key authentication solves this problem. You generate a key pair, consisting of a public key (which everybody is allowed to know) and a private key (which you keep secret and do not give to anybody). The private key is able to generate signatures. A signature created using your private key cannot be forged by anybody who does not have that key; but anybody who has your public key can verify that a particular signature is genuine.

The Authentication layer uses one or more of the following authentication methods to validate the user:

1. Password Authentication
2. RSA/DSA Public-Key Authentication

- 3. Kerberos Authentication
- 4. Host-based Client Authentication

We have focused only on the RSA Public-Key based Authentication in this process.

NOTE: The SSH-key, which is stored on the device is a public key. The ENX expects that the filename's extension is "*.pub".

The SSH connection is established by using an SSH-key which is stored locally. The SSH-key must be configured by admin as it is not pre-defined on the device.

Two option are possible, when an SSH-key is stored on the device. Either the key is used solely for the SSH-connection ("Connection Key"), or the key is also used for login ("Direct Login Key").

NOTE: If a SSH-key is stored on the device, it will always be used for SSH-connection setup.

Direct Login Key

The SSH-key is used for SSH-connection as well as for CLI login. As soon as the key is verified and the access is granted, the SSH-connection is established and the login to the CLI is done. No further inquiry is needed.

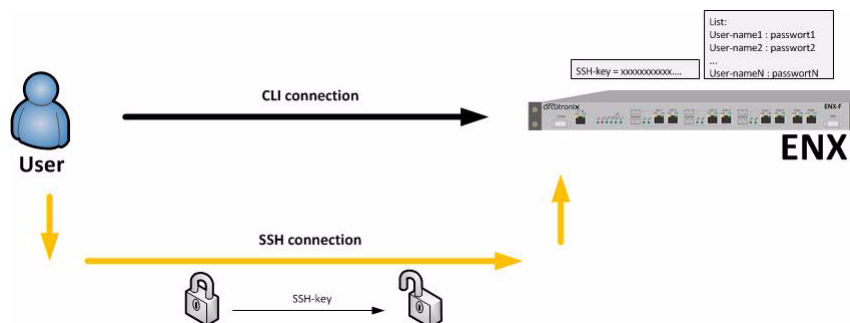


Figure 7-4 SSH-connection using SSH-Key (Direct Login)

Connection Key

The SSH-key is solely used to establish the SSH-connection. After successful SSH-setup, the user is asked for his login data (user-name and password). The user's login data may be locally stored and/or on a NAS. See chapter "User Administration" on page 4-36 for defining local users and usage of TACACS+.

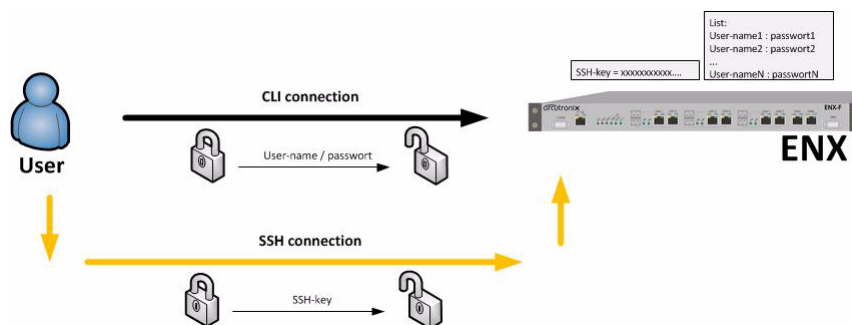


Figure 7-5 SSH-connection using SSH-Key (Connection Key)

Security Issues

The SSH/CLI is accessible via any TCP/IP link to the device, so it might be that other persons than the intended ones get connection and will see the login prompt. To avoid forbidden configuration or burglary of information, the access is protected against intruders via user-name and password.

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

Be careful with 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 4-34, how to define other users and how to change the user's password.

SSH Client

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.

To connect to the ENX SSH-server establish a link via TCP/IP:

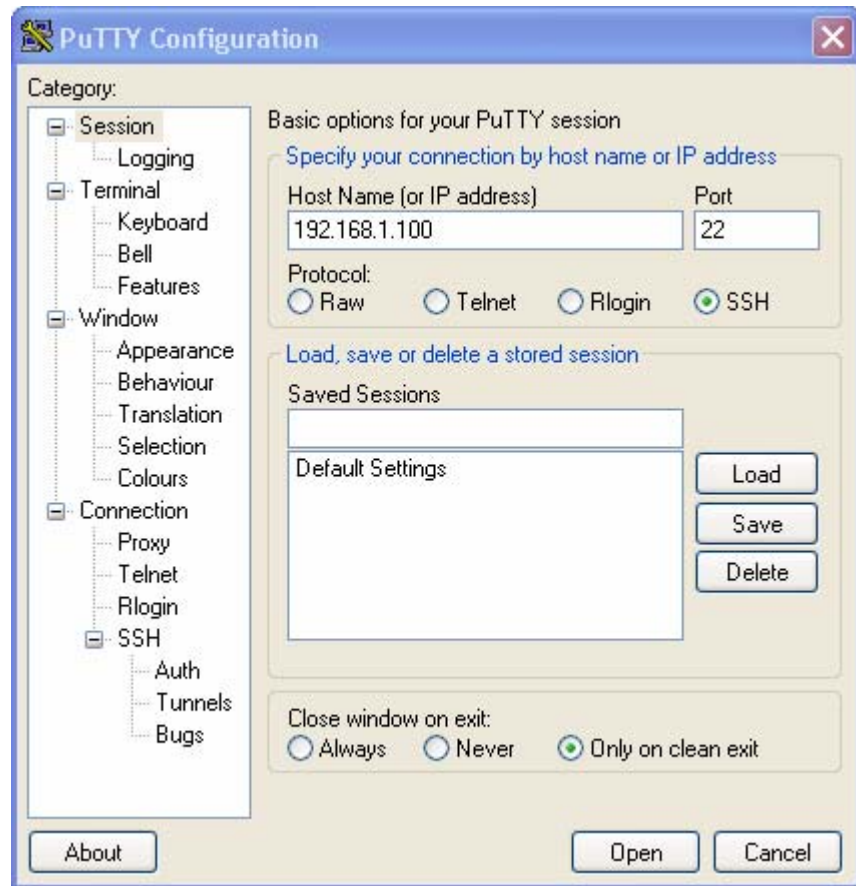


Figure 7-6 PuTTY SSH-Connection

NOTE: Please make the shell-window at least 200 wide, otherwise some help-messages could be corrupted when shown.

After pressing “Open”, the Secure Shell will be opened and a prompt is visible.



Figure 7-7 Secure Shell

Now enter the user-name, which shall be used for the communication (e.g. admin) and enter the password (e.g. private).

The next message is "Welcome <username>!" and the connection is established.

Command Line Interface (CLI)

Introduction to the CLI

Many devices that come with support for CLI provide a huge number of different commands configuring the various functions of the device. All of these commands come with their own syntax and parameters. The CLI of arcutronix devices follows a different and more intuitive approach.

In contrast to the devices mentioned before, the CLI of arcutronix devices provides direct access to configurable parameters and device properties, so-called variables, which can be read-only (e.g. for fixed device properties) or modifiable (for configurable parameters).

Since there is a vast number of those variables, they are organized in a hierarchical menu structure. The menu structure and the ordering of information therein is logically aligned with the device functions. Once familiar with the layout of the menu structure, which is easily comprehensible, the user quickly and intuitively navigates through the menu structure and easily manipulates the device settings as needed. The CLI supports this further by giving context-sensitive help as well as automatic command and parameter completion where ever possible.

As a result, only a single command is needed configuring all aspects of the device and its functions: the “config” command explained later. It provides everything that is needed to navigate through the menu structure, to look at the information provided in submenus and to manipulate the value of configurable parameters. Each item in the menu structure (submenu, variables and possible variable values) may have helpful descriptions associated with them that can be viewed with the “config” command as well.

The navigation through the menu structure is designed to follow a principle that every computer user knows: it closely resembles the navigation through a file system. Here, menus and submenus represent directories on the hard drive, whereas configurable parameters are similar to files on the disk. The “config” command supports full path names in every place where the name of an item in the menu structure is expected. Those path names can either be relative to the current position in the menu tree, or be a path starting from the root of the menu structure. Path names are formed like file names by concatenating menu, submenu and variable names with a directory separator, for which the UNIX-style forward slash “/” was chosen. The usual name “..” for the parent menu is supported as well.

This file system similarity is also applied to more complex elements of the menu structure. For tables, which do naturally occur if there is more than one instance of an equivalent hardware component or software function present, each table row is translated into a submenu where the table columns are presented as scalar variables. Within the submenu representing the table row, editable columns can be modified as usual and further submenus of the table row become available.

Usually, the manipulation of a variable will have an immediate effect. Once the new variable value is successfully submitted, the device will make immediate use of the changed value and adjust its operation to it. Occasionally, there are cases where a group of variables needs to be consistently changed as a whole. These variable groups are also translated into submenus called “Form Pages”. Whenever the user navigates to such a form page, the CLI starts a new transaction that is automatically aborted when the user navigates away. Changes to variables within the form page will not immediately be activated but become part of the transaction data. Each form group has a **BUTTON** variable that fulfills the task of submitting the data and activating the changes.

CLI Editor Features

Context Sensitive Help

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

NOTE: The CLI is case-sensitive in matters of the commands!

Path & Command Completion

Commands and path-entry can be completed with <TAB> to make entry quicker. When the so far entered entry is definite, the entry will be completed by pressing <TAB>. If the entry is ambiguous, the possible completion is displayed after pressing <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.

NOTE: While the CLI is case-sensitive in matters of command entry, the path and variable entry is independent of the case.

Reduced Entry of Path & Command

Commands and path-entry can be abbreviated as long as the entry is definite. This is helpful when typing CLI scripts, where the auto-completion feature (with <TAB>, see above) is not available.

For example, the path “/General System Information/Inventory” can be reduced to “/G/I”.

NOTE: The CLI is case-sensitive in matters of the commands!

Prompt and Path

The prompt of the CLI is built by 4 sections, which are added in the following sequence:

1. Device Type = ENX-F,
2. Device Name = “ENX-F” by default. The device name can be changed,
3. Path = the actual location within the menu-tree,
4. Explicit end = \$>

Examples: After login, you reach the root-directory and the prompt is:


ENX-F "ENX-test" / \$>
1. 2. 3. 4.

After navigating to the submenu “General System Information”, the prompt will be:

```
ENX-F ENX-test "/General System Information $>
```

To avoid problems with some CLI and SSH-clients, the path-statement is limited to 30 characters. If the path-statement is longer than 30 characters, the leading characters are all replaced by one dot. So after navigating to the submenu “Inventory”, the prompt will look like this:

```
ENX-F ENX-test ".l System Information/Inventory $>
```



The complete path can always be checked by the “config path” command, which prompts the actual submenu and the path from the root directory.

Comment

The CLI offers the possibility to write scripts to automate configuration and reproduce settings easily. In scripts it is worth to add comments for better understanding. A CLI comment can be written by adding a hash-symbol (#) in front of the comment. The comment may start at the beginning of a line or at any position. All text following the # will be treated as comment.

Hot Keys

For many editing functions, the ENX CLI editor provides hot keys. Table 7-6 lists some editing short-cuts that are available.

Table 7-1 ENX 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.

Table 7-1 ENX CLI Hot Keys (continued)

Hot Key	Description
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 unexperienced users to complete commands, gives correct syntax and shows possible entries at all stages!

CLI Commands

Once an SSH-session is established, one can navigate within ENX CLI like in a hierarchically structured tree. Command options and applications vary depending on position within this hierarchy.

To assist users in navigation through ENX 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 identifying “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.

```
$> config go "General System Information"          or
$> config go General\ System\ Information
```

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

Table 7-2 and Table 7-3 show a summary of commands and the corresponding syntax.

Table 7-2 CLI Command CONFIG

Command CONFIG	Syntax / Explanation
Summary:	
config shows or changes configuration settings. Configurations are grouped and this command can also be used to display/change configuration menu. Without an argument config shows the current configuration menu and its settings/submenus. For more details see “The command CONFIG” on page 7-15.	
8 optional syntax flavours are defined:	
config	config

Table 7-2 CLI Command CONFIG (continued)

Command CONFIG	Syntax / Explanation
	<p>Shows all the content of the current configuration submenu. The first character in each row indicates the type of variable that is shown:</p> <ul style="list-style-type: none"> • > for submenus, • F for form pages, • * for read-writeable variables, • ! for read-writeable password variables, • + for executable commands, • (blank) for read-only variables. <p>Options: none</p>
config path	<p>config path</p> <p>Shows the complete path of the current configuration page. As the CLI's prompt does only show a reduced path (30 characters), it might be helpful to see the complete path for verification.</p> <p>Options: none</p>
config go	<p>config go <PATH></p> <p>Changes to a different configuration page.</p> <p>Options:</p> <ul style="list-style-type: none"> • <PATH> = root: topmost menu • <PATH> = up: go to parent menu • otherwise: go to submenu identified by PATH. The PATH may start at the present submenu or at root (/). Suitable submenus are identified by: <ul style="list-style-type: none"> • > (regular submenu) • F (form page)
config VARIABLE	<p>config [PATH]VARIABLE</p> <p>Display the current value of VARIABLE.</p> <p>Options:</p> <ul style="list-style-type: none"> • <PATH>: path to VARIABLE in submenu identified by PATH. The PATH may start at the present submenu or at root (/). If empty, VARIABLE must exist in the current submenu. Suitable submenus are identified by: <ul style="list-style-type: none"> • * (read-write) • ! (read-write password) • (blank: read-only) • VARIABLE: management variable to be displayed.
config help	<p>config help [PATH]VARIABLE</p>

Table 7-2 CLI Command CONFIG (continued)

Command CONFIG	Syntax / Explanation
	<p>Display help-information for VARIABLE.</p> <p>Options:</p> <ul style="list-style-type: none">• PATH: path to VARIABLE in submenu identified by PATH. The PATH may start at the present submenu or at root (/).• VARIABLE: management variable. Allowed are all items that the config command displays.
config set	<p>config set [PATH]VARIABLE VALUE</p> <p>Change the value of VARIABLE to new VALUE.</p> <p>Options:</p> <ul style="list-style-type: none">• PATH: path to VARIABLE in submenu identified by PATH. The PATH may start at the present submenu or at root (/).• VARIABLE: management variable to be modified. Allowed are variables identified by:<ul style="list-style-type: none">• * (read-write)• ! (read-write password)• VALUE: New value of the variable. Value must be according the defined value range of VARIABLE.
config hidden	<p>config hidden [PATH]VARIABLE</p> <p>Change the value of the protected (password) VARIABLE in a hidden mode. The password will be prompted for in a new line. The typed value will be invisible for security reasons. To protect from accidentally mistyping errors, the new value has to be re-entered for confirmation.</p> <p>Options:</p> <ul style="list-style-type: none">• PATH: path to VARIABLE in submenu identified by PATH. The PATH may start at the present submenu or at root (/).• VARIABLE: A special protected (password) VARIABLE. Allowed are variables identified by:<ul style="list-style-type: none">• ! (read-write password)
config do	<p>config do [PATH]COMMAND</p> <p>Start or execute COMMAND.</p> <p>Options:</p> <ul style="list-style-type: none">• PATH: path to VARIABLE in submenu identified by PATH. The PATH may start at the present submenu or at root (/).• COMMAND: A command starts a complex action. Allowed are variables identified by:<ul style="list-style-type: none">• + (executable command)

Table 7-3 All other CLI Commands

Command	Syntax / Explanation
help	<p>help [COMMAND Short-cut]</p> <p>help without any further entry shows all the commands and short-cuts, which are available. When help followed by a command or short-cut, the detailed help-text for it will be presented.</p> <p>For help an alias is available: ?</p> <p>help is in any context available.</p> <ul style="list-style-type: none"> • ARG COMMAND - any available command.
log	<p>log [LINES]</p> <p>Show last entries of the log file. The optional parameter allows to specify the number of lines to show.</p> <ul style="list-style-type: none"> • ARG LINES - The number of lines to print at most (default: 100).
quit	<p>quit</p> <p>Quit the current CLI session.</p>
show	<p>show [<PATH>]</p> <p>Displays the settings in the selected (or current) menu in a format suitable for copying the lines back into the CLI. Changeable settings are printed as CLI commands, read-only settings are printed as comments. Each line is terminated by a semi-colon.</p> <p>ARG PATH - Path to a menu. If omitted, current menu-path is used.</p>
showall	<p>showall [<PATH>]</p> <p>Displays the settings in the selected (or current) menu including all submenus in a format suitable for copying the lines back into the CLI. Changeable settings are printed as CLI commands, read-only settings are printed as comments. Each line is terminated by a semi-colon.</p> <p>ARG PATH - Path to a menu. If omitted, current menu-path is used.</p>
save_devlog	<p>save_devlog</p> <p>Save the developer log-files onto the "Logfile server".</p>
print_devlog	<p>print_devlog</p> <p>Print the developer log-files.</p>

The command CONFIG

The command CONFIG is the most mighty tool in the ENX CLI and will be depicted here after more in detail and some examples are given.

For complete overview to all variables see additional document [axRefGuideCLI_ENX].

When entering the command CONFIG apart in any context, the available menu-entries are shown:

```
ENX-F "arcutronix" / $> config
--Login
> General System Information
> Administration
> Alarm Management
> Ethernet Ports
> Operation and Maintenance
> RMON Monitors
> Clock Configuration
> Log View
```

The first 1-2 characters in the resulting overview are type-indicators which shows what can be done with this entry and which `config`-command can be used.

Table 7-4 Menu Indicators and corresponding CONFIG Commands

Type	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>Submenu:</p> <p>">" indicates a submenu, which can be accessed via CONFIG GO <submenu-name></p> <p>Example:</p> <pre>\$> config --Login > General System Information > Administration > Alarm Management > Firmware Update \$> config go Administration /Administration \$></pre>

Table 7-4 Menu Indicators and corresponding CONFIG Commands (continued)

*	<p>Changeable Management Variable</p> <p>“*” indicates a menu-entry which can be changed via</p> <p>CONFIG SET <variable-name> <value></p> <p>Example:</p> <pre>/General System Information \$> config --General System Information * Device Name: "ENX-F" . . . /General System Information \$> config set Device\ Name "New Name" /General System Information \$> config --General System Information * Device Name: "New Name" . . . /General System Information \$></pre>
!	<p>Password or other sensitive data. This variable should be configured with care. When entering a new value for the variable and the configuration can be done in “hidden” mode.</p> <p>!“ indicates a menu-entry which can be changed in hidden mode (with double entry for verification) or standard mode (with single entry and the entry is readable).</p> <p>CONFIG HIDDEN <variable-name> or</p> <p>CONFIG SET <variable-name> <value></p> <p>Examples:</p> <p>By hidden command (config hidden):</p> <pre>..Modify Account/Change Password \$> config -- Modify Account ! Password: <hidden> + [Change Password] Form data will only be submitted after executing 'config do Change Password' ..Modify Account/Change Password \$> config hidden Password Enter password: Retype password: ..Modify Account/Change Password \$> config do Change\ Password Really change the Password (y/n)? Proceed? [yes no] \$> y Data submitted. ..Modify Account/Change Password \$></pre>

Table 7-4 Menu Indicators and corresponding CONFIG Commands (continued)

or by standard config set command:

```
..Modify Account/Change Password $> config
-- Modify Account
! Password: <hidden>
+ [Change Password]
  Form data will only be submitted after executing 'config do
Change Password'
..Modify Account/Change Password $> config set Password NelwPw_
..Modify Account/Change Password $> config do Change\ Password
Really change the Password (y/n)?
Proceed? [yes|no] $> y
Data submitted.
..Modify Account/Change Password $>
```

+ 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
```

blanc Read-Only Variable

No sign (or blanc character “”) indicates a read-only variable which can be read via

CONFIG <variable-name>

Example:

```
/General System Information $> config
--General System Information
.
.
.
Device Temperature: "35.5"
.
/General System Information $> config Device\ Temperature
"35.5"
/General System Information $>
```

There are some special CONFIG commands, which help to navigate:

Table 7-5 Special CONFIG Commands

Typ e	Explanations / Examples
	<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>

Short-cuts

Some of the settings via CLI seem to occur more often than others. To avoid protracted entries of CLI commands, the ENX supports some short-cuts.

Table 7-6 CLI Short-cuts

<pre>\$>F [ip IP] [netmask NETMASK] [nodhcp]</pre>	
Description	<p>Makes the dedicated management port (out-of-band interface "F/Q") an F interface (local management).</p> <p>Optionally allows specifying a network configuration.</p>
• ARG ip IP	<p>Enter the designated IP address of the device. If none is given, the default address (192.168.1.100) will be set.</p>
• ARG netmask NETMASK	<p>Enter the designated net-mask for the management interface. If none is given, the default net-mask (255.255.255.0) will be used.</p>
• ARG nodhcp	<p>If present, do not start a DHCP server on the management interface. Otherwise a DHCP server will be started.</p>
<pre>\$>Q [ip IP] [netmask NETMASK] [gateway GATEWAY] [dhcp] [vlan VLAN-ID]</pre>	

Table 7-6 CLI Short-cuts (continued)

Description	
	Makes the dedicated management port (out-of-band interface “F/Q”) an Q interface (remote management). Two possible syntax are allowed, with or without DHCP-client option. If the DHCP-client shall be enabled, only the VLAN-option can be set. If no DHCP-client is started, the IP configuration and the VLAN can be entered:
	<pre>\$>Q [ip IP] [netmask NETMASK] [gateway GATEWAY] [vlan VLAN-ID]</pre>
	<pre>\$>Q dhcp [vlan VLAN-ID]</pre>
• ARG ip IP	Enter the designated IP address of the device. If none is given, the default address (192.168.1.100) will be set.
• ARG netmask NETMASK	Enter the designated net-mask for the management interface. If none is given, the default net-mask (255.255.255.0) will be used.
• ARG gateway GATEWAY	Enter designated IP address of the gateway. If none is given, gateway settings will not be changed.
• ARG dhcp	If given, use DHCP-client for IP address assignment and ignore IP/NETMASK/GATEWAY. Otherwise do not use DHCP. If given, the options IP, NETMASK and GATEWAY are obsolete.
• ARG vlan VLAN-ID	If present, force the management interface to use given VLAN ID. Otherwise accept untagged management traffic. VLAN may be used with or without DHCP option.

More may come, when operation makes it meaningful.

Quick Usage Guide for CLI-Commands

Table 7-7 CLI Quick Reference

Show options in actual menu:
<pre>\$> config</pre>
Change Contact Person: [General System Information -> Contact Person]

Table 7-7 CLI Quick Reference (continued)

```
$> config go General\ System\ Information  
$> config set Contact\ Person "new Name"
```

Reboot Device: [Administration -> Reset System]

```
$> config go Administration  
$> config go Reset\ System  
$> config set Reset\ Mode Immediate\ Reset  
$> config do Start\ Reset
```

Go back 1 Step in Menu:

```
$> config go up
```

Go back to Top-Level Menu (/):

```
$> config go root
```

Show the complete path (remember, the path within the prompt is limited to 30 characters):

```
$> config path
```

Example for SSH-Script

TeraTerm and other SSH-clients are supporting scripting to execute commands in always the same way. In the following, a short example for an TeraTerm-script is given to show the initial setup to a host and how to enter some simple commands.

The script will do the following:

1. Connect to the device (192.168.1.100) with user-name "admin" and password "private" using SSH2
2. Change the contact person's name to "Miss Marple",
3. Change the units name to "test-unit with new name",
4. Disconnects the session.

Table 7-8 Example for SSH-Script

Step	Code
0	<pre>;; Tera Term Macro ;; ===== ;; file __prog_ENX.ttl ;; ;; desc Example for Teraterm programming-file. ;; ===== ;; HISTORY ;; ;; 2011-02-21 arcutronix GmbH Initial Version ;; ;; =====</pre>
1	<pre>;; open Tera Term ;; connect '192.168.1.100 /SSH /2 /auth=password /user=admin /passwd=private</pre>
2	<pre>wait '/ \$> ' sendln 'config go "General System Information"' wait ' \$>' sendln 'config set "Contact Person" "Miss Marple"'</pre>
3	<pre>wait ' \$>' sendln 'config go "General System Information"' wait ' \$>' sendln 'config set "Device Name" "test-unit with new name"'</pre>
4	<pre>pause 1 disconnect 0 end</pre>

Appendix A

Technical Specifications

ENX Hardware Specification

Hardware & Power

Table A-1 to Table A-9 provide the general technical data of the ENX - Synchronous Ethernet Network Termination.

Table A-1 Physics and Environment

ENX-Family	ENX-F	ENX-S	ENX-V
Physical Dimensions			
Parameter			
Height	43,6 mm		
Width	448 mm		
Width with 19"-angle	482,6 mm		
Depth	305,8 mm		
Weight	2.9 kg		
Environmental Conditions			
Operation:			
Temperature (hardened version)	-40 ... +70 °C		
Humidity	10 ... 100%, non-cond.		
Storage (in packing) ⁱ :			
Temperature	-35 ... +55 °C		
Humidity	10 ... 100%, non-cond.		
Transportation ⁱⁱ :			
Temperature	-40 ... +70 °C		
Humidity	10 ... 95%, non-cond.		
Others			
Ingress Protection:	IP30		
DIN EN 60529 (VDE 0470 Part 1)			
Fan:	none		
Cooling:	Convection cooling through ventilation slots in the housing environment		

Technical Specifications

ENX Hardware Specification

- i. ETSI ETS 300 019-1-1, class 1.2
- ii. ETSI ETS 300 019-1-2, class 2.3

Table A-2 Security and EMC

ENX-Family	ENX-F	ENX-S	ENX-V
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-3 Power Supply

ENX-Family	ENX-F	ENX-S	ENX-V
Power Supply			
AC power supply ⁱ			
Supply voltage	110/240 V AC \pm 10 %		
Frequency	50 Hz		
Supply current	< 500 mA		
DC power supply ⁱⁱ			
Supply voltage -48VDC	-40...-57 V DC		
Supply voltage -60VDC	-50...-72 V DC		
Supply current	< 1.4 A		
Power Consumption ⁱⁱⁱ			
w/o SFP	15.0 VA		
with Standard SFP(s) (700mW)	19.2 VA (6x SFP)		
Max. power to be used per SFP(s)	1.8 VA		
Fuses			

Table A-3 Power Supply (continued)

ENX-Family	ENX-F	ENX-S	ENX-V
Fuse, type			
AC	T1.0A; 250V; 5x20		
DC	2.5A; 125V; onboard		
<ul style="list-style-type: none"> i. ETSI EN 300 132-1 ii. ETSI EN 300 132-2 iii. The total power need depends on the used SFP(s). 			

Table A-4 Power Saving

ENX-Family	ENX-F	ENX-S	ENX-V
Thermal Protection			
Device shutdown to almost 0W remaining power consumption	@75°C		
Unused PHYs			
Shutdown of unused (disabled) or inactive combo-ports	yes		

Interfaces

Table A-5 Number of Interfaces

Type		
Number of Interfaces		
ENX-F	6x Gigabit Ethernet 10/100/1000BaseT (RJ45) or	General Purpose (Combo-port)
	6x Gigabit Ethernet 1000BaseX (SFP),	General Purpose (Combo-port)
	1x 10/100BaseT	Out-of-band Management I/F
	1x RS-232 (D-SUB9, female)	Console port
	1x Clock-Input (2,048MHz or 2,048Mbps HDB3), RJ45	T3an reference
	1x Clock-Input (2,048MHz or 2,048Mbps HDB3), RJ45	T4ab reference
	1x PPS-Output (1Hz), D-SUB9	Peak-per-second
	1x Alarm Connector	NOC (normal open connector)
ENX-S	ndy	
ENX-V	ndy	

Table A-6 Technical Data of the Interfaces

Interfaces	
Fast Ethernet Interfaces (Copper)	
Type:	IEEE 802.3 (full- and half-duplex, Autonegotiation)
Data-rate	10 or 100Mbps

Table A-6 Technical Data of the Interfaces (continued)

Interfaces	
Fast Ethernet Interfaces (Copper)	
Connection type:	Twisted-Pair interface (TP)
Function, electrical values, pin-assignment:	according to IEEE 802.3i (10BaseT), IEEE 802.3u (100BaseTX)
Impedance:	100 Ohm (balanced)
Connector:	8 pin RJ45 connector according to ISO 8877
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 802.3i (10BaseT), IEEE 802.3u (100BaseT), IEEE 802.3ab (1000BaseT)
Impedance:	100 Ohm (balanced)
Connector:	8 pin RJ45 connector according to ISO 8877
Gigabit Ethernet Interface (SFP)	
Type:	IEEE 802.3 (full-duplex)
Connection type:	Fibre Optics (FO), SFP
Function, electrical values:	IEEE 802.3z (1000Base-X)
Connector:	LC or RJ45
SFP:	According to "[SFP MSA]", Rev 4.5, Aug. 31, 2006 All vendors supported. Max. 100 insertion / extraction.
Console Port	
Type:	EIA-232-F (RS-232)
Connector:	D-SUB9, female
Connection type:	DCE
Speed, Settings:	115,200kBaud, 8 Bits, 1 Stop-bits, no bit parity, no flow control: (115k, 8N1)
Other Connectors	
AC plug	IEC 60320-1; C14

Table A-6 Technical Data of the Interfaces (continued)

Interfaces	
Fast Ethernet Interfaces (Copper)	
DC plug	RIA (3 pin)
Alarm Connector:	RIA (3 pin)

Dataplane and Switching

Table A-7 Technical Data Dataplane

Type	
Switching Capabilities	
Latency	Low latency handling of VoIP/Video services
Number of MAC addresses	8k MAC addresses supported
Jumbo-Frames supported:	MTU (Maximum Transmission Unit): 10k Bytes
Packet Buffer Memory	1 Mbit
MAC Addresses	8k
Quality of Service	
Queues	4 priority queues per port for traffic management
Classification	Traffic classification/priority based on TOS/DSCP/802.1P/802.1Q
Queuing	Programmable Weighted Fair Queuing
Ingress Rate Limiter	4 limiters per port (LAN and LINE-ports!)
Egress Shaper	Egress bandwidth shaping per port (LAN and LINE-ports!)
Virtual LAN	
Virtual LAN	802.1Q VLAN: forwarding, stacking (802.1Q-in-Q)
Number of VLAN	4096 port based VLANs with tagging acc. IEEE802.1Q

µController, Display & Clock

Table A-8 Display Functions

Type	
Display Functions	
System:	6 LEDs for system, operating and error status
Fast Ethernet interface (MGMT):	2 LEDs for Link Status, Activity and 10/100Mbps recognition (only TP ports)
Copper Gigabit Ethernet interfaces:	2 LEDs each, for Link Status, Activity and 10/100/1000Mbps recognition (only TP ports)
Fibre Gigabit Ethernet interfaces:	1 LED each, for Link Status and Activity

Table A-9 µController and Clock

Type	
Electronics	
Main processor:	32 Bit power PC, Freescale MPC8313E
Non-volatile memory:	64 MB
Main memory:	128 MB SDRAM
Real Time Clock	
Accuracy	10ppm (<1sec/day)
Hold Time (without ext. power)	min. 11 days
Onboard Clock (TCXO)	
Accuracy	0.5ppm
Frequency stability over temperature range	2.5ppm
Aging (1st year)	1.0ppm

ENX Software Specification

Table A-10 Technical Data of the ENX - Software

ENX-F		
General Information		
Valid SW-Version for this manual: V 1_1_00 ⁱ		
Standards		
Internet Protocol:	IPv4	
IP-address assignment:	manually	
	DHCP	RFC 2131
SNMP:	SNMPv2c	RFC 1901, RFC 1905, RFC 1906
	SNMPv3	IETF RFC 3410 - RFC 3418
	SNMPv2-MIB	RFC 3418
	RMON MIB (rmon1, rmon2, rmon3, rmon4 and rmon9)	
	IF-MIB	RFC 2863
Secure Shell (SSH)	SSHv1	draft-ylonen-ssh-protocol-00.txt
	SSHv2	RFC 4250 - RFC 5256
TFTP		RFC 1350
SFTP		draft-ietf-secsh-filexfer-02.txt
http	http /1.1	RFC 2616

i. If you use higher SW-version, please check with arcutronix or your local partner, whether there is a new release of the manual available.

Table A-11 Management & Security

ENX-Family	ENX-F	ENX-S	ENX-V
HTTP server	yes		
CLI console port	yes		
CLI (via SSH)	yes		
Web and CLI authentication and authorization	yes		
Software download through Web	yes		
Software download through FTP	yes		
Configuration download or upload	yes		
SNMPv2c/v3Agent	yes		
TACACS+	yes		

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: ENX – Synchronous Ethernet Network Termination
Members: ENX-F
Number: 1102-1001

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, 21.10.2011

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