

arcutronix

Synchronize the Ethernet

USER GUIDE

RPX
GS1



arcutronix GmbH
Deutschland

**Installation and
Operation Manual**

Version 1.1

RPX16 - Remote Power Unit

USER GUIDE



Covered Variants of RPX by this User Guide:

RPX16: 1303 - 1000

Covered Software Versions of RPX by this User Guide:

SW-Version: V 1_2_02

Boot-Loader: V 1_4

Part-Number (User-Guide): 1303 00 65.man

Version: V 1.1

Date of Issue: 2014-05-07

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 2013, 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 RPX16 - Remote Power Unit. 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 RPX16 - Remote Power Unit. 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 RPX devices and applications for use.

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

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

Chapter 4, **Functionality:** Remote Feeding, Supervision of Power and Current.

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

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

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

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

Appendix EC, **EC Declaration of Conformity:** Valid for the RPX 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

- 2014-05-07 Version 1.1 Editor: mjz
Added and changed the following topics:
- 3rd Ethernet port was added due to customer's demand. This is new HW and SW.
- 2014-02-14 Version 1.0 Editor: mjz
Added and changed the following topics:
- Released for customer DTAG.
- 2013-11-21 First issue of the RPX User Guide.

Referenced and Related Documents

- [axRefGuideWebGUI_RPX] arcutronix GmbH (2013): RPX Web-GUI, Reference Guide.
- [axRefGuideCLI_RPX] arcutronix GmbH (2012): RPX Command Line Interface, Reference Guide.
- [ETSI TS 101 524] Technical Specification ETSI TS 101 524 (2003), Access transmission system on metallic access cables; Symmetric single pair high bitrate Digital Subscriber Line (SDSL).
- [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.
- [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 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.
- [ITU-T G.991.2] Recommendation ITU-T G.991.2 (2003), Single-pair high-speed digital subscriber line (SHDSL) transceivers.
- [ITU-T G.991.2__Amd3] Recommendation ITU-T G.991.2 (2003)– Amendment 3.
- [ITU-T G.994.1] Recommendation ITU-T G.994.1 (2003), Handshake procedures for digital subscriberline (DSL) transceivers.

-
- [ITU-T M.3010] Recommendation ITU-T M.3010 (2000), TMN and Network Maintenance: International transmission systems, telephone circuits, telegraphy, facsimile and leased circuits.
- [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.

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
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

RPX16 Description	1-1
General	1-1
Application Areas for the RPX	1-1
Feeding SDSL Repeater	1-1
Feeding CPE	1-2
Separate Cable	1-3
RPX16 Functions at a Glance	1-4
Power Feeding & Supervision	1-4
Management	1-4
Housing and Power Supply	1-4
Alarm Conditions and Relay	1-4
Order Information	1-5

Chapter 2 Getting Started

Delivered Parts	2-1
Preparing the Start-up	2-1
Operating Conditions	2-1
Ambient Conditions	2-1
Mounting Options	2-2
Rack-Mount 19"-Rack	2-2
Airflow Requirements	2-3
Start-up of the RPX16	2-3
Switching on the Device	2-3
Power-Up Sequence	2-3
LED Start-Up	2-4
Configuration Access	2-5
Local and Remote IP-Access	2-5
Serial Access	2-6
Configuration Methods	2-7
Web Access	2-7
Secured Web Access	2-7
SSH Access	2-7
SNMP Access	2-7
Command Line Interface	2-8

Chapter 3 Hardware & Interfaces

Hardware Overview	3-1
Block-Diagram	3-1
Connectors and LEDs	3-3
Power Connector	3-3
DC Power Supply	3-3
Management Interfaces	3-4
Ethernet Features	3-4
10/100BaseT (RJ45)	3-5
Auto-Cross-Over	3-5
VLAN Features	3-6
IP Features	3-6
SDSL Ports	3-6
LEDs	3-10
ON & ALM	3-10
Ethernet	3-10
Remote Feeding Status	3-11
Console Port	3-12
Pinning	3-12
RS232 Connection Cable	3-12
Labels	3-13

Chapter 4 Functionality

- Remote Feeding 4-1
 - General 4-1
 - Operation-States 4-2
- User & Access Administration 4-4
 - Access-Options to the RPX 4-4
 - SSH-Access 4-5
 - User Administration 4-6
 - Locally Stored Users 4-6
 - Rules for Usernames 4-6
 - Rules for Passwords 4-7
 - TACACS+ 4-7
 - TACACS Example Configuration 4-8
- Auto-Logout 4-9
 - Time-Based Auto-Logout 4-9
 - Protocol-Based Auto-Logout 4-9
 - Hardware-Based Auto-Logout 4-9
- Management Port Configuration 4-10
 - Port Settings 4-10
 - IP-Addressing 4-10
 - Management Port "local" 4-10
 - Management Ports "north" and "south" 4-11
 - DHCP and Manual Address Assignment 4-11
 - F- and Q-Interface 4-11
 - DNS-Support 4-12
- Firmware-Update 4-12
- File-Transfer to/from Servers and via HTTP(S) 4-13
 - SFTP and TFTP 4-14
 - HTTP and HTTPS 4-15
- Miscellaneous Features 4-15
 - Auto Negotiation 4-15
 - Speed and Duplex 4-15
 - Alarm Management 4-17
 - Alarm Types 4-17
 - Alarm States 4-18
 - Not Available 4-18
 - Inactive 4-18
 - Ignored 4-19
 - Acknowledged 4-19
 - Warning 4-19
 - Error 4-19
 - Alarm Acknowledgement Behaviour 4-19
 - Keep Acknowledged Until Inactive 4-20
 - Unacknowledge When Raising Severity 4-20

Unacknowledge on State Change	4-20
Example	4-20
Alarm Properties	4-22
Common Alarm Properties	4-22
Digital Alarm Properties	4-22
Analogue Alarm Properties	4-22
Alarm Groups	4-23
Global Alarm Status	4-23
Active Alarm List	4-23
Date & Time Settings	4-24
NTP and Encryption	4-24
Configuration Management	4-24
Diagnostics	4-25
Logging	4-26
<INFO>	4-26
<AUDIT>	4-26
<ALARM>	4-27
<ERROR>	4-27

Chapter 5 RPX 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 RPX	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
Quick Usage Guide for CLI-Commands	7-18
Example for SSH-Script	7-19

Appendix A Technical Specifications

RPX Hardware Specification	A-1
Hardware & Power	A-1
Interfaces	A-4
Remote Power Feeding	A-5
µController, Display & Clock	A-6
RPX Software Specification	A-7

Appendix EC EC Declaration of Conformity

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

List of Figures

Figure 1-1	RPX Application SDSL Repeater	1-2
Figure 1-2	RPX Application CPE-Feeding	1-2
Figure 1-3	RPX Application CPE Multiple-Feeding	1-3
Figure 1-4	RPX Application Extra-Feeding Net	1-3
Figure 2-1	Rack Mount-Angles 19-Inch	2-2
Figure 2-2	Rack Mount-Angles ETSI	2-2
Figure 2-3	RPX Ventilation Louvres	2-3
Figure 2-4	Management Access	2-6
Figure 3-1	RPX16 Block-Diagram	3-2
Figure 3-2	RPX Front-View	3-3
Figure 3-3	RPX Management Access	3-4
Figure 3-4	RPX Label	3-13
Figure 4-1	Single Remote Feeding DC/DC Converter	4-1
Figure 4-2	Operation-States of the Remote Feeding	4-3
Figure 4-3	Management Protocol Stack	4-5
Figure 4-4	TACACS+	4-8
Figure 4-5	File-Transfer	4-14
Figure 4-6	Acknowledge of Alarms	4-21
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	1-5
Table 2-1	Ambient Conditions.	2-1
Table 2-2	RPX16 Front-View	2-4
Table 2-3	LED Start-Up.	2-4
Table 3-1	DC-Input Connection	3-3
Table 3-2	Standards	3-5
Table 3-3	SDSL_in Port Pinning	3-7
Table 3-4	SDSL_out Port Pinning.	3-8
Table 3-5	Pin-assignment Control Port (RS232).	3-12
Table 4-1	Settings Auto-Negotiation	4-16
Table 7-1	RPX 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 Quick Reference.	7-18
Table 7-7	Example for SSH-Script	7-19
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	Number of Interfaces	A-4
Table A-5	Technical Data of the Interfaces	A-4
Table A-6	Technical Data remote Power Feeding.	A-5
Table A-7	Display Functions	A-6
Table A-8	µController and Clock.	A-6
Table A-9	Technical Data of the RPX - Software	A-7
Table A-10	Management & Security	A-8

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.

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.

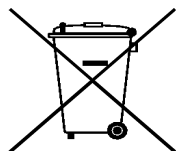
Repair

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.

Chapter 1

Abstract

RPX16 Description

General

The RPX16 - Remote Power Unit is a device to feed devices across twisted pair. It offers 16 independent feeding interfaces. The RPX16 is designed to be placed into a SDSL line, mainly in between the Central Office (MSAN etc.) and a repeater. But the applications are not limited to this case.

Each of the 16 remote feeding units offer a capability of 115VDC and up to 60mA (for a short period of Time the power supply can offer 70mA), which is roundabout 7W per line. Each line is individually monitored, whether the voltage and current is in given ranges. In case of detected errors, the line is automatically shut-down to prevent dangerous situation and damage of devices.

The RPX16 is a fully managed device. Several protocols can be used to get access to the device for configuration and monitoring. Alarms can be detected and raised. Web-based GUI gives a user-friendly interface and ssh-CLI is more for automating processes. With SNMP the integration into umbrella management systems can easily be done.

Application Areas for the RPX

Feeding SDSL Repeater

The main application for RPX16 is feeding up to 16 x 2 SHDSL-repeaters from central office place.

The RPX16 is installed between LT and the first repeater and adds the remote feeding power onto the SDSL-line. The SDSL signal is neither derated nor in other ways effected. The repeater takes the remote power for its feeding and can forward it to the next unit, if required.

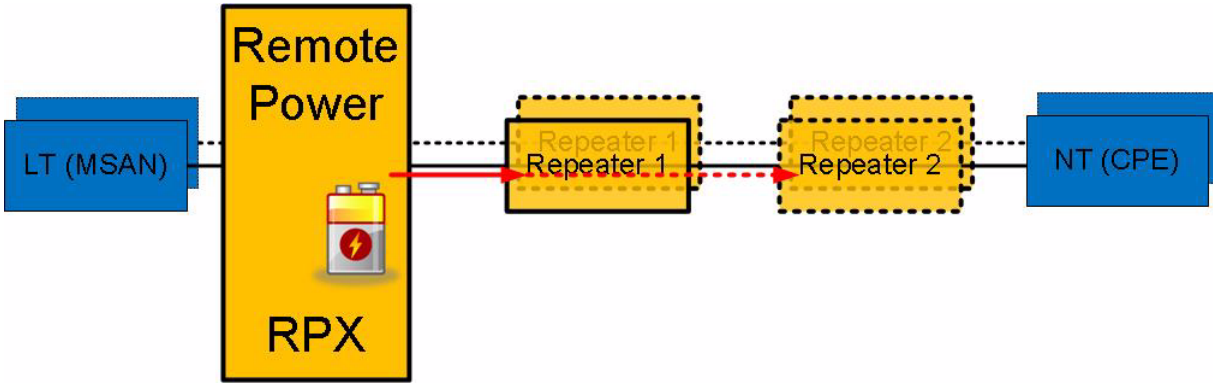


Figure 1-1 RPX Application SDSL Repeater

Feeding CPE

The remote feeding is not limited to a special load-device. Other devices than repeaters can be served, e.g. the NT. Only limitation is the maximum power, which can provided per line (7W).

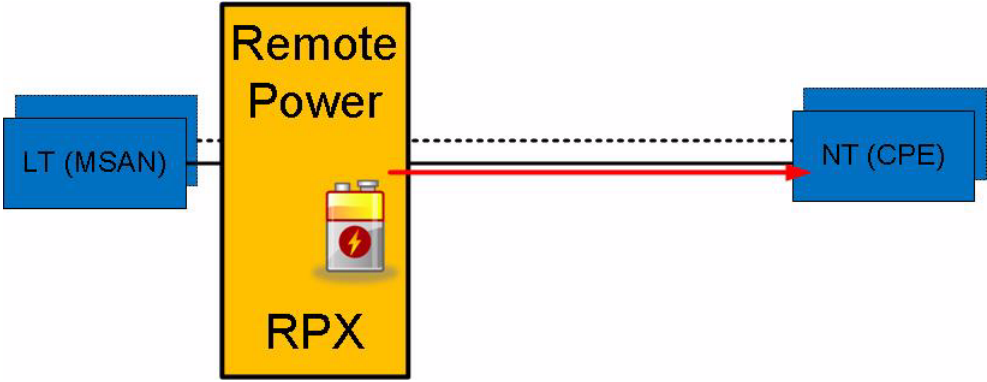


Figure 1-2 RPX Application CPE-Feeding

In cases, were the CPE does has higher power demand than 7W, more than 1 feeding line can be bundled to achieve higher power capability. Each feeding current is transported over a separate copper TP and the CPE has to add them.

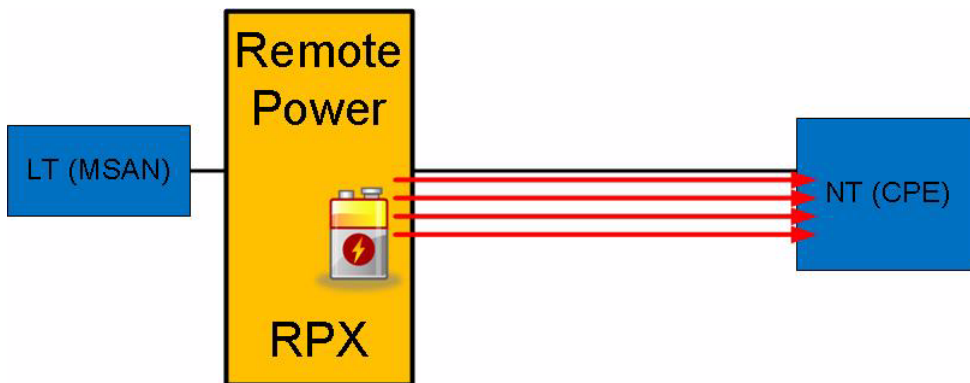


Figure 1-3 RPX Application CPE Multiple-Feeding

Separate Cable

The RPX16 is not limited to be used in conjunction with SDSL data transmission. It can also be used to feed a remote device, which is used for fibre optic data transmission. In this case, the feeding copper-pair is not used for data-transport but solely for the remote-feeding. A good way to power optical repeaters, demarcation units etc.

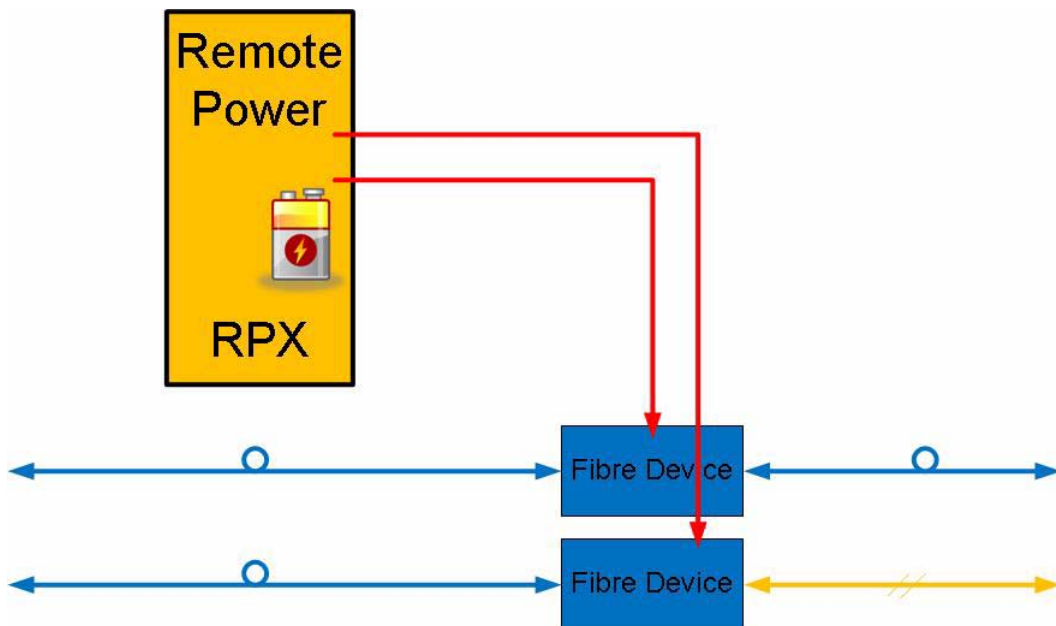


Figure 1-4 RPX Application Extra-Feeding Net

RPX16 Functions at a Glance

The RPX16 - Remote Power Unit can provide remote power on up to 16 lines. Each line can be powered with 7W. The intention is mainly to power 2 repeaters (BRX1) on each line, but the usage is not limited to this application. The filters onboard are designed to place the device into a SDSL-line. The onboard agent capability makes it easy to integrate the RPX into provider's network management system.

RPX16 incorporates the following features:

Power Feeding & Supervision

- Remote power feeding for up to 16 lines
 - each line has the capability to feed 114VDC, 60mA (peak 70mA) --> 7W
- each line can be individually enabled/disabled
- ongoing measurement of voltage and current for each line
- open circuit detection for each line
- short-circuit detection for each line
 - automatic switch-off if short-current is detected
 - automatic restart of the line after 30sec
- ongoing measurement of earth leakage and asymmetrical line

Management

- Network management for monitoring and management
 - HTML based WEB-GUI,
 - Built-in SNMP-agent and
 - SSH (CLI)
- Local management interface (TCP/IP) available.
- Two remote management interfaces (TCP/IP) available. The two ports are switched onboard to cascade the DCN easily.

Housing and Power Supply

- Fan less solution at Rack-montage and Desktop Units
- DC power supply: -48/-60VDC
- 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 RPX monitors its power supplies. If there is a failure detected the RPX 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 RPX16 is the sole member of RPX16 - Remote Power Unit family.

Table 1-1 Order Matrix

Art.- No.	Short Name	Description
1303-1001	RPX16	Remote Power Unit: <ul style="list-style-type: none">• 16 lines with up to 2 fed units per line;• 114V, 60mA per line;• Used for SDSL data transmission via copper TP;• DC (-48V/-60V) power supply.

Chapter 2

Getting Started

For the start-up of the RPX 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:

- RPX16 - Remote Power Unit,
- Short User-Information.

Preparing the Start-up

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

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 RPX, are shown in Table 2-1.

Table 2-1 Ambient Conditions

Operating Temperature	+5°C to +55°C
Max. Relative Humidity (non-condensing)	<100% (30°C)

Getting Started

Preparing the Start-up

Table 2-1 Ambient Conditions (continued)

Input Voltage DC	-40 to -75VDC
Power Consumption:	
• all RF-ports disabled	< 6.5 VA
• max, when all ports in full load	< 27.0 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 RPX can be mounted into a ETSI- or 19"-rack. For this purpose, two mounting angles are pre-assembled on both sides the unit. In factory default, the angels fit for 19" racks. Use them to fix the unit as usual



Figure 2-1 Rack Mount-Angles 19-Inch

In case the device shall be installed into an ETSI-shelf, the two angels can be loosen and attached in the opposite way. Then it fits for ETSI.



Figure 2-2 Rack Mount-Angles ETSI

Airflow Requirements

There are no fans installed inside the RPX 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 2-3 RPX Ventilation Louvres

Start-up of the RPX16

Switching on the Device

The RPX does not have any power switch. If power is supplied to the unit, it will start fully automatically. The RPX does have 1 single power input: DC (-48 or -60VDC).

Power-Up Sequence

After providing power to the RPX, the RPX will be powered up. The start-up will take several seconds, while internal SW is started and some tests are done to verify the RPX 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 the user to

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

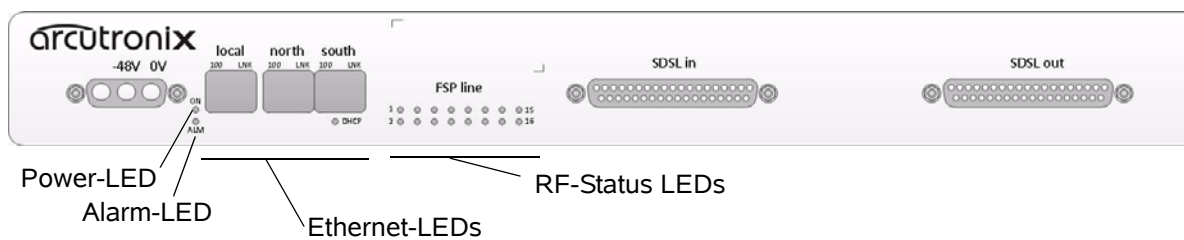
LED Start-Up

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

- Power- and Alarm-LED
- RF-Status LEDs
- Ethernet LEDs, build-in RJ45 connectors and below the RJ45

See the following picture for the different categories:

Table 2-2 RPX16 Front-View



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

Table 2-3 LED Start-Up

State	ON-LED	Alarm-LED	RF-Status-LEDs	Ethernet-LEDs
S1 "Boot-Seq.", (after Power On) Duration: ~10sec	LED is blinking fast	LED is ON	All LEDs are OFF	All LEDs are OFF
S2 "Boot-Finished" Duration: ~2sec	LED is ON	LED is ON	All LEDs are ON	All LEDs are red
S3 "Start Linux" Duration.: ~3 sec	LED is ON	LED is ON	Normal operation.	All LEDs are red

Table 2-3 LED Start-Up (continued)

State	ON-LED	Alarm-LED	RF-Status-LEDs	Ethernet-LEDs
S4 “Start Apps” Duration.: ~15 sec	LED is ON	LED is ON	Normal operation.	LED colour switches from red to yellow and then from yellow to green
O1	LED is ON	Normal operation = Alarm status of the card/rack is shown.	Normal operation.	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 RPX has three Ethernet interfaces, which can be used for management access. The “local” port is mainly intended to be used by direct connection using a local Laptop/PC.

The both ports “north” and “south” are switched internally and shall be used for remote management access via a DCN. The switching capability of the two ports makes it easy to install several units of RPX in one rack and cascade the DCN from one RPX to the next.

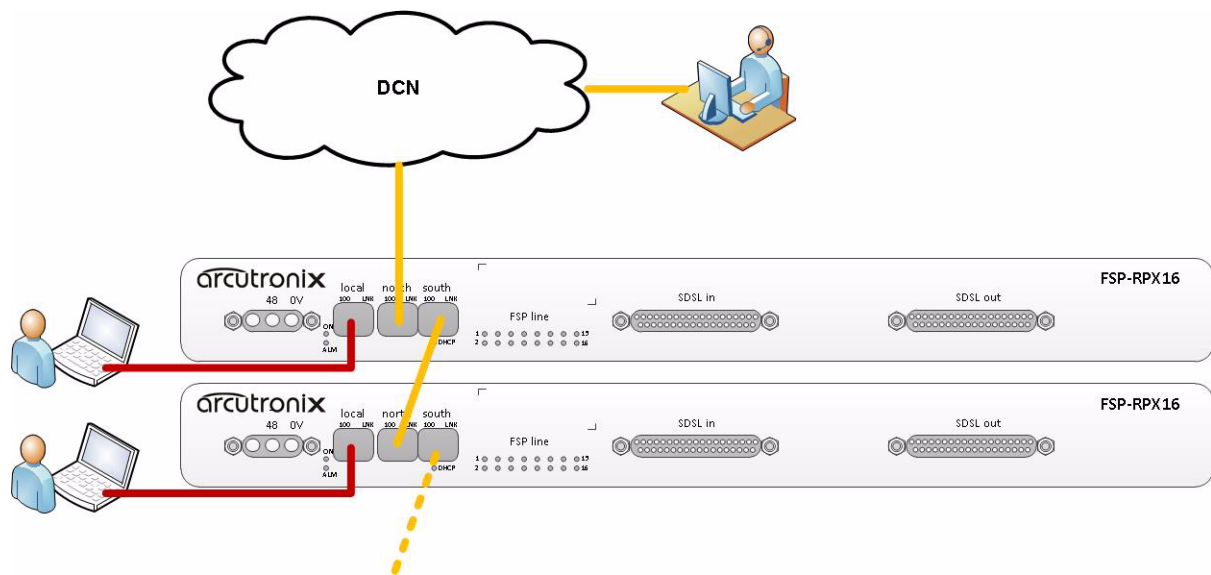


Figure 2-4 Management Access

All three interfaces are 10/100BaseT ports, supporting Auto-Negotiation and Auto-Cross-Over. The default setting for Auto-Neg is 100M, Full Speed, Duplex Mode.

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 RPX and maintain the chassis via a long distance. The Ethernet-based transmission systems can be used to hub the RPX into your local environment. The RPX 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 “remote” interfaces support the operation as Q-interface, according, [ITU-T M.3010]. In Q-mode, the device is waiting for an IP-address to be assigned via DHCP. As long as there is no valid IP-address assigned in Q-mode, the “DHCP”-LED is blinking. As soon as the IP-address is successfully assigned, the DHCP-LED is on.

By default the two interfaces do have the following settings

- “Local” is configured as F-interface (IP = 192.168.1.100/24).
 - The “Local” port is configured to act as DHCP-server and provides a valid IP-address in the subnet 192.168.1.0/24 to the attached PC/Laptop.
- “Remote” is configured as Q-interface (IP = DHCP-client).

Serial Access

The RPX 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 RPX 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 device.
2. The RPX "local"-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.

Secured Web Access

A secured web-access (https) is available. The access is the same as depicted in Chapter 2, Web Access, see above.

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.

SNMP Access

The RPX 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 both ports.

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 RPX16 - Remote Power Unit. This consist of block-diagram and a detailed description of all external interfaces and function indicators.

The RPX16 is a compact unit. All external connection points for data lines, control elements and power 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 RPX16. The main blocks are shown and their logical connections are presented as lines in between.

The RPX16 can be divided into five functional blocks:

- Control-Plane,
- Local Power,
- Remote Power Feeding.

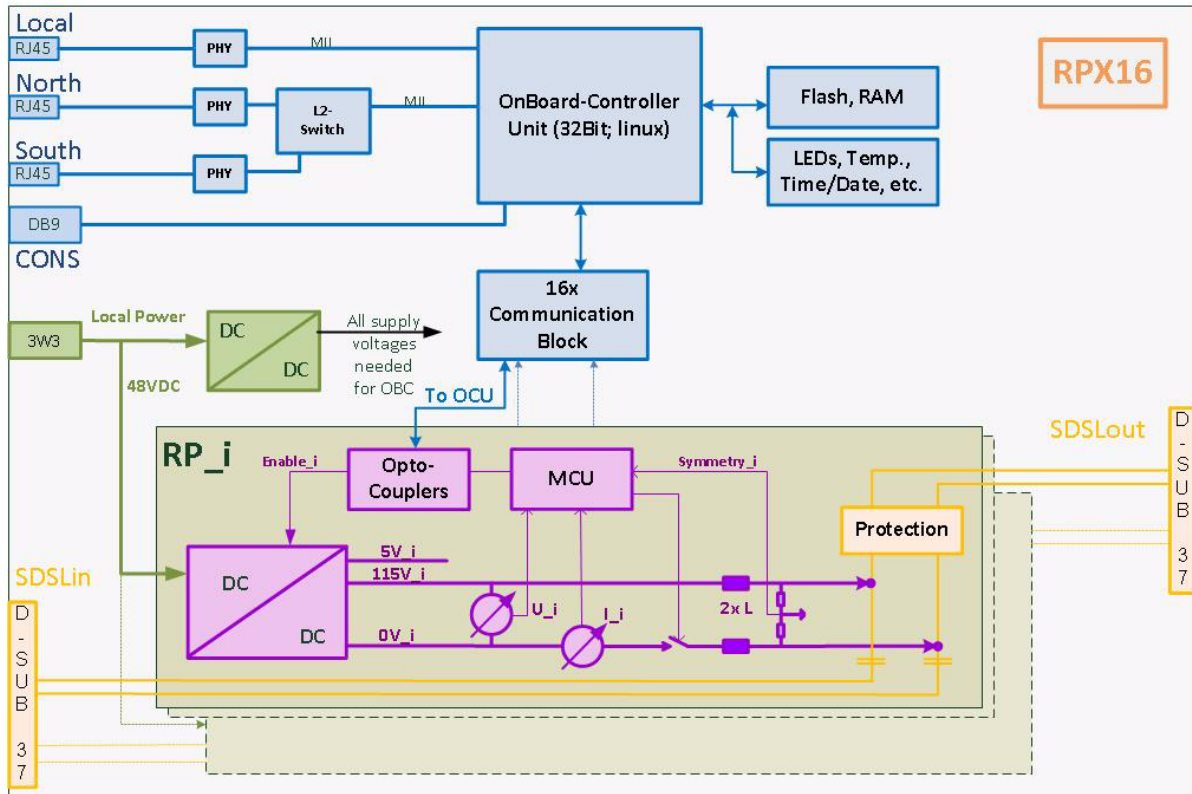


Figure 3-1 RPX16 Block-Diagram

Figure 3-1 gives an overview to the functional blocks. On the top one sees the OnBoard-Controller which controls 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 “Local”,
- Out-of-band management I/Fs, called “North” and “South”,
- RS-232 serial interface, called “Console”.

The local power-block generates all required supply voltages which are needed for the OBC and its peripheral devices. Its input is the DC-connector.

The RPX16 carries 16 independent Remote-Power blocks. The 16 blocks are identical to each other and each provides the capability of 115DVC, 70mA which can be added to the SDSL line. Each RP-block includes a small micro-controller unit (MCU), which checks voltage and current. If a failure is detected, the MCU can limit the current and disable the output to prevent dangerous situations. The OBC can communicate with each of the MCUs to get knowledge about the status of each block and to change settings during run-time. If one RP-block is needed at all, the OBC can disable the complete block to save energy.

Connectors and LEDs

The RPX16 has all its 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.

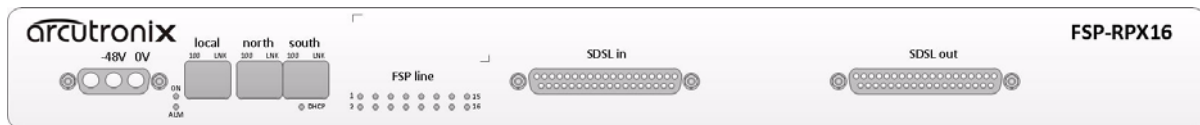


Figure 3-2 RPX Front-View

Figure 3-2 shows the complete front. The front can be separated in 4 parts, which will be depicted in more details, hereafter:

- Power
- Management & Status,
- Remote-Feeding Status LEDs,
- SDSL in- and out-ports.

Power Connector

Most to the left of the front panel the access port for DC-power is located.

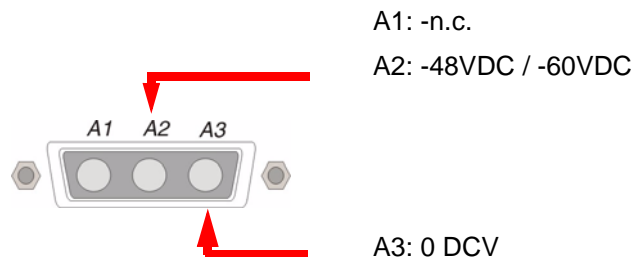


While working with the system, always adhere to the appropriate safety measures for handling electronic devices. Read the power precaution in Chapter 0, **Power Precautions** carefully before using the device.

DC Power Supply

The RPX offers one DC power supply. It can operate at in a range of -48 to -60 VDC (-40...-72VDC). The DC input is protected by a 5A fuse. The connector for the DC-input is a male 3W3-connector. Table 3-1 shows the right connection of the DC input connector.

Table 3-1 DC-Input Connection



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".

Management Interfaces

The RPX16 offers 3 management interfaces:

- LOCAL
- NORTH
- SOUTH

Ethernet Features

All three management ports are equipped with an "auto-crossover" function so that both crossover cable and patch cables can be used at any time. "Auto cross-over" feature works independently and needs no configuration or support of the user.

The 'LOCAL' port is intended to be used for local management access via laptop / PC, providing direct access to the management application of the device. The "local" IP interfaces (with local IP address) can be used.

The ports called 'NORTH' and 'SOUTH' are internally connected via an Ethernet switch and can pass data in both directions. The interface "NORTH" is for connecting to a DCN, which allows remote access to the device. The interface "SOUTH" is used for cascading the DCN to a next device. (The cascade is done by connecting the SOUTH-port to the next NORTH-port). The device has, in addition of the local IP interfaces, a "remote" IP interface, to access the device via the DCN. The remote IP interface is only accessible via the NORTH port! Packets coming from the SOUTH-port are only forwarded to the NORTH-port, but can never reach the device.

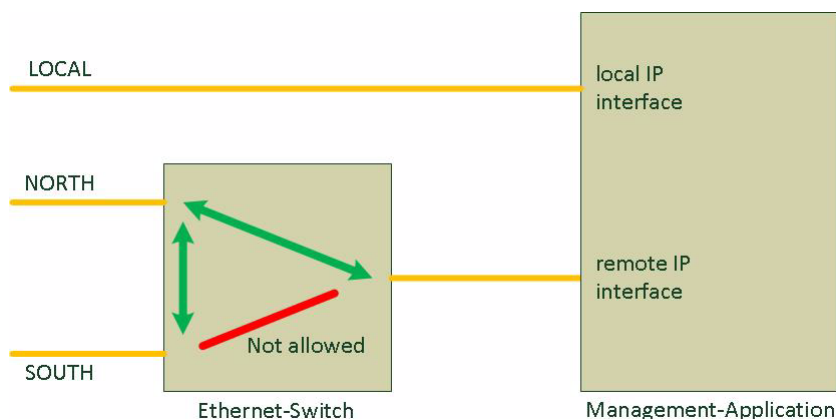


Figure 3-3 RPX Management Access

10/100BaseT (RJ45)

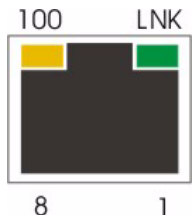
The Ethernet ports have two indicators each to give information about link state and activity (LNK), and speed (100). The device negotiates the operating mode of the corresponding interface automatically with the remote station using Auto Negotiation (if activated). Half-duplex and full-duplex connections 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	RJ45 8-pins:

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	-



- 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.

VLAN Features

The device supports VLAN at the remote management access. For the remote access a (management) VLAN ID can be assigned. All packages should be sent to Application Management, then you must have this VLAN on NORTH port. Likewise, all packets that are sent from the management application on the NORTH-port, provided with this VLAN ID.

IP Features

The RPX16 supports both IPv4 and IPv6.

The RPX16 offers two management IP interfaces through which the device is accessible:

- Local IP Interface
- Remote IP Interface

The local IP interface can only be achieved through the management port "LOCAL". This interface is configured to operate as a DHCP server and assign an IP address to a connected laptop / PC fully automatically. This is to facilitate communication as soon as possible. The (default) IP address on the local IP interface is:

- 192.168.1.100 / 24

The remote IP interface can only be achieved through the management port "NORTH". This port is configured as a DHCP slave and expects to assign a valid IP address. As long as the DHCP LED flashes no valid IP address could be obtained. Only if the DHCP LED glows continuously, assignment worked.

SDSL Ports

The RPX16 has one a connection port that leads to the MSAN, and one port that leads in the direction of the remote device (RD). Each port is a DSUB37 and all 16 SDSL interfaces (upstream and downstream) are placed there. For security reasons, the two ports are different in their mechanics:

- SDSL_in: port in direction to MSAN is a DSUB37 plug,
- SDSL_out: port in direction to RD is a DSUB37 jack.

Only the port in direction to RD can be charged with the remote feeding. Upon delivery, all 16 remote supply units are turned off. After a power failure or shut-down of the unit, the previously status for each of the 16 lines is automatically recovered.

Table 3-3 *SDSL_in Port Pinning*

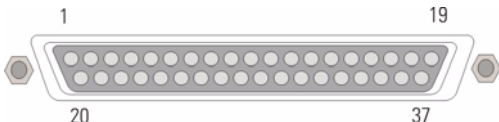
Pin	Signal	Meaning
SDSL_in (to MSAN): D-SUB37, male		
		
1	SHD	Shield
19	SDSL_in_1a	tip/ring line1 to MSAN
37	SDSL_in_1b	
18	SDSL_in_2a	tip/ring line2 to MSAN
36	SDSL_in_2b	
17	SDSL_in_3a	tip/ring line3 to MSAN
35	SDSL_in_3b	
16	SDSL_in_4a	tip/ring line4 to MSAN
34	SDSL_in_4b	
15	SDSL_in_5a	tip/ring line5 to MSAN
33	SDSL_in_5b	
14	SDSL_in_6a	tip/ring line6 to MSAN
32	SDSL_in_6b	
13	SDSL_in_7a	tip/ring line7 to MSAN
31	SDSL_in_7b	
12	SDSL_in_8a	tip/ring line8 to MSAN
30	SDSL_in_8b	
11	SDSL_in_1a	tip/ring line9 to MSAN
29	SDSL_in_1b	
10	SDSL_in_2a	tip/ring line10 to MSAN
28	SDSL_in_2b	

Table 3-3 *SDSL_in Port Pinning*

Pin	Signal	Meaning
9	SDSL_in_3a	tip/ring line11 to MSAN
27	SDSL_in_3b	
8	SDSL_in_4a	tip/ring line12 to MSAN
26	SDSL_in_4b	
7	SDSL_in_5a	tip/ring line13 to MSAN
25	SDSL_in_5b	
6	SDSL_in_6a	tip/ring line14 to MSAN
24	SDSL_in_6b	
5	SDSL_in_7a	tip/ring line15 to MSAN
23	SDSL_in_7b	
4	SDSL_in_8a	tip/ring line16 to MSAN
22	SDSL_in_8b	
2, 3, 20, 21	-	not used.

Table 3-4 *SDSL_out Port Pinning*

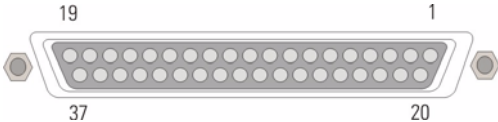
Pin	Signal	Meaning
SDSL_out (to RD / Repeater): D-SUB37, female		
		
19	SHD	Shield
1	SDSL_in_1a	tip/ring line1 To RD / Repeater
20	SDSL_in_1b	
2	SDSL_in_2a	tip/ring line2 To RD / Repeater
21	SDSL_in_2b	

Table 3-4 *SDSL_out Port Pinning*

Pin	Signal	Meaning
3	SDSL_in_3a	tip/ring line3 To RD / Repeater
22	SDSL_in_3b	
4	SDSL_in_4a	tip/ring line4 To RD / Repeater
23	SDSL_in_4b	
5	SDSL_in_5a	tip/ring line5 To RD / Repeater
24	SDSL_in_5b	
6	SDSL_in_6a	tip/ring line6 To RD / Repeater
25	SDSL_in_6b	
7	SDSL_in_7a	tip/ring line7 To RD / Repeater
26	SDSL_in_7b	
8	SDSL_in_8a	tip/ring line8 To RD / Repeater
27	SDSL_in_8b	
9	SDSL_in_1a	tip/ring line9 To RD / Repeater
28	SDSL_in_1b	
10	SDSL_in_2a	tip/ring line10 To RD / Repeater
29	SDSL_in_2b	
11	SDSL_in_3a	tip/ring line11 To RD / Repeater
30	SDSL_in_3b	
12	SDSL_in_4a	tip/ring line12 To RD / Repeater
31	SDSL_in_4b	
13	SDSL_in_5a	tip/ring line13 To RD / Repeater
32	SDSL_in_5b	
14	SDSL_in_6a	tip/ring line14 To RD / Repeater
33	SDSL_in_6b	
15	SDSL_in_7a	tip/ring line15 To RD / Repeater
34	SDSL_in_7b	

Table 3-4 *SDSL_out Port Pinning*

Pin	Signal	Meaning
16	SDSL_in_8a	tip/ring line16 To RD / Repeater
35	SDSL_in_8b	
17, 18, 36, 37	-	not used.

LEDs

Several LEDs show the (operational) status of the device. During start-up of the device the LED have different meaning than during normal operation (see “LED Start-Up” on page 2-4). In this chapter, the behaviour after successful start-up is depicted.

ON & ALM

The ON-LED is used for power-supply indication, while the ALM-LED shows the alarm status of the device. After Power-On of the device, both LEDs will be on.

ON-LED Display states of the LED:



off No supply voltage.



on Supply voltage available.



flashing Power available, device did not start (yet).

ALM-LED Display states of the LED:



off Neither error nor warning detected.



on Device has at least one error detected.





blinking 1.5 Hz Device has at least one warning (and no error) detected.

Ethernet




The device does have 2 management ports, which are used for Ethernet based access to the device. The two ports are RJ45 with integrated 2 LEDs each. The label of the 2

LEDs are 100 and LNK. The “REMOTE”-port does have an additional LED (DHCP), which indicates the status of IP-address assignment to this port.




100-LEDs Display states of the LED:

-  off The Ethernet port speed is 10Mbps (10BaseT).
-  on The Ethernet port speed is 100Mbps (100BaseT).

LNK-LEDs Display states of the LED:

-  off No Ethernet link detected.
-  on Ethernet link is established, and no traffic is ongoing.
-  blinking 1.5Hz Ethernet link is established, and traffic is transferred. The LNK-LED blinks for ingressing or egressing packets.



DHCP-LED Display states of the LED:



-  off Remote port is disabled or is acting as F-interface (DHCP-server is activated on this port).
-  on “REMOTE” port is operational and it has at least one valid IP-address (IPv4 or IPv6).
-  blinking 1Hz “REMOTE” port is searching an DHCP-server and waits for IP-address assignment.

Remote Feeding Status

Each of the 16 remote feeding units, has one LED to signal the actual status. the RF-status LEDs are all bi-colour: red and green. By mixing red and green, the LED can signal a third status: orange.

RF Status-LEDs Display states of the LED:

-  off The RF port is disabled.
-  green RF port is enabled and fully operational (no error).

-  on RF port has detected a warning status (current out of range or asymmetry).
-  on RF port has detected an error status (open circuit, overload, or over-voltage).

Console Port

For the RPX, 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 3-5 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 RPX operates in DCE mode, so “RXD” is an output, while “TXD” is an input!

Note: You have to connect the DTR signal (**D**ata **T**erminal **R**eady) 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 RPX. It must be full equipped cable, with all 9 signals connected (e.g. DCX-DB9M-DB9F [9500-0101] from arcutronix).

Labels

The unit carries 1 label with all the required data on it.



Figure 3-4 RPX Label

Remote Feeding

General

The RPX16 is mainly acting as a “managed” feeding unit with 16x fully independent DC/DC-converters. Each of the 16 DC/DC-converter are fully identical and provide the remote feeding power out of the DC input power.

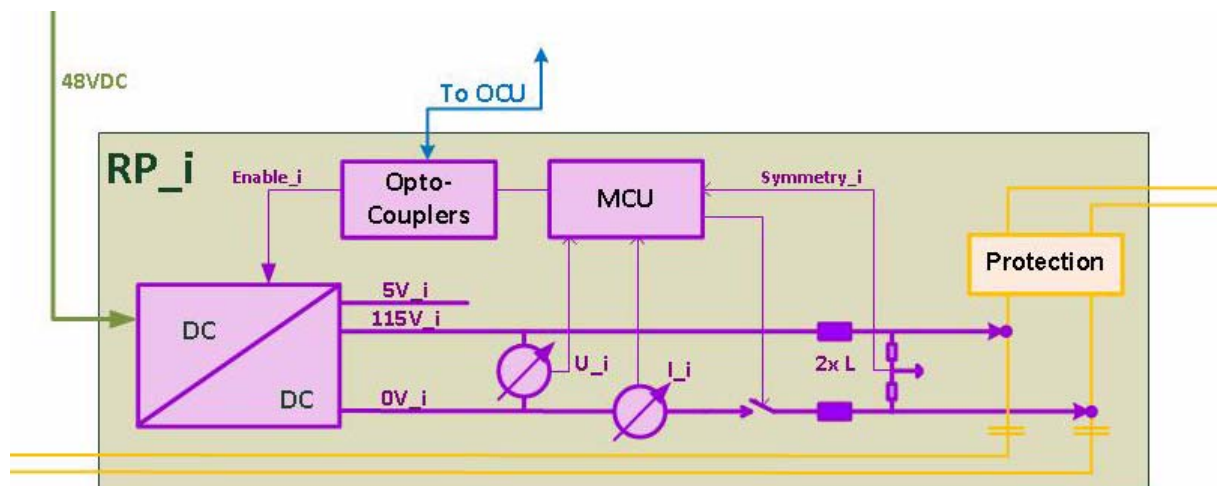


Figure 4-1 Single Remote Feeding DC/DC Converter

Each Remote-Feeding block, as shown in Figure 4-1, has in addition to the pure generation of the required output power also facilities to measure and supervise the outgoing power, the actual current and the symmetry of the SDSL-line. Some protection for each line completes the feature set.

The Remote-Feeding block can communicate with the control block on the device to report actual results of the measurement and to get settings like enable and disable. As the Remote-Feeding block is fully independent and galvanic isolated against all other blocks and the control block, some opto-coupler are needed to bring the communication channel from one side to the other.

The Remote-Feeding block monitors the power and current. In case a over-current or over-voltage is detected, the shut-down is done without the help of the control block. This is to make the security demands independent from any performance issue on the on-board controller. It is assured, that e.g. a SW-update or other resource hungry tasks will not affect the security and speed of reaction.

In case the Remote-Feeding block is not needed it can be disabled by management. The complete block is powered down and not only the feeding is disabled. This spares energy and increases the benefits.

Operation-States

The Remote-Feeding block measures the provided current and output-voltage. In dependency of the actual values, the system will generate an Operation-States, which is displayed (e.g. Web-GUI and LEDs) and reported in status-messages (traps).

8 different states are defined for the remote feeding:

#	State	Remark	LED
0	disabled	The port is disabled. The DC/DC converter is disabled.	off
1	normal operation	Everything is fine. Current and voltage are within the expected limits.	green
2	open circuit	An open circuit is detected, which is a current below ~6mA.	red
3	low current	Low current is detected. Low current is an indicator, that there is a load attached to the remote feeding, but it is lower than the expected low of 1 repeater. Either the attached repeater is not operating well, or something else is attached to the remote feeding. Low current is between ~6mA and ~10mA.	yellow
4	high current	High current is detected. High current is an indicator, that there is a load attached to the remote feeding, which causes a higher current than expected as maximum load. maximum load is 2x repeater plus 2x 650Ohms line-impedance. Either the attached repeater(s) are not operating well, or something else is attached to the remote feeding. High current is between ~50mA and ~60mA.	yellow
5	overload	In overload situation, there is too much current detected on the remote feeding. Overload is reached, when the current is above ~65mA. The current is limited to a absolute maximum of 70mA. when 70mA is reached, the remote feeding is activating the current limiter, which leads to a dramatic sink of the output voltage.	red

#	State	Remark	LED
6	overload shutdown	<p>The remote feeding block is shut-down due to an enduring overload situation. The overload shutdown is executed, when the output voltage falls below 90V (which is the case during current limiting) for more than 4 seconds.</p> <p>The remote feeding block is re-enabling the feeding every 30 seconds, to verify, whether the overload-situation is corrected and normal feeding can be re-established again.</p>	red
7	overvoltage shutdown	<p>Voltage above 120V is detected. This is a failure which can cause severe risk and the remote feeding is disabled for security reasons.</p> <p>The voltage is monitored permanently. As soon as the voltage drops below 118V, the remote feeding port is enabled again.</p>	red

Figure 4-2 displays the different operation states of the remote feeding ports and corresponded values of current and voltage:

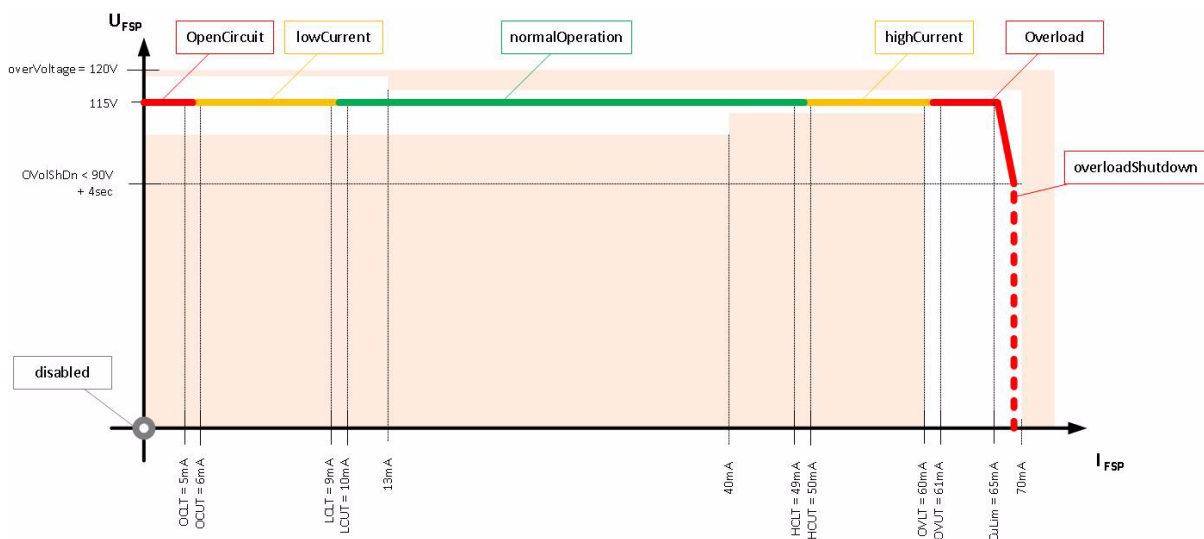


Figure 4-2 Operation-States of the Remote Feeding

The borders between the different states do have always 2 values (upper and lower value) to achieve a hysteresis. When the upper level is exceeded, the state is left and the state more to the left in the diagram is reached. When the value falls below the lower level, the state more to the right in the diagram is reached.

In the figure above a corridor is shown, in which the controller of the remote feeding keeps the voltage and current. The corridor is very narrow for high current to make

sure, the feeding can provide the required power for 2 repeaters in maximum distances and, in addition, to keep the voltage in a secure area for humans.

User & Access Administration

Access-Options to the RPX

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

- HTTP (Web-based GUI via TCP/IP)
 - See Chapter 5, RPX Web-GUI, and [axRefGuideWebGUI_RPX].
- HTTPS (Secured Web-based GUI via TCP/IP)
 - See Chapter 5, RPX Web-GUI, and [axRefGuideWebGUI_RPX].
- 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_RPX].
- CONSOLE-port (command-line-interface via RS-232)
 - See Chapter 7, SSH and CLI, and [axRefGuideCLI_RPX].

All five 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 RPX will deny to accept this.

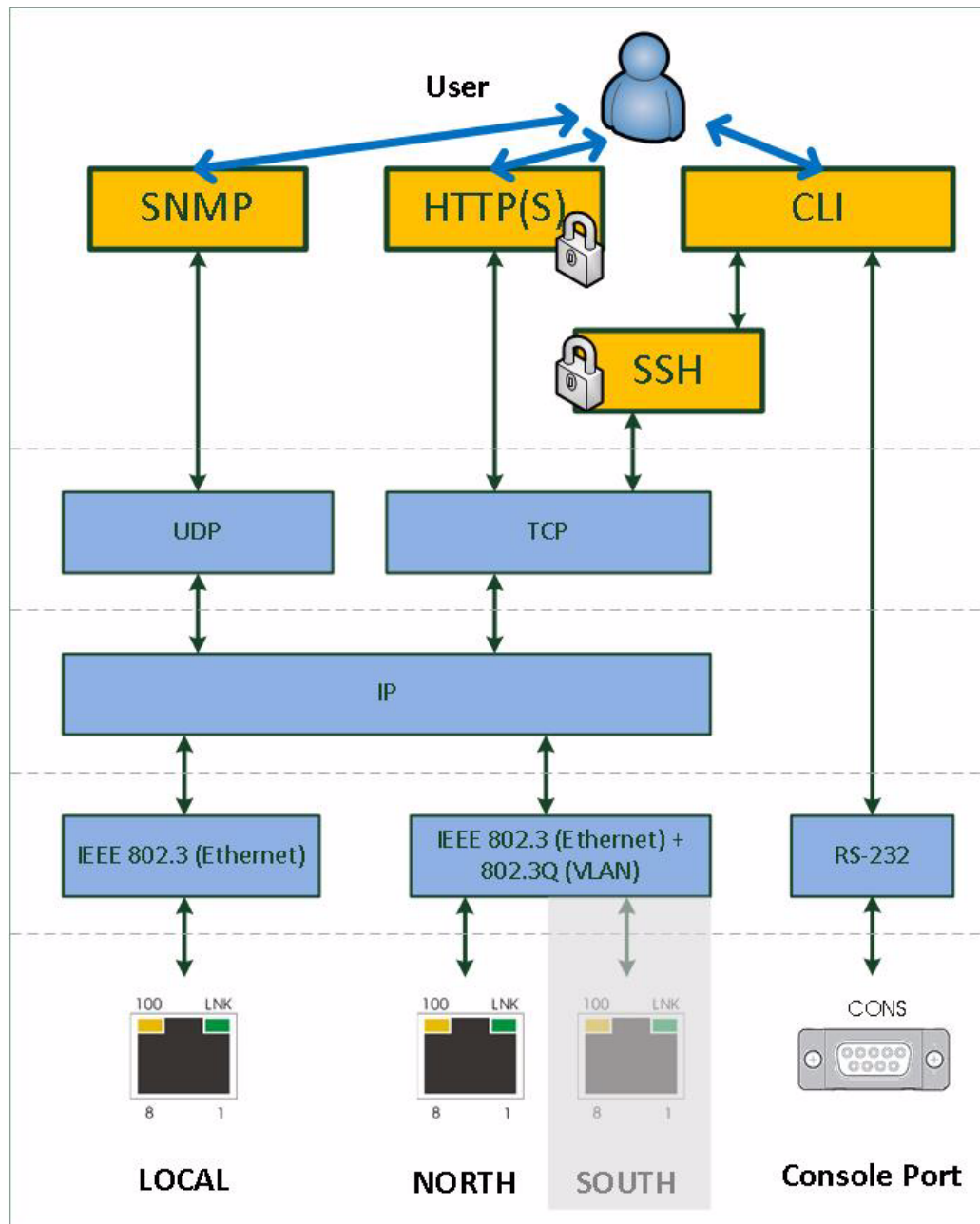


Figure 4-3 Management Protocol Stack

Figure 4-3 shows the protocol stack for the management access to the RPX and the attendant 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 RPX are protected by user-name and password. Several users can be configured on the RPX 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 RPX 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 RPX 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 RPX 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 RPX. 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 RPX, 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.

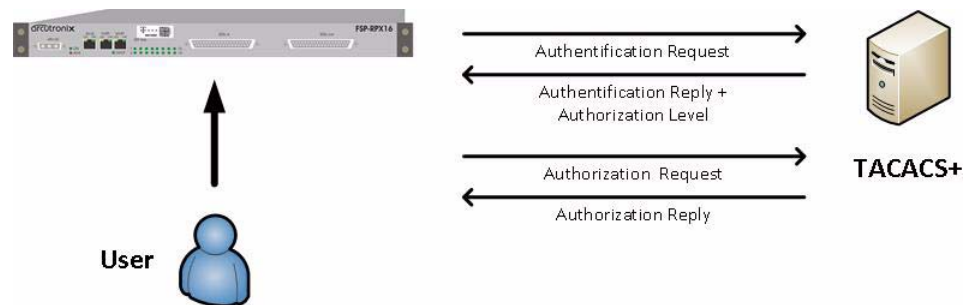


Figure 4-4 TACACS+

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 RPX can be managed via different protocols using the TCP/IP stack (see Figure 4-3) across the management interfaces "local" and "remote".

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 4-15.

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 a read-only entry.

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

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 "local"

The out-of-band management port "local" can be used in local (F-interface) mode only. The different behaviour are depicted in "F- and Q-Interface" on page 4-11.

The integration of the “local” port into a larger network management environment is not foreseen.

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

Management Ports “north” and “south”

The out-of-band management port “north” and “south” are linked together via a 3-port Ethernet switch. the 3rd port is connected to the onboard controller unit (OBU), so both interfaces can be used for access. “North” and “south” are intended for remote access via DCN.

The two ports can be used in remote (Q-interface) mode, only. The different behaviour are depicted in “F- and Q-Interface” on page 4-11. The default is Q-interface mode.

To integrate the “remote” port into a larger network management environment, it can be configured to use VLAN-tagging on the port. This is only sensible, 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.

As the “remote” management port is operating as DHCP-client by default, a DHCP-server is 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: no VLAN enabled
- Other Defaults: Act as DHCP-Client

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 RPX, 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 RPX is reachable within the existing IP-network.

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 RPX 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 RPX 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 RPX 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).

DNS-Support

RPX does support name service (DNS) to support easy access to the device. In f-interface mode, one can reach the RPX by using “ax-<device-type>” instead of the IP-address. For the RPX16 it would be **ax-RPX16**.

An example is shown below. The RPX16 has been assigned the IP-address **192.10.4.10**. A ping-command will result in the following:

```
C:\> ping ax-RPX16

Ping ax-RPX16 [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 RPX. In this case the new firmware can be uploaded to the device via several ways:

- HTTP, HTTPS, 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(S)” 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 RPX, 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(S)

The RPX 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 RPX:

- HTTP, HTTPS, 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:

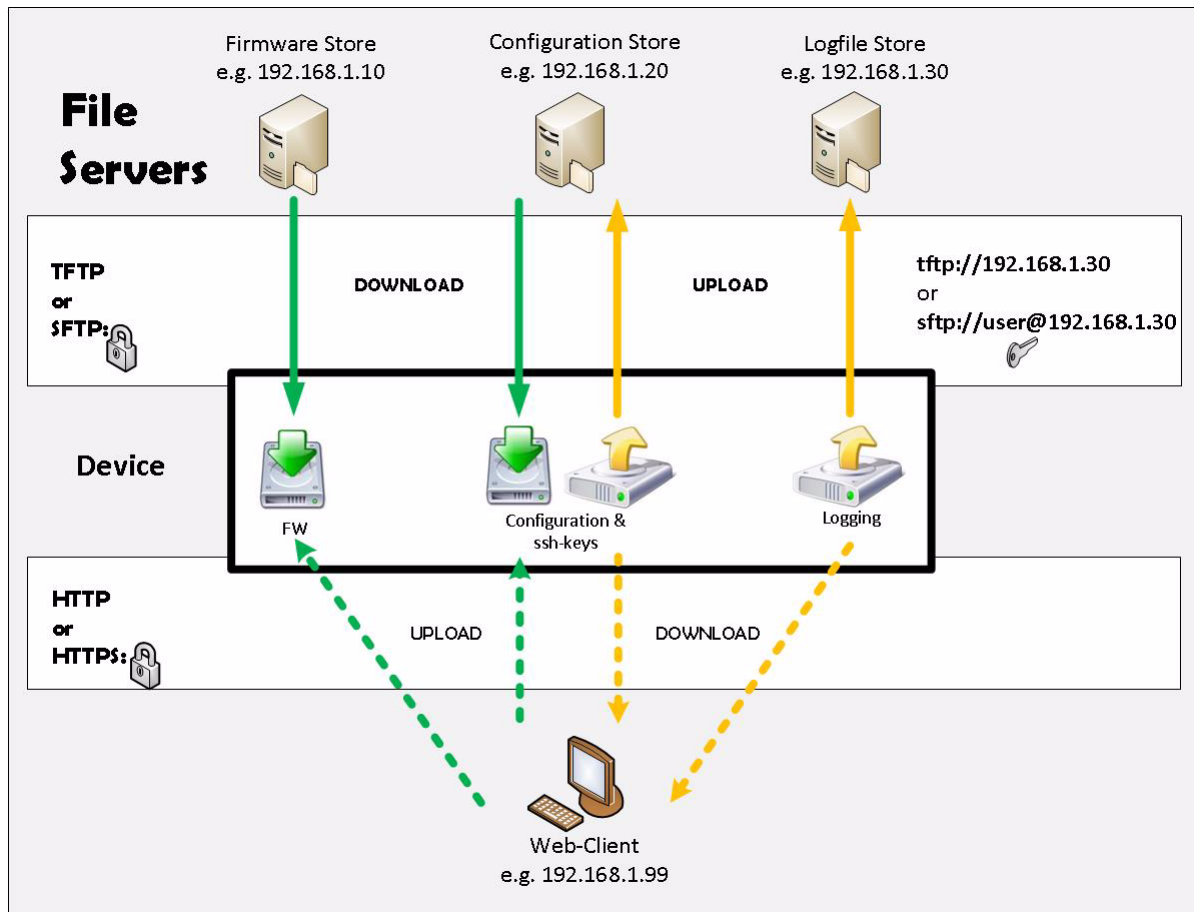


Figure 4-5 File-Transfer

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

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

HTTP-and/or HTTPS-file transfer can be disabled entirely due to security reasons.

NOTE: The usage of http (https) is only possible via a http- (https-) 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, RPX 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 4-1 *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 4-1 Settings Auto-Negotiation (continued)

Setting (Port Speed)	Result		
	Speed	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 RPX ports do support full duplex mode.

Alarm Management

The RPX 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.

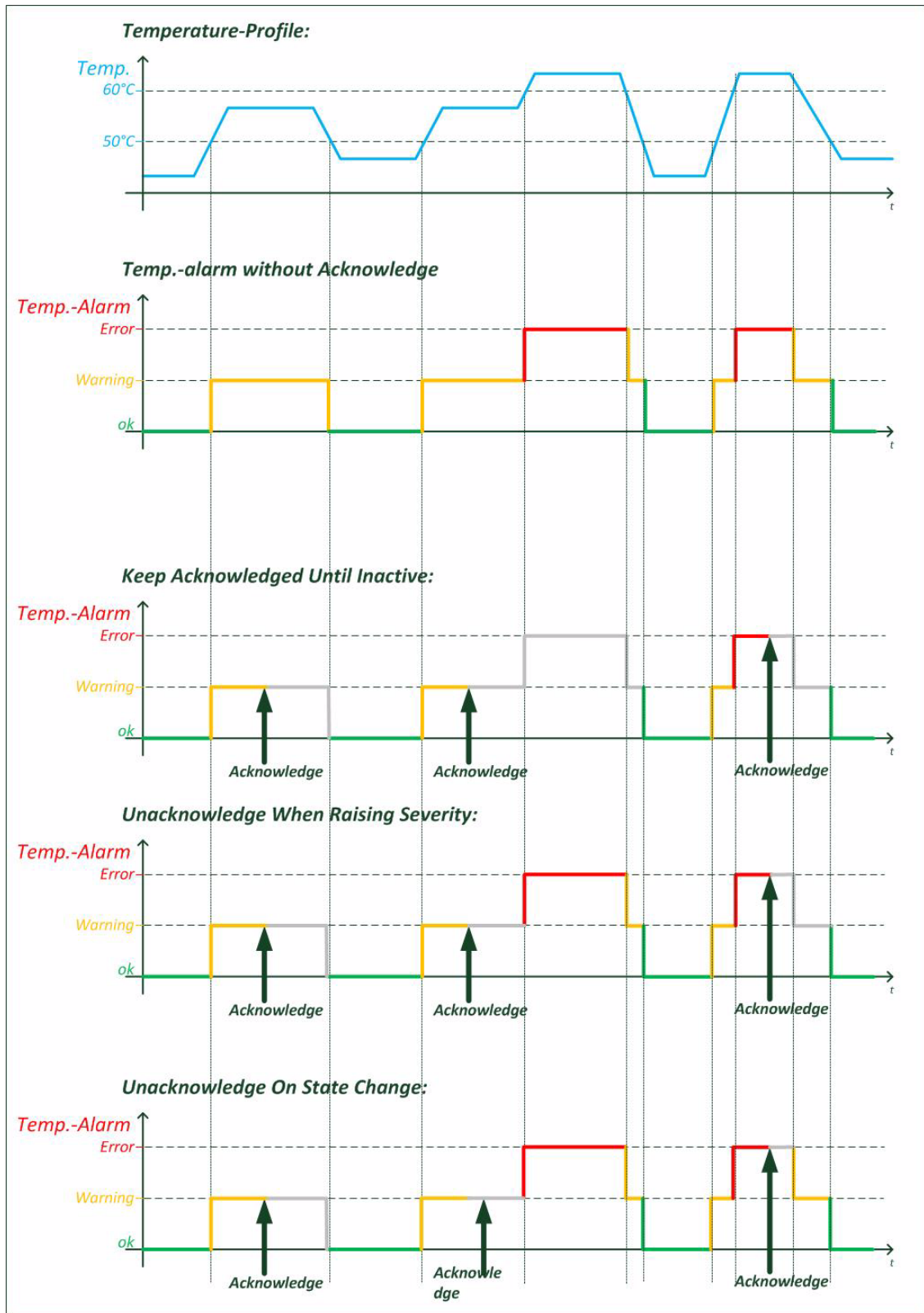


Figure 4-6 Acknowledge of Alarms

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 RPX 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 RPX does have an internal clock, which can be set by either user or via NTP-server(s). This gives the RPX the chance to provide proper time-stamps in logging and alarms. In case of power-failure, the RPX 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 RPX 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 RPX 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 RPX 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 RPX 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 RPX sends a request for time to a NTP-server. The server responds to the RPX with a time-stamp along with any one of a number of pre-agreed encrypted keys. On receipt of the time-stamp, the RPX un-encrypts the supplied key and verifies it against a list of trusted keys. The RPX can then be sure that the received time-stamp was indeed transmitted from the intended server. RPX 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 RPX 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
MGMT IP Config	All the IP settings for both management interfaces (out-of-band management ports), including: IP-address, net-mask, Default-GW and 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.

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 RPX. 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 RPX 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(s).

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

RPX Web-GUI

The RPX 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_RPX].

Introduction

Access to the Device

The RPX Web-GUI can be accessed via the both management ports (“LOCAL” and “REMOTE”). 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 RPX 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 4-4, 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 RPX, 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 RPX Web-GUI. At the top left is the Arcutronix logo. At the top right, there is a warning icon followed by the text "FSP-RPX16: #A201300112" and "Serial: A201300112". Below this, there are two input fields: "User Name" and "Password". A "Login" button is positioned below the password field. The background of the login area is light blue.

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 RPX 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.

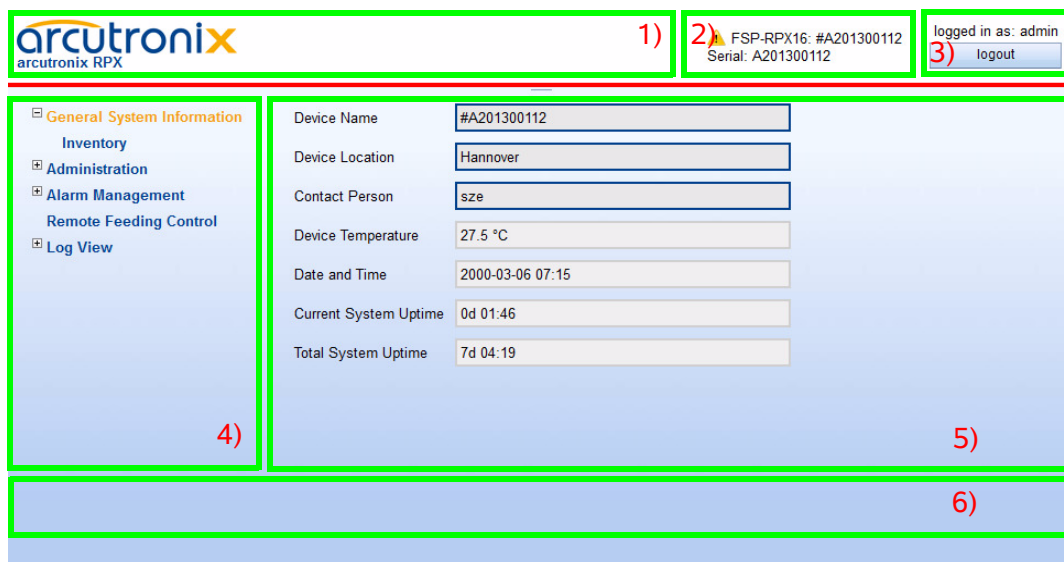


Figure 5-2 Web-GUI's Appearance



1. Logo/Family Pane.
2. Info Pane: Info about
 - device-type (here RPX-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 RPX

The main view of the RPX 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_RPX]. 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 RPX.

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 RPX by SNMP, one has to prepare the SNMP management system. First install the MIBs for the RPX 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)

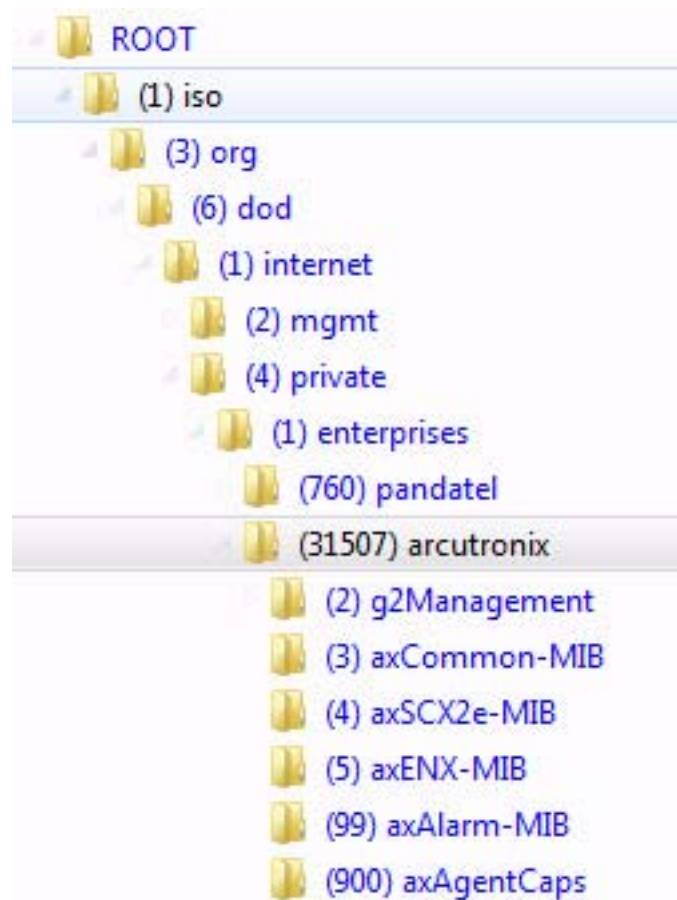


Figure 6-1 The SNMP ax-MIB Tree (1.3.6.1.2.4.1.31507)

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 RPX 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_RPX].

Access to the Device

The RPX CLI can be accessed either via

- CONSOLE port (115200, 8N1),
- LOCAL management interface,
- REMOTE management interfaces.

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 3-12.

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

SSH Connection

To establish the SSH connection between RPX 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 4-6 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.

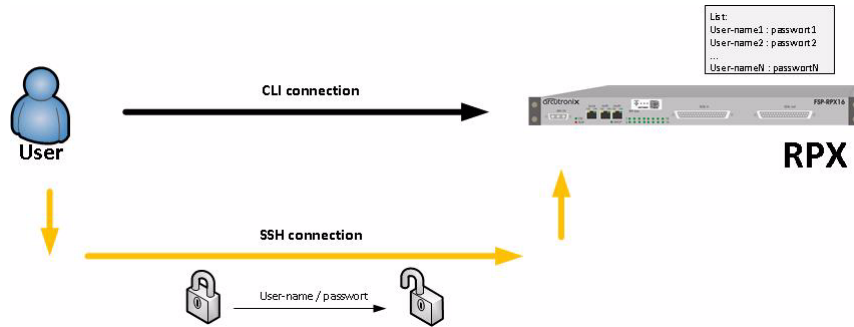


Figure 7-1 SSH-connection using User-Name and Password

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 4-6 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.

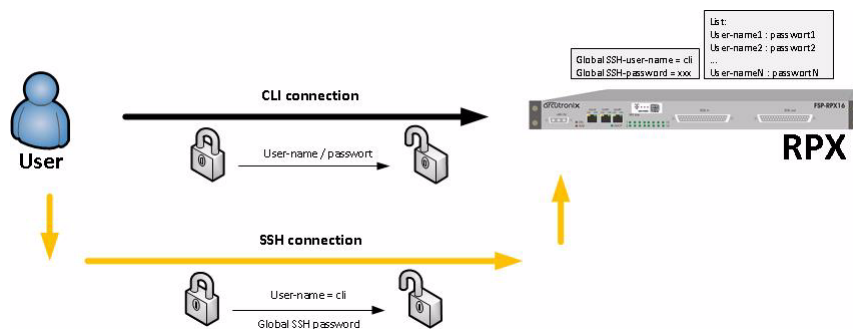


Figure 7-2 SSH-connection using Global SSH-Password

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.

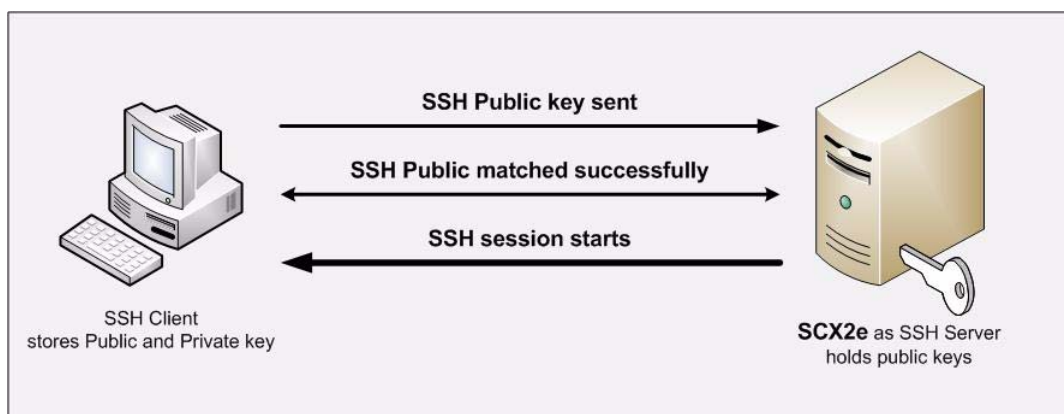


Figure 7-3 Secure Shell - Public Key

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 RPX 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.

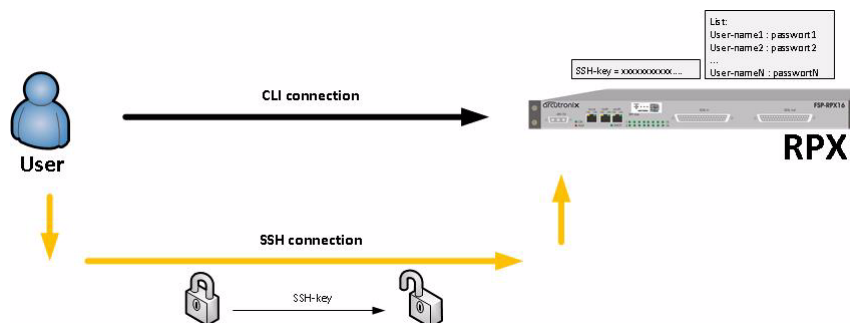


Figure 7-4 SSH-connection using SSH-Key (Direct Login)

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 4-6 for defining local users and usage of TACACS+.

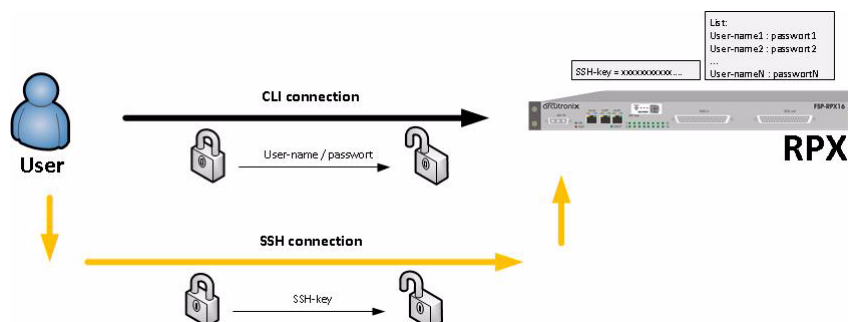


Figure 7-5 SSH-connection using SSH-Key (Connection Key)

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 RPX 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 4-4, 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 RPX SSH-server establish a link via TCP/IP:

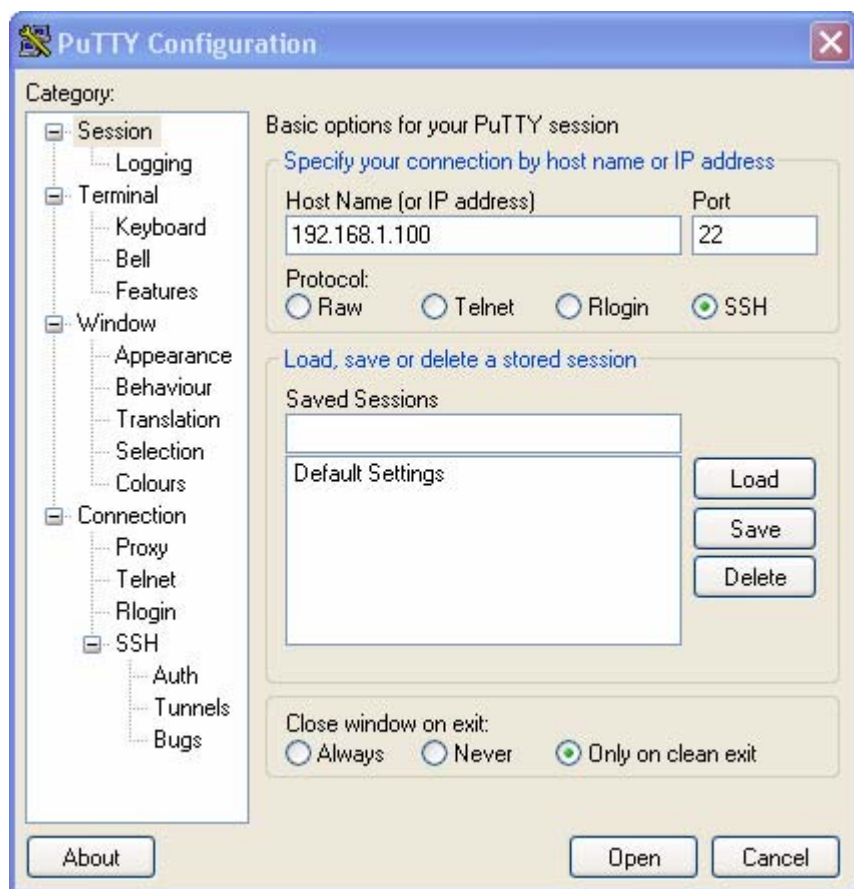


Figure 7-6 PuTTY SSH-Connection

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

RPX 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 = RPX16,
2. Device Name = “RPX16” 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:


RPX16 "RPX-test" / \$>
1. 2. 3. 4.

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

```
RPX16 RPX-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:

```
RPX16 RPX-test" /.1 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 RPX CLI editor provides hot keys.

Table 7-1 RPX 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 RPX 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 RPX CLI like in a hierarchically structured tree. Command options and applications vary depending on position within this hierarchy.

To assist users in navigation through RPX 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 RPX 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_RPX].

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

```
RPX16 "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

Type	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>

Quick Usage Guide for CLI-Commands

Table 7-6 CLI Quick Reference

Show options in actual menu:
<pre>\$> config</pre>
Change Contact Person: [General System Information -> Contact Person]
<pre>\$> config go General\ System\ Information \$> config set Contact\ Person "new Name"</pre>
Reboot Device: [Administration -> Reset System]
<pre>\$> config go Administration \$> config go Reset\ System \$> config set Reset\ Mode Immediate\ Reset \$> config do Start\ Reset</pre>
Go back 1 Step in Menu:
<pre>\$> config go up</pre>
Go back to Top-Level Menu (/):
<pre>\$> config go root</pre>
Show the complete path (remember, the path within the prompt is limited to 30 characters):
<pre>\$> config path</pre>

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 7-7 Example for SSH-Script

Step	Code
0	<pre>;; Tera Term Macro ;; ===== ;; file __prog_RPX.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

RPX Hardware Specification

Hardware & Power

Table A-1 to Table A-8 provide the general technical data of the RPX16 - Remote Power Unit.

Table A-1 Physics and Environment

RPX-Family	RPX16
Physical Dimensions	
Parameter	
Height	44 mm
Width	434 mm
Width with 19°-angle	482 mm
Width with ETSI-angle	532 mm
Depth	213 mm
Weight	2.9 kg
Environmental Conditions	
Operation:	ETSI ETS 300 019-1-3, class 3.1E
Temperature (hardened version)	-5 ... +55 °C
Humidity	10 ... 90%, non-cond.
Storage (in packing)	ETSI ETS 300 019-1-1, class 1.2
Temperature	-25 ... +55 °C
Humidity	10 ... 100%, non-cond.
Transportation:	ETSI ETS 300 019-1-2, class 2.3
Temperature	-40 ... +70 °C
Humidity	10 ... 95%, non-cond.
Others	
Ingress Protection:	IP30
DIN EN 60529 (VDE 0470 Part 1)	

Table A-1 Physics and Environment (continued)

RPX-Family	RPX16
Fan:	none
Cooling:	Convection cooling through ventilation slots in the housing environment

Table A-2 Security and EMC

RPX-Family	RPX16
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

RPX-Family	RPX16
Power Supply	
DC power supply ⁱ	
Supply voltage -48VDC	-40...-57 V DC
Supply voltage -60VDC	-50...-72 V DC
Supply current	< 4.0 A
Power Consumption ⁱⁱ	
Idle (no Remote Power enabled)	6.3 VA
Full Load (all Remote Power enabled and fully loaded)	20.0 VA
Max. power to be used per SDSL port	8.0 VA
Fuses	

Table A-3 Power Supply (continued)

RPX-Family	RPX16
Fuse, type	
DC	6A; 125V; onboard

- i. ETSI EN 300 132-2
- ii. The total power need depends on the remote feeding.

Interfaces

Table A-4 Number of Interfaces

Type		
Number of Interfaces		
RPX16	16x SDSL input (DSUB37, male),	General Purpose (Combo-port)
	16x SDSL output (DSUB37, female),	General Purpose (Combo-port)
	3x 10/100BaseT	Out-of-band Management I/Fs
	1x RS-232 (D-SUB9, female)	Console port
	1x Alarm Connector	NOC (normal open connector)

Table A-5 Technical Data of the Interfaces

Interfaces	
Fast Ethernet Interfaces (Copper)	
Type:	IEEE 802.3 (full- and half-duplex, Autonegotiation)
Data-rate	10 or 100Mbps
Connection type:	Twisted-Pair interface (TP)
Function, electrical values, pin-assignment:	according to IEEE 802.3i (10BaseT), IEEE 802.3u (100BaseTX)
Impedance:	100 Ohm (balanced)
Connector:	8 pin RJ45 connector according to ISO 8877
Console Port	
Type:	EIA-232-F (RS-232)
Connector:	D-SUB9, female

Table A-5 Technical Data of the Interfaces (continued)

Interfaces	
Fast Ethernet Interfaces (Copper)	
Connection type:	DCE
Speed, Settings:	115,200kBaud, 8 Bits, 1 Stop-bits, no bit parity, no flow control: (115k, 8N1)
Other Connectors	
DC plug	3W3. male
Alarm Connector:	RIA (3 pin)

Remote Power Feeding

Table A-6 Technical Data remote Power Feeding

Type	
Voltage, Current	
Output voltage	112V, +/- 3V
Output Current	min 60mA, max 70mA
Current Limitation	70mA; after T=3sec the RF will be shut-down to prevent limiter from damage.
Automatic switch-off	
Output Voltage	If (accumulated) voltage at SDSLout is higher than 120V, the device will switch off the RF within 200ms.
Output Current	The current is limited to max 70mA. After 3 secs of current limitation, the RF will be switched off.
Re-Enable	After the reason for the above mentioned switch-off disappears, the RF shall be switched-on again within 30 s.
Measurements	
U (a-b)	Remote power voltage between a-wire and b-wire is measured.
U (a-gnd)	Remote power between a-wire and ground is measured.
U (b-gnd)	Remote power between b-wire and ground is measured.
I (out)	Remote power current is measured.

Table A-6 Technical Data remote Power Feeding (continued)

Type	
Cycle Time	Measurements is done periodically. The duration of a measurement cycle over all measurements of the RPX16 does not exceed 10 s.

µController, Display & Clock

Table A-7 Display Functions

Type	
Display Functions	
System:	19 LEDs for system, operating and error status
Fast Ethernet interface (MGMT):	2 LEDs for Link Status, Activity and 10/100Mbps recognition

Table A-8 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

RPX Software Specification

Table A-9 Technical Data of the RPX - Software

RPX16		
General Information		
Valid SW-Version for this manual: V 1_1_00 ⁱ		
Standards		
Internet Protocol:	IPv4	
	IPv6	
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-10 Management & Security

RPX-Family	RPX16
HTTP server	yes
HTTPS 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: RPX – Remote Power Unit
Members: FSP-RPX16
Number: 1303-1001

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, 14.03.2014

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